Selbstdatenschutz im vernetzten Fahrzeug

Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug

Veröffentlichung Nummer: D1

Version 1.0

GEFÖRDERT VOM

Projekt Akronym: SeDaFa
Vollständiger Projekttitel: Selbstdatenschutz im vernetzten Fahrzeug
Projektwebseite: http://www.sedafa-projekt.de/

Veröffentlichungsdatum	02.08.2017	
Seitenanzahl:	126	
Schlagwörter:	Vernetztes Fahrzeug, Privatsphäre, Datenschutz, Selbstdatenschutz	

Autoren:	Nadine Sinner	accessec GmbH
	Christian Plappert	Fraunhofer SIT
	Sebastian Mauthofer	Fraunhofer SIT
	Daniel Zelle	Fraunhofer SIT
	Christoph Krauß	Fraunhofer SIT
	Jonas Walter	Technische Universität Darmstadt
	Bettina Abendroth	Technische Universität Darmstadt
	Rasmus Robrahn	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
	Harald Zwingelberg	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
	Thilo von Pape	Universität Hohenheim
	Hendrik Decke	Volkswagen AG
	Niko Gasch	Daimler AG
	Florian Springborn	Daimler AG
	Tanja Verdezki	Der Hessische Datenschutzbeauftragte

Inhaltsverzeichnis

Executive Summary

In der Automobilindustrie spielt die digitale Informationserhebung und –verarbeitung eine immer größere Rolle. Im Fahrzeug werden Sensordaten nicht mehr nur in den einzelnen Steuergeräten direkt verarbeitet, sondern kommen auch in Fahrerassistenzystemen und Komfortfunktionen zum Einsatz. Hinzu kommt, dass die Vernetzung der Fahrzeuge kontinuierlich zunimmt und immer mehr Fahrzeugdaten im Internet gesammelt und verarbeitet werden. Teils mit dem Zweck den Fahrzeugnutzern Mehrwertdienste anbieten zu können, teils um Produktverbesserungen zu ermöglichen. Bereits jetzt sind viele der dabei anfallenden Daten personenbezogen oder personenbeziehbar und ermöglichen z.B. die Erstellung von Bewegungsprofilen oder von Profilen des Fahrverhaltens des Fahrzeugnutzers. Ziel von SeDaFa ist es, Selbstdatenschutz für den Fahrzeugnutzer sicherzustellen. Hierzu werden neue Ansätze und Werkzeuge entwickelt, um Fahrzeugnutzern transparent darzustellen, welche Daten im Fahrzeug vorhanden sind, wie der Personenbezug aussieht, wie sie verarbeitet und weitergeleitet werden und welche Risiken bestehen. Weiterhin werden neue Ansätze entwickelt, die dem Fahrzeugnutzer eine selbstbestimmte Kontrolle bei der Weitergabe der eigenen Fahrzeugdaten ermöglicht. Hierzu werden u.a. Ansätze zur Anonymisierung und Pseudonymisierung und geeignete Verschlüsselungsverfahren zur Sicherstellung der Vertraulichkeit entwickelt, die sowohl rechtliche als auch sozial- und wirtschaftswissenschaftliche Aspekte berücksichtigen.

Zunächst wird eine Referenzarchitektur vorgestellt, welche die beteiligten Komponenten und deren Verbindungen in einer abstrakten Form darstellt. Der Fokus liegt hierbei darauf, für den Datenschutz relevante Schnittstellen und Datenflüsse unabhängig von einem spezifischen Fahrzeugmodell darstellen und beschreiben zu können. Es ist nicht Ziel der Architektur eine technisch möglich genaue Abbildung moderner Fahrzeuge zu erstellen.

Nach der Einführung der Fahrzeugarchitektur werden konkrete Anwendungsfälle beschrieben. Die Anwendungsfälle sind so gewählt, dass sie beispielhaft einen Großteil der Funktionen abbilden, bei denen Fahrzeuge Informationen mit der Außenwelt teilen. Sie bilden die Grundlage der weiteren Untersuchungen. Angelehnt sind die Anwendungsfälle an tatsächliche Anwendungen in vernetzten Fahrzeugen, entsprechen aber nicht notwendiger Weise der wirklichen Implementierung oder dem wirklichen Datenfluss. Teilweise wurden auch bewusst datenschutzkritische Datenflüsse erzeugt um Probleme des vernetzten Fahrzeugs aufzuzeigen. Konkret wurden zehn Anwendungsfälle spezifiziert, die sich einer von sechs übergeordneten Kategorien zuordnen lassen, und möglichst alle datenschutzrelevanten Datenflüsse im vernetzen Fahrzeug abdecken sollen.

Die erste Kategorie „Mehrfache Fahrzeugnutzung“ umfasst dabei Anwendungsfälle bei denen mehr als eine Person Zugriff auf ein Fahrzeug haben, wozu zum Einen Car Sharing Dienste zählen, bei denen Kunden dasselbe Fahrzeug nutzen können, als auch zum Anderen die Werkstatt, bei der zum Beispiel der KFZ-Mechaniker innerhalb eines Werkstattbesuchs Zugriff auf das Fahrzeug bekommt. Innerhalb der Kategorie „Lokationsbasierte Dienste“ wird der Anwendungsfall „Ortung und Reaktion“ betrachtet, bei dem im Zusammenhang mit der Position des Fahrzeugs bestimmte Aktionen ausgeführt werden. Unter die Kategorie „Smartphone Integration/Drittanbieter Erweiterungen“ fallen die Anwendungsfälle „Android Auto“ und „Paket Auto“, wobei der erstere die Interaktion des Smartphones als integrative Komponente im Fahrzeug untersucht, während der zweite das Zusammenspiel zwischen Fahrer und Fahrzeug mit Hersteller- und Drittanbieter-Diensten, in diesem Fall einem Paketzustelldienst, betrachtet. Zur vierten Kategorie „Statistische Analysen“ lassen sich die Anwendungsfälle „Umgebung“, bei dem Umgebungssensoren der Fahrzeuge für die Erkennung freier Parkplätze genutzt werden, als auch „Verschleißanalyse“ zusammenfassen, bei dem im Fahrzeug zum Beispiel kontinuierlich Zustandsdaten über Verschleißteile erhoben und an das Backend von Herstellern bzw. Zulieferern zur weiteren Verarbeitung gesendet werden. Im Umfeld der Elektromobilität beschränken wir uns auf den konkreten Anwendungsfall „Laden und Bezahlen“ und den damit verbundenen datenschutzrelevanten Datenflüssen. Die letzte Kategorie „Insassenüberwachung“ umfasst schließlich die Überwachung von Fahrer- und Fahrverhalten und ihr werden die beiden Anwendungsfälle „Fahrerverhalten“ und „Fahrerüberwachung“ zugeordnet. Der erste beschäftigt sich mit der Überwachung des Fahrverhaltens wie es von sogenannten “Pay-As-You-Drive”-Versicherungen angeboten wird, um entsprechend der Fahrweise des Fahrers verschiedene Konditionen anbieten zu können, während sich der zweite Anwendungsfall direkt mit der Überwachung des Fahrers zum Beispiel im Fall Müdigkeitserkennung beschäftigt.

Das Kapitel Datentaxonomie zielt darauf ab Transparenz und Verständlichkeit hinsichtlich des Umgangs mit den anfallenden Daten zu ermöglichen. Die Taxonomie stellt ein Regelwerk zur umfassenden Einordnung der anfallenden Daten in spezifische verschiedene distinkte Klassen dar, wobei eine mehrfache Zuordnung möglich ist um verschiedene Perspektiven abbilden zu können. Neben einer sinnvollen Granularität liegt ein besonderes Augenmerk auf der Darstellung der gesetzlichen Realität. Es werden sowohl Klassifikationen aus rechtlicher Perspektive, technischer Perspektive und aus

Nutzersicht betrachtet.

Unter Berücksichtigung der Anwendungsfälle und der Datentaxonomie wird anschließend eine Risikobewertung und Schutzbedarfsfeststellung nach dem Standard-Datenschutzmodell (SDM) vorgenommen. Eine Risikobewertung nach SDM hat die Aufgabe den Schutzbedarf eines bestimmten Verfahrens festzustellen. Die Feststellung des Schutzbedarfs ist dann im nächsten Schritt Grundlage für die Entwicklung eines Anforderungskatalogs. Je höher der Schutzbedarf ist, desto umfassender müssen auch die technischen und organisatorischen Anforderungen an ein personenbezogenes Verfahren sein.

Das darauffolgende Kapitel beschäftigt sich mit der Nutzersicht auf das Thema Datenschutz in Fahrzeugen. Zum einen wird auf bereits existierende Untersuchungen hingewiesen, zum anderen werden Ergebnisse von zwei Studien vorgestellt, die im Rahmen des SeDaFa-Projektes durchgeführt wurden. Eine Studie ist eine quantitative Befragungsstudie und verfolgt die Fragen unter welchen Bedingungen Nutzer bereit sind ihre Daten preis zu geben, welche Zusammenhänge zwischen der Datenschutzeinstellung im Auto und dem Datenschutzverhalten im Alltag bestehen und welche Maßnahmen die Bereitschaft zur Datenpreisgabe steigern. Die andere Studie ist eine qualitative Nutzerstudie und behandelt die Wahrnehmung der Problematik des Selbstdatenschutzes, der Erwartungen und Einstellungen der Nutzer zum Datenschutz und der Strategien und Verhaltensweisen zum Schutz der eigenen Daten.

Abschließend werden juristische Anforderungen und Anforderungen die sich aus der Nutzersicht ergeben gesammelt und daraus technische Anforderungen für den Selbstdatenschutz abgeleitet. Diese bilden die Grundlage für die nachfolgenden Arbeitspakete.

1. Motivation

IT ist einer der größten Innovationsmotoren in der Automobilindustrie und ist unabdingbar für viele Anwendungen wie z.B. Assistenzsysteme, Mehrwertdienste oder auch das autonome Fahren. Viele der dabei anfallenden Daten sind jedoch personenbezogen oder personenbeziehbar und ermöglichen z.B. die Erstellung von Bewegungsprofilen oder von Profilen des Fahrverhaltens des Fahrzeugnutzers. Ziel von SeDaFa ist es, neue Wege für den Selbstdatenschutz durch Fahrzeugnutzer zu entwickeln und bewerten.

Hierzu werden neue Ansätze und Werkzeuge entwickelt, um Fahrzeugnutzern transparent darzustellen, welche Daten im Fahrzeug vorhanden sind, wie der Personenbezug aussieht, wie sie verarbeitet und weitergeleitet werden und welche Risiken bestehen. Weiterhin werden neue Ansätze entwickelt, die dem Fahrzeugnutzer eine selbstbestimmte Kontrolle bei der Weitergabe der eigenen Fahrzeugdaten ermöglicht. Dazu werden u.a. Ansätze zur Anonymisierung und Pseudonymisierung und geeignete Verschlüsselungsverfahren zur Sicherstellung der Vertraulichkeit entwickelt, die sowohl rechtliche als auch nutzerseitige und wirtschaftliche Aspekte berücksichtigen. Dafür ist das Projektkonsortium interdisziplinär aufgestellt. Es umfasst Experten und Akteure in Fragen der Datensicherheit, des Datenschutzrechts, der Herstellung von Fahrzeugen und IT-Sicherheitslösungen, der Ergonomie und der nutzerseitigen Privatheitseinstellungen.

In diesem Dokument werden Datenflüsse im Fahrzeug in Form von Anwendungsfällen erfasst und die dabei anfallenden Daten kategorisiert. Weiter werden auf der Basis von Rechtstexten und Befragungsstudien juristische und nutzerseitige Voraussetzungen für den Selbstdatenschutz erarbeitet. Abschließend werden aus den gesammelten Erkenntnissen die technischen, rechtlichen und nutzerorientierten Anforderungen ermittelt anhand derer Konzepte und Verfahren zum Selbstdatenschutz in Fahrzeugen entwickelnden.

Als Arbeitsdefinition für den Begriff des vernetzten Fahrzeugs stützen wir uns hier auf eine Unterscheidung aus der gemeinsamen Erklärung des Verbands der Autoindustrie und der Datenschutzbehörden. Diese differenziert zwischen vernetzten („online“) und nicht vernetzten („offline“) Fahrzeugen in Abhängigkeit vom Zeitpunkt der Datenerhebung durch eine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes: „Hier ist zu unterscheiden, ob es sich um Kraftfahrzeuge handelt, bei denen eine Datenspeicherung innerhalb des Fahrzeuges stattfindet („offline“), oder ob eine Übermittlung von Daten aus dem Fahrzeug heraus erfolgt („online“), wie etwa bei der Übermittlung und Speicherung von Fahrzeugdaten auf Backend-Servern“. Notwendiges und hinreichendes Merkmal für ein vernetztes Fahrzeug ist also, dass eine solche Übermittlung online von Daten aus dem Fahrzeug heraus erfolgt.

2. Referenzarchitektur

Um ein allgemeines Verständnis für die Datenflüsse im Kontext Fahrzeug zu erlangen, wird zunächst eine Referenzarchitektur vorgestellt, welche die beteiligten Komponenten in einer abstrakten Form darstellt. Diese wird in Abbildung 2.1 gezeigt und die einzelnen Komponenten werden in Tabelle 2.1 beschrieben. Der Fokus liegt hierbei darauf eine abstrakte Darstellung der für den Datenschutz relevanten Schnittstellen und Datenflüsse zu ermöglichen. Es ist nicht Ziel, eine technisch möglichst genaue Abbildung moderner Fahrzeuge zu erstellen. Daher wird beispielsweise zwischen unterschiedlichen Steuergeräten nicht unterschieden, da die dahinterstehende Funktion im Sinne des Projektes im Gegensatz zu den von ihnen konsumierten und erzeugten Daten irrelevant ist.

Tabelle 2.1: Komponenten der Referenzarchitektur

Komponente	Beschreibung	Beispiel
Aktor	Technisches Bauteil, das elektrische Signale in physikalische Größen umsetzt.	Motoren (z.B. Elektro- oder Rotationsmotor), Einspritzventil, Heizungsregler
Datenmarktplatz	Vernetzung verschiedener Anbieter und Abnehmer von Daten mit ggf. wechselnden Beziehungen. Daten können sowohl direkt gehandelt oder auch gemeinsam von mehreren Interessenten oder Anbietern zusammengetragen werden.	Nokia Here; Werbeindustrie
Diagnoseadapter	Ein Adapter, der mit einem Diagnoseport verbunden wird, um Funktionen des Diagnoseports externen Geräten oder Systemen zur Verfügung zu stellen.	Bluetooth-ODB-II-Adapter, um per Smartphone Diagnosewerte auszulesen oder OBD-2-Internetadapter, die in Pay-As-You-Drive Szenarien Informationen zum Fahrverhalten per Mobilfunk an einen Server schicken.
Diagnosegerät	Gerät, mit welchem unter anderem Fehlercodes über den Diagnoseport abgerufen oder Fehlerspeicher zurückgesetzt werden können.	OBD-II-Diagnosegerät
Diagnoseport	Vom OEM vorgesehene und gesetzlich vorgeschriebene Schnittstelle um Werkstätten Zugriff auf das Fahrzeug zu geben.	OBD-II-Schnittstelle
Domäne	Sensoren, Aktoren und ECU, die zu einem gemeinsamen Funktionsbereich gehören, werden in Domänen separiert. Teilweise werden diese Domänen von einer Mischung aus zentralem Steuergerät und Gateway (“Domänencontroller”) kontrolliert. Zwischen den unterschiedlichen Domänen ist dadurch nur eine exakt definierte Kommunikation möglich.	Domänen: z.B. Antriebstrang, Karosserie, Fahrdynamik
Externe Dienstleister	Dienstleistungen von Drittanbietern, welche Daten vom Fahrzeug benötigen oder Daten zum Fahrzeug senden.	Kartenanbieter, Wetterdienste, Google (Android Auto), Apple (CarPlay)
Gateway	Vermittler zwischen verschiedenen Fahrzeugbussen bzw. Domänen; kontrolliert ggf. auch den Informationsfluss	
Infotainmentsystem	Zusammenführung verschiedener Fahrzeugsysteme im Bereich Komfort, Information und Entertainment; hohe Rechenleistung	Komponenten: Autoradio, Navigationssystem, Freisprecheinrichtung, Klimakontrolle, …

Komponente	Beschreibung	Beispiel
Infrastruktur	(Stationäre) Systeme im Umfeld des Fahrzeugs mit denen eine Interaktion bzw. Kommunikation stattfindet; meistens ist die Position und Identität der Infrastrukturkomponenten bekannt	Ladesäule, Ampel, Baustellenanhänger
Kombiinstrument	Anzeige für den Fahrer mit den wichtigsten Fahrzeuginformationen	Komponenten: Tachometer, Kilometerzähler, Drehzahlmesser, Tankanzeige, Kühlmitteltemperaturanzeige, Kontrollleuchten, Fahrtrichtungsanzeiger
OEM-Backend	Im Speziellen Dienstleistungen des Herstellers welche Daten vom Fahrzeug benötigen oder Daten zum Fahrzeug senden.	Navigation, Verkehrsinformationen, Kundenservice, ...
Schnittstellen	Technische Bauteile mit denen das Fahrzeug mit seiner Umwelt bzw. die Umwelt mit dem Fahrzeug kommunizieren kann.	Diagnoseport, Wechseldatenträger, Funk- und Kabelverbindungen
Sensor	Technisches Bauteil, das physikalisch/chemische Eigenschaften in der Umgebung oder im Fahrzeug qualitativ/quantitativ erfasst und in ein elektrisches Signal umwandelt.	Temperaturmessfühler, Beschleunigungssensor, Abstandssensor, ...
Steuergerät (ECU)	Technische Bauteile, die nach dem EVA-Prinzip arbeiten. Sie verarbeiten Informationen etwa von Sensoren oder anderen ECUs und führen abhängig von der Verarbeitung Aktionen etwa Ansteuerung von Aktoren oder Weitergabe der Daten an ECUs aus.	Motorsteuergerät, Getriebesteuergerät, Klimaanlagensteuergerät.
TK-Anonymisierung	Dienst des Telekommunikationsanbieters, der Daten vom bzw. zum Fahrzeug zunächst anonymisiert bevor diese in das Fahrzeug bzw. zu Dienstleistern gelangen.	Telekom für Stauinfos
Umwelt	Alle Entitäten (Menschen oder Geräte/Maschinen), die mit dem Fahrzeug über die Schnittstellen kommunizieren	Nutzer, KFZ-Mechaniker, Externer Dienstleister, Verkehrsteilnehmer, Infrastrukturkomponente
Verkehrsteilnehmer	Vernetzte Entitäten, die sich mit dem Fahrzeug im Straßenverkehr befinden.	andere KFZ, Infrastrukturkomponenten
Zentrales Steuergerät	Ein Steuergerät mit hoher Rechenleistung zur domänenübergreifenden Darstellung einer oder mehrerer Funktionen.	Steuergerät für automatisches Fahren

Wie Abbildung 2.1 und der Tabelle 2.1 zu entnehmen ist, werden zukünftige Fahrzeuge nicht mehr in sich abgeschlossene technische Systeme sein, sondern über eine Vielzahl externer Schnittstellen mit der Außenwelt kommunizieren und interagieren. Hierbei ist prinzipiell zwischen drei Typen von Kommunikationsschnittstellen zu unterscheiden. Erstens existiert der gesetzlich vorgeschriebene Diagnoseport über den eine festgelegt Mindestmenge von Daten und Protokollen zur Verfügung gestellt werden. Zweitens gibt es eine wachsende Menge von drahtlosen Kommunikationskanälen welche von Bluetooth, LTE/GSM über WLAN bis zu Car2Car- oder Car2X-Kommunikation reichen. Diese Schnittstellen sollen dabei immer eine spezifische Rolle erfüllen und sind selten redundant gegeneinander austauschbar. Zuletzt gibt es physikalische Ports im Fahrzeug in welche Datenträger eingebracht werden können. Hierzu gehören CD- und DVD-Laufwerke, USB-Ports sowie SD-Kartensteckplätze. Diese Vielzahl von Schnittstellen sind in diesem Projekt besonders relevant, da bezüglich des Datenschutzes erst in dem Fall eine Datenübertragung relevant wird, wenn diese Daten aus dem Inneren des Fahrzeuges an die Außenwelt kommuniziert, was in der Referenzarchitektur nur an diesen Schnittstellen möglich ist.

Innerhalb des Fahrzeuges werden Daten zwischen verschiedenen Komponenten, Steuergeräten und Systemen übertragen. Das Fahrzeug ist dabei in mehrere logische Domänen eingeteilt wie zum Beispiel „Antrieb“, „Karosserie“ oder „Fahrdynamik“. Innerhalb dieser Domänen existieren eine Vielzahl von Steuergeräten (kurz ECUs), Aktoren und Sensoren, welche untereinander direkt über einen oder mehrere geteilte Kommunikationskanäle (z.B. CAN, LIN oder FlexRay) je Domäne verbunden sind. Die verschiedenen Kommunikationskanäle im Fahrzeug sind für die Kommunikation zwischen unterschiedlichen Domänen durch ein Gateway voneinander getrennt. Das Gateway ist dafür zuständig nur erlaubte und

gewünschte Daten zwischen unterschiedlichen Domänen weiterzuleiten. Weiterhin gibt es einige besondere Komponenten, die eine oder mehrere Sonderrollen im Fahrzeug einnehmen. Hierzu gehören das Kombiinstrument zur Anzeige der aktuellen Fahrwerte und des Kilometerstandes, ein Infotainment-System zur Ausführung von Multimedia-Inhalten und Online-Diensten sowie spezielle zentrale Steuergeräte, die domänenübergreifend Funktionen ausführen.

Außerhalb des Fahrzeuges existiert eine Vielzahl weiterer Komponenten und Akteure. Hierzu gehören ein KFZ-Mechaniker/-Dienstleister, welcher mit einem Diagnosegerät am Diagnoseport Daten ausliest, weitere Verkehrsteilnehmer, Infrastruktur(komponenten), Mobiltelefone und PCs, welche über unterschiedliche Schnittstellen Daten mit dem Fahrzeug austauschen. Weiterhin kann ein Teil dieser Daten entweder direkt vom Fahrzeug oder indirekt durch einen der anderen Akteure im bzw. über das Internet kommuniziert werden. Hier können die Daten nach der Übertragung über das Internet entweder auf dem Backend des Fahrzeug-OEMs, bei anderen externen Dienstleistern oder auf einem Datenmarktplatz landen. Auf dem Weg in die verschiedenen Backend-Stationen kann eine TK-Anonymisierung zwischengeschaltet sein, welche IP-Adressen und weitere Informationen verschleiert um den Absender der Daten zu verstecken. Der wichtigste Akteur ist schlussendlich der Nutzer. Dieser interagiert mit den Mensch-Maschinen-Schnittstellen und dem Infotainment-System des Fahrzeuges, dem Smartphone, den PCs und den sonstigen Akteuren innerhalb der Referenzarchitektur. Mit welchen Komponenten der Nutzer dabei interagiert ist vom spezifischem Anwendungsfall abhängig.

Mit diesem ersten Überblick über das vernetzte Fahrzeug betrachten wir im nächsten Kapitel mögliche Anwendungsfälle bei denen Daten aus dem Fahrzeug ausgelesen oder übertragen werden.

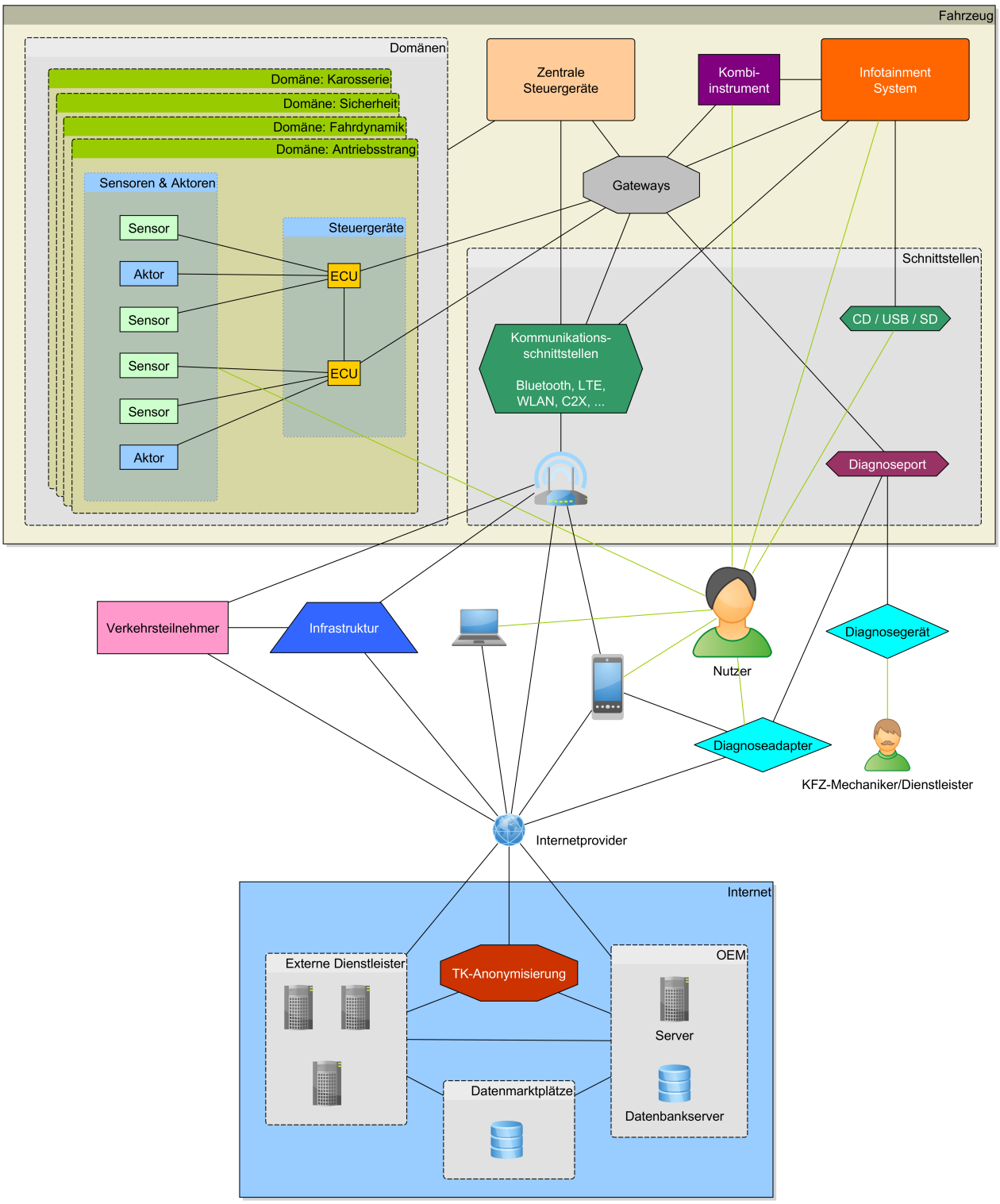


Abbildung 2.1: Abstrakte Referenzarchitektur

3. Anwendungsfälle

Nach der Einführung der Fahrzeugarchitektur mit ihren vielfältigen Schnittstellen zur Außenwelt betrachten wir nun konkrete Anwendungsfälle, bei denen diese Schnittstellen genutzt werden, die die Grundlage weiterer Untersuchungen bilden. Angelehnt sind die Anwendungsfälle an tatsächliche Anwendungen in vernetzten Fahrzeugen, entsprechen aber nicht notwendiger Weise der wirklichen Implementierung oder dem wirklichen Datenfluss. Teilweise wurden auch bewusst datenschutzkritische Datenflüsse erzeugt, um Probleme des vernetzten Fahrzeugs aufzuzeigen.

Konkret wurden zehn Anwendungsfälle spezifiziert, die sich einer von sechs übergeordneten Kategorien zuordnen lassen, die möglichst alle datenschutzrelevanten Datenflüsse im vernetzen Fahrzeug abdecken sollen (s. Tabelle 3.1).

Die ersten Kategorie *Mehrfache Fahrzeugnutzung* umfasst dabei Anwendungsfälle, bei denen mehr als eine Person Zugriff auf ein Fahrzeug haben, wozu zum Einen *Car Sharing* Dienste zählen, bei denen Kunden dasselbe Fahrzeug nutzen können, als auch zum Anderen die *Werkstatt*, bei der zum Beispiel der KFZ-Mechaniker innerhalb eines Werkstattbesuchs Zugriff auf das Fahrzeug bekommt. Innerhalb der Kategorie *Lokationsbasierte Dienste* wird der Anwendungsfall *Ortung und Reaktion* betrachtet, bei dem im Zusammenhang mit der Position des Fahrzeugs bestimmte Aktionen ausgeführt werden. Unter die Kategorie *Smartphone Integration/Drittanbieter-Erweiterungen* fallen die Anwendungsfälle *Android Auto* und *Paket-Auto*, wobei der erstere die Interaktion des Smartphones als integrative Komponente im Fahrzeug untersucht, während der zweite das Zusammenspiel zwischen Fahrer und Fahrzeug mit Hersteller- und Drittanbieter-Diensten, in diesem Fall einem Paketzustelldienst, betrachtet.

Tabelle 3.1: Anwendungsfallübersicht

	Kategorie	*Anwendungsfall*
1	Mehrfache Fahrzeugnutzung	Car Sharing, Werkstatt
2	Lokationsbasierte Dienste	Ortung und Reaktion
3	Smartphone Integration / Drittanbieter-Erweiterungen	Android Auto, Paket-Auto
4	Statistische Analysen	Umgebung, Verschleißanalyse
5	Elektromobilität	Laden und Bezahlen
6	Insassenüberwachung	Fahrerverhalten, Fahrerüberwachung

Zur vierten Kategorie *Statistische Analysen* lassen sich die Anwendungsfälle *Umgebung*, bei dem Umgebungssensoren der Fahrzeuge für die Erkennung freier Parkplätze genutzt werden, als auch *Verschleißanalyse* zusammenfassen, bei dem im Fahrzeug zum Beispiel kontinuierlich Zustandsdaten über Verschleißteile erhoben und an das Backend von Hersteller bzw. Zulieferer zur weiteren Verarbeitung gesendet werden. Im Umfeld der *Elektromobilität* beschränken wir uns auf den konkreten Anwendungsfall *Laden und Bezahlen* und den damit verbundenen datenschutzrelevanten Datenflüssen. Die letzte Kategorie *Insassenüberwachung* umfasst schließlich die Überwachung von Fahrer- und Fahrverhalten und ihr werden die beiden Anwendungsfälle *Fahrerverhalten* und *Fahrerüberwachung* zugeordnet. Der erste beschäftigt sich mit der Überwachung des Fahrverhaltens wie es von sogenannten “Pay-As-You-Drive”-Versicherungen angeboten wird, um entsprechend der Fahrweise des Fahrers verschiedene Konditionen anbieten zu können, während sich der zweite Anwendungsfall direkt mit der Überwachung des Fahrers zum Beispiel im Fall Müdigkeitserkennung beschäftigt.

In den folgenden Kapiteln werden die oben vorgestellten Anwendungsfälle im Detail beschrieben, wobei die konkreten Abläufe nicht nur textuell-tabellarisch und anhand von UML-Diagrammen mit jeweils beteiligen Entitäten beschrieben werden, sondern auch explizit datenschutzrelevante Datenflüsse inklusive der betroffenen Daten gesondert aufgeführt werden.

3.1. Definition der Akteure

Speziell im Automobilkontext wird sind meherer Entitäten involviert die sich häufigst wiederholen und deren Rollen sich teilweise überschneiden. An dieser Stellen sollen die Entitäten vorgestellt und definiert werden, die in den Anwendungsfällen vorkommen.

3.1.1. Fahrzeug

Das Fahrzeug ist zentraler Bestandteil aller Anwendungsfälle. Da dieses Projekt sich mit datenschutz im Fahrzeug dreht handelt es sich dabei vorrangig aber nicht ausschließlich um PKWs, aber auch Transporter oder LKWs.

3.1.2. Kunde

Ein Kunde ist eine Person, die einen Vertrag abschließt um ein Objekt oder eine Dienstleistung zu erhalten

3.1.3. Halter

Der Halter ist der eingetragene Besitzer eines Fahrzeugs.

3.1.4. Fahrer

Der Fahrer ist eine Person die das Fahrzeug lenkt.

3.1.5. Insassen

Insassen sind alle personen, die sich in einem Fahrzeug befinden. Der Fahrer ist auch ein Insasse.

3.1.6. Hersteller (OEM)

Der Hersteller meint hier den Fahrzeughersteller.

3.2. Car Sharing

In diesem Anwendungsfall wird ein Car Sharing Szenario betrachtet.

Innerhalb des Anwendungsfalls müssen Fahrzeuge auf Anfrage des Car Sharing Kunden in seinem Umfeld angezeigt werden können, d.h. diese müssen zu einem bestimmten Zeitpunkt geortet werden. Sobald sich der Kunde im Fahrzeug befindet, kann er sein mobiles Endgerät (bspw. Smartphone) mit dem Fahrzeug verbinden, um Daten (bspw. Kontakte, Musik) mit Fahrzeug zu synchronisieren. Während der Fahrt können noch weitere externe Anwendungsfälle wie etwa *Android Auto* oder *Laden und Bezahlen* hinzukommen, falls der Kunde sich bspw. entschließt Apps herunterzuladen oder ein elektrisches Fahrzeug laden will. Mit einem Checkout beendet der Kunde seine Buchung und das Fahrzeug wird für weitere Buchungen wieder freigegeben.

Aus datenschutzrechtlicher Sicht ist in diesem Anwendungsfall sowohl die Ortung der Fahrzeuge während der Fahrzeugsuche, die unter Umständen die Erstellung von Bewegungsprofilen erlaubt, als auch der kontinuierliche Fahrerwechsel relevant, der eine Löschung eingebrachter Daten notwendig macht.

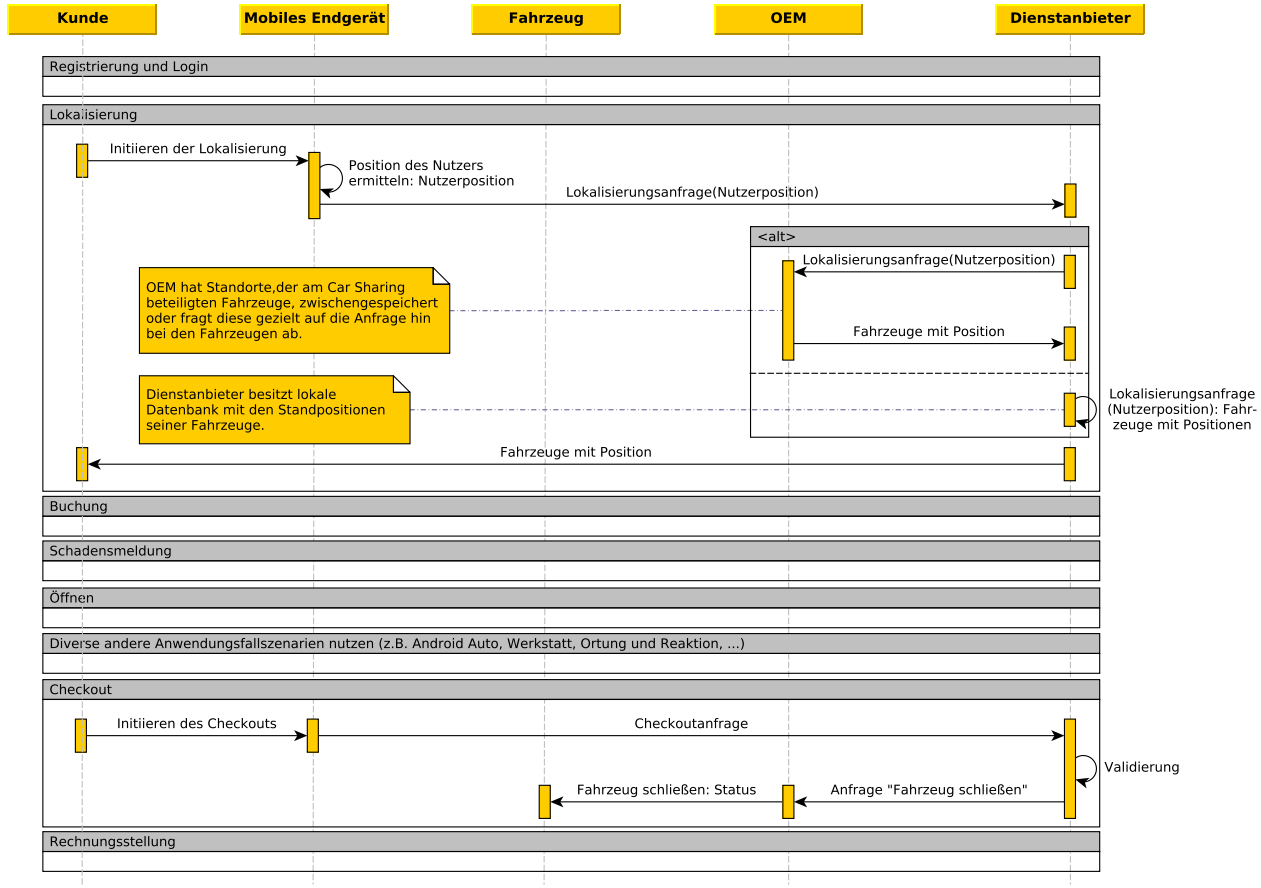
3.2.1. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Registrierung und Login: Kunde registriert sich bei dem Car Sharing Anbieter und erhält Zugangsdaten. Mit diesen loggt er sich beim Anbieter ein, um den Service zu nutzen.	Kunde, Dienstanbieter	Dienstanbieter ist derjenige der den Car Sharing Service anbietet.	—

2. *Lokalisierung der Fahrzeuge:* Der Kunde sucht nach geeigneten Fahrzeugen (bspw. mit Smartphone App oder Webapplikation). Die Suchanfrage mit gewünschter Position (und evtl. Suchradius) wird zum Anbieter weitergeleitet.	Beteiligte Entitäten sind von der Umsetzung abhängig (s. 2.1. bzw. 2.2.)		Position von Fahrzeugen, die möglicherweise gerade in Benutzung sind.
2.1. Direkt: Der Anbieter ruft die Positionen der Fahrzeuge im gewünschten Gebiet direkt ab und sendet diese zurück zum Kunden.	Kunde, Fahrzeug, Dienstanbieter		s.o.
2.2. Anbieter Backend: Der Anbieter ruft die Positionen der Fahrzeuge im gewünschten Gebiet in seiner eigenen Datenbank ab und sendet diese zurück an den Kunden.	Kunde, Dienstanbieter		s.o.
3. Buchung: Der Kunde bucht aufgrund der erhaltenen Daten ein verfügbares Fahrzeug für eine selbstdefinierte Zeitspanne. Das Fahrzeug wird für den Zeitraum für neue Buchungen gesperrt.	Kunde, Dienstanbieter		Buchungszeitpunkt
3.1. Nachbuchung: Der Kunde verlängert, sofern möglich, den Buchungszeitraum.	Kunde, Dienstanbieter		s.o.
4. Schadensmeldung: Der Kunde meldet einen Schaden an den Anbieter.	Kunde, Dienstanbieter	Wenn es sich um fahrzeug-interne Schäden handelt, sendet das Fahrzeug evtl. Fehlerspeicher an das Backend	Daten des vorherigen Fahrers (s. auch *8. Checkout*)
4.1. Vor Fahrtantritt: Der Kunde überprüft vor Fahrtantritt sein Fahrzeug und protokolliert eventuelle Schäden.	Kunde, Dienstanbieter (Fahrzeug)		s.o.
4.2. Während der Fahrt: Der Kunde verursacht den Schaden während der Fahrt.	Kunde, Dienstanbieter (Fahrzeug)		s.o.
5. Öffnen/Schließen des Fahrzeugs: Der Kunde öffnet oder schließt das Fahrzeug bspw. mit Smartphone App oder Zugangskarte (SmartCard).	Kunde, (Fahrzeug,) Dienstanbieter		Solange das Schließen nicht im Rahmen des *8. Checkout* passiert, dürfen Daten wie Ort und Zeitpunkt das Fahrzeug nicht verlassen.
5.1 Direkt: Kunde öffnet das Fahrzeug direkt durch Nahfunktechnik (z.B. NFC, Bluetooth).			
5.2 Via Backend: Kunde kontaktiert Anbieter der das Fahrzeug über eine Internetverbindung öffnet.			
6. Synchronisationsdienste: Der Fahrer synchronisiert Daten mit dem Fahrzeug (s. Use Case Synchronisationsdienste).	s. Use Case Synchronisationsdienste	s. Use Case Synchronisationsdienste	s. Use Case Synchronisationsdienste
7. AddIn Use Cases: Während der Fahrt kann der Fahrer diverse Aktionen durchführen. Diese können z.B. einen App Download (Use Case*Android Auto*), eine Reparatur (Use Case *Werkstatt*) oder Navigation (Use Case *Ortung und Reaktion*) umfassen.	s. entsprechenden Use Case.	s. entsprechenden Use Case.	s. entsprechenden Use Case.

8. *Checkout:* Der Kunde beendet seine Fahrt und gibt das Fahrzeug wieder für Buchungen frei.	Kunde, Fahrzeug, Dienstanbieter	Das Fahrzeug muss dem Backend seine Position mitteilen und z.B., ob es auch verschlossen wurde. Evtl. sind auch Statuswerte des Fahrzeugs wichtig (z.B. Tankfüllung und Betriebswerte für Abrechnung).	Vom Kunde eingebrachte Daten (Navigationsziele, synchronisierte Adressbücher, ...) müssen gelöscht werden
8.1. Vorzeitige Rückgabe: Der Kunde beendet die Buchung früher z.B. wegen eines Schadens am Fahrzeug.	Kunde, Fahrzeug, Dienstanbieter		
8.2. Verspätete Rückgabe: Der Kunde überzieht den vorher festgelegten Buchungszeitraum.	Kunde, Fahrzeug, Dienstanbieter	Evtl. Strafgebühren	
8.3. Ungültige Rückgabeposition des Fahrzeugs: Der Kunde gibt das Fahrzeug nicht an der vorgesehenen Station bzw. außerhalb des festgelegten Rückgabegebiets zurück.	Kunde, Fahrzeug, Dienstanbieter	Evtl. Strafgebühren, Fahrzeug muss vom Anbieter wieder an eine geeignete Stelle gebracht werden, je nach Umsetzung kann das Fahrzeug selbst die Rückgabe verhindern (z.B. durch Geofencing)	
9. Rechnungsstellung: Nachdem der Fahrer den Checkout erfolgreich durchgeführt hat, wird die Rechnungsstellung in die Wege geleitet und der entsprechende zu zahlende Preis ggf. aufgrund von zurückgelegter Strecke und/oder Ausleihdauer ermittelt.	Kunde, Dienstanbieter		

3.2.2. UML-basierte Beschreibung



3.2.3. Datenfluss-basierte Beschreibung

Use Case	Grund	Betroffene Daten	Datenfluss
Lokalisierung	Der Anbieter muss über die Position seiner Fahrzeuge informiert sein. Allerdings sollte dies nicht möglich sein, wenn ein Fahrzeug gerade von einem Kunden benutzt wird bzw. lediglich beim Checkout (s.u.).	Fahrzeugposition	Telemetrik-Einheit → Anbieter Backend
Checkout	Beim kundenseitigen Checkout muss sichergestellt werden, dass das Fahrzeug an einer gültigen Position abgestellt worden ist (*Geofencing*). Die Position darf nur beim Checkout abgefragt/übermittelt werden.	Fahrzeugposition	Telemetrik-Einheit → Anbieter Backend
Checkout	Zu Beginn des Checkout-Prozesses werden alle kundeneingebrachten Daten gelöscht.	Kundeneingebrachte Daten (z.B. synchronisierte Daten wie Adressbücher, Musik, ...)	-

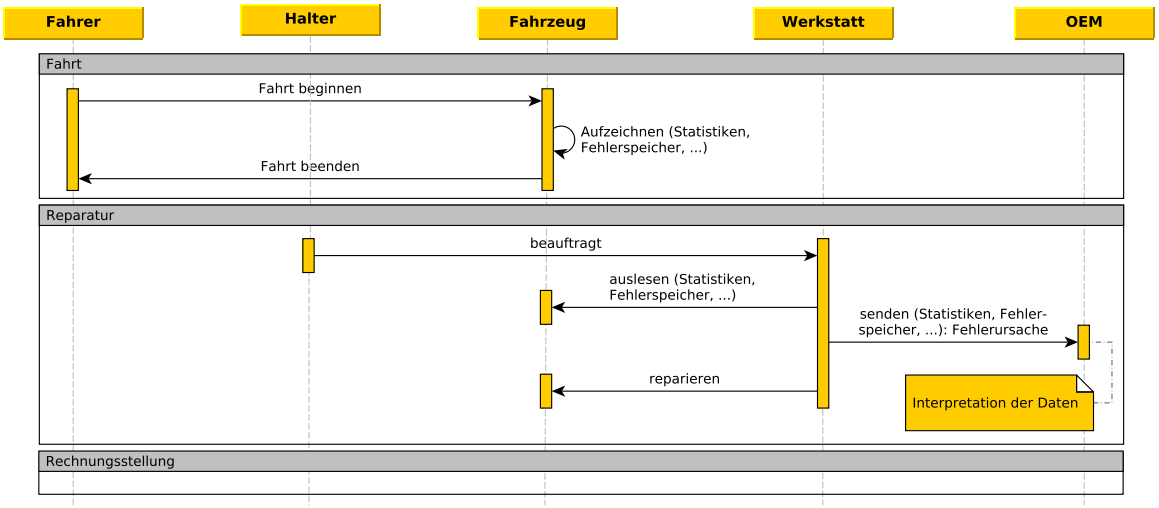
3.3. Werkstatt

Der Use Case beschreibt, wie Fahrzeugdaten von Werkstätten genutzt werden können. Dabei existieren drei Varianten. Das Fahrzeug kann erstens Daten zunächst in einem lokalen Speicher sammeln und diese werden dann bei einem Werkstattbesuch abgerufen. Die zweite Variante sieht vor, dass zwischen Fahrzeug und Werkstatt mit einer gewissen Regelmäßigkeit eine Kommunikation stattfindet, auf deren Grundlage dann beispielsweise der Bedarf für einen Werkstattbesuch festgestellt wird oder Updates eingespielt werden können. In der dritten Variante wird ein Unfalldatenspeicher in das Auto implementiert, der bei einem Verkehrsunfall gewisse Daten über das Fahrverhalten in einem gewissen Zeitraum vor dem Unfall dauerhaft speichert. Kommt es nicht zu einem Unfall, werden die Daten regelmäßig überschrieben. Zusätzlich kann bei einem Unfall automatisch oder manuell eine Verbindung mit einer Notrufzentrale hergestellt werden.

3.3.1. Textuelle Beschreibung: Variante “Datenerhebung in der Werkstatt”

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Implementierung der Diagnoseschnittstelle: Durch den Hersteller wird eine Schnittstelle im Fahrzeug integriert, über die Werkstätten Daten, die das Auto während des Betriebs sammelt, abrufen können.	Fahrzeughersteller		—
2. Aufzeichnung von Daten während des Fahrzeugbetriebs: Das Fahrzeug erfasst Daten in einem internen Speicher.	Fahrzeug, Fahrer		Fehlermeldungen, Verschleißdaten, Zähler für Anzahl und Länge Fahrten, Positionsdaten, Batteriezustand, Kilometerstand, Verbrauch, Reifendruck, Navigationsdaten
3. Werkstattbesuch, Wartungs- oder Reparaturauftrag	Fahrzeug, Fahrer, Halter, Werkstatt		
3.1 Auslesen der Daten: Die Daten werden aus dem internen Speicher des Fahrzeugs ausgelesen.	Fahrzeug, Werkstatt, evtl. Hersteller		
3.2 Analyse der Daten	Werkstatt, evtl. Hersteller		
3.3 Abhängig von 3.2 ggf. Konfiguration des Fahrzeugs	Fahrzeug, Halter, Werkstatt		
4. Aufzeichnung von Daten während des Fahrzeugbetriebs.	Fahrzeug, Fahrer		Grundsätzlich wie 2., kann aber auch von 3.2 abhängen.

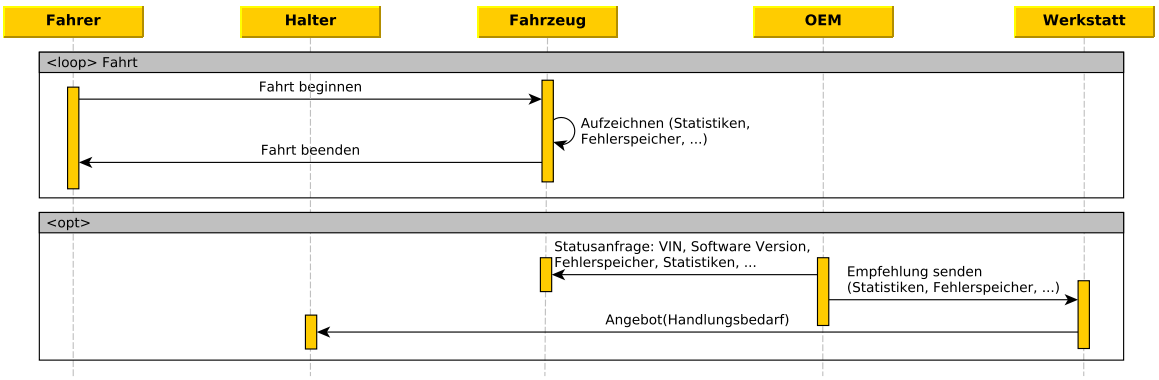
3.3.2. UML-basierte Beschreibung: Variante “Datenerhebung in der Werkstatt”



3.3.3. Textuelle Beschreibung: Variante “Fernwartung”

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Implementierung einer Fernwartungsschnittstelle.	Hersteller		
2. Registrierung für Fernwartungsdienst.	Fahrzeug, Halter, Werkstatt		Abrechnungsdaten, Fahrzeugidentifikator, Umfang der gebuchten Leistungen
3. Aufzeichnung von Daten.	Fahrzeug,		Fehlermeldungen, Verschleißdaten, Zähler für Anzahl und Länge Fahrten, Positionsdaten, Batteriezustand, Kilometerstand, Verbrauch, Reifendruck, Navigationsdaten
4. Übermittlung von Daten an Werkstatt oder Hersteller.	Fahrzeug, Halter, Werkstatt, Hersteller		
5. Ggf. Übermittlung der Daten an Werkstatt und Analyse der Daten.	Fahrzeug, Hersteller, Werkstatt		
6. Rückmeldung des Analyseergebnisses.	Fahrzeug, Halter, Werkstatt		
7. Einspielen von Updates.	Fahrzeug, Fahrer, Werkstatt		
8. Werkstattbesuch: Abhängig von Analyseergebnis. Siehe Variante 1 Nr. 3.	Fahrzeug, Fahrer, Werkstatt		Evtl Erheben von weiteren Daten

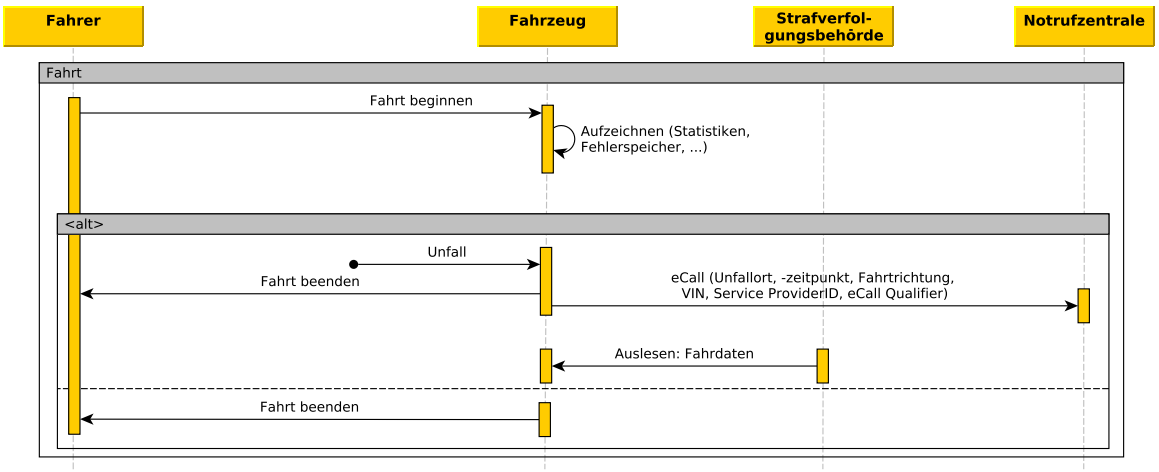
3.3.4. UML-basierte Beschreibung: Variante “Fernwartung”



3.3.5. Textuelle Beschreibung: Variante “Unfalldatenschreiber”

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Implementierung eines Unfalldatenschreibers.	Hersteller		
2. Fahrt und Aufzeichnung von Daten, regelmäßiges Überschreiben des Speichers.	Fahrer, Fahrzeug		Geschwindigkeit, Richtung, Beschleunigung, Blinkertätigkeit, Bremstätigkeit, Ort, Zeit, Auslösung von Assistenzsystemen,
3. Unfallereignis wird registriert.	Fahrzeug		
4. Überschreiben des Speichers wird beendet.	Fahrzeug		
5. Notsignal wird abgesendet (z.B. eCall Minimum Set of Data).	Fahrzeug, Notrufzentrale		Unfallort, Unfallzeitpunkt, Fahrtrichtung, FahrzeugID, Service ProviderID, eCall-Qualifier
6. Auslesen des Speichers durch Sachverständigen.	Halter/Fahrer/Eigentümer, Fahrzeug, Werkstatt (Sachverständiger)		
7. Weitergabe von Daten.	Halter/Fahrer/Eigentümer, Werkstatt (Sachverständiger), Versicherungen, Strafverfolgungsbehörden		

3.3.6. UML-basierte Beschreibung: Variante “Unfalldatenspeicher”



3.4. Location-based Services

Dieser Use Case fasst ortsbasierte Dienste wie POI, Fahrzeugortung oder Heimautomatisierung zusammen. Gemeinsam ist allen Diensten, dass basierend auf der Position des Fahrzeuges eine Aktion ausgelöst wird und z.B. Informationen übermittelt werden.

3.4.1. Varianten

A: Der Kunde legt initial seine Einstellungen/Präferenzen/Interessen fest. Wenn sich das Fahrzeug einem relevanten Ort nähert, wird eine Aktion ausgelöst (z.B. wird dem Nutzer die gewünschte Information angezeigt).

B: Der Kunde löst manuell eine Aktion (z.B. POI-Suche) aus. Dabei übermittelt er seine Interessen und das relevante Gebiet, was sowohl der direkte Umkreis des Fahrzeugs als auch eine geplante Strecke sein kann. Die Reaktion wird unmittelbar erwartet (z.B. Anzeige aller relevanten POIs für das Suchgebiet).

C: Eine Halter/Kunde oder ein System außerhalb des Fahrzeugs ortet das Fahrzeug, um basierend auf der Position weitere Aktionen auszuführen.

3.4.2. Textuelle Beschreibung (A)

1. **Registrierung und Login:** (optional) Der Kunde registriert sich bei dem Anbieter und erhält Zugangsdaten. Mit diesen loggt er sich beim Anbieter ein, um den Service zu nutzen.
2. **Konfiguration:** Der Kunde konfiguriert seine Einstellungen und legt die Bedingungen fest (z.B. wann, wo und unter welchen Umständen), unter denen bestimmte Aktionen ausgeführt werden sollen. Dies kann entweder lokal im Fahrzeug oder online beim Dienstanbieter geschehen.
3. **Lokalisierung:** Die Position des Fahrzeugs wird regelmäßig unter Verwendung der im Fahrzeug vorhandenen Sensoren (z.B. GPS, Koppelnavigation) bestimmt.
   a) **Option:** Die Position wird an den Dienstanbieter zur weiteren Analyse übermittelt
   b) **Option:** Die Position wird lokal im Fahrzeug verarbeitet und verlässt das Fahrzeug nicht. In diesem Fall muss das Fahrzeug alle Informationen lokal vorhalten die für die Relevanzprüfung der Position erforderlich sind.
4. **Abgleich mit den Aktionsbedingungen:** Es wird überprüft, ob sowohl die aktuelle Position als auch alle weiteren Bedingungen für eine oder mehrere Aktionen erfüllt sind. Die Verarbeitung kann wie bei der Lokalisierung entweder lokal oder extern erfolgen.
5. **Ausführen der Aktionen:** Die mit den Bedingungen verknüpften Aktionen werden ausgeführt. Dies kann gegebenenfalls auch mit der Übertragung von Informationen aus dem Fahrzeug ins Internet oder mit dem Abruf zusätzlicher Informationen einhergehen.

3.4.3. Datenfluss-basierte Beschreibung (A)

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Login	1. Beschränkung des Dienstes auf Registrierte Kunden; 2. Online-Profil in dem Einstellungen und Präferenzen verwaltet werden; 3. Verknüpfung mit weiteren Systemen	Identifizierende oder pseudonyme Daten die eine Verknüpfung mit einem Profil erlauben	Infotainmentsystem / Nutzer-Endgerät → Anbieter Backend
Konfiguration	Verwalten von Aktionsbedingungen	Vom Kunden eingegebene Informationen	Infotainmentsystem / Nutzer-Endgerät → Anbieter Backend
Lokalisierung	Relevanzanalyse der aktuellen Position	Fahrzeugposition	Sensoren → Anbieter Backend
Abgleich mit den Aktionsbedingungen	Überprüfung ob alle Bedingungen für eine Aktion erfüllt sind	Vom Nutzer festgelegte Daten, sofern sie im Fahrzeug anfallen, z.B. Richtung, Geschwindigkeit	Sensoren → Anbieter Backend
Ausführen der Aktionen	Notwendige Daten um die festgelegten Aktionen ausführen zu können	Beispiele: Fahrzeugposition, Logindaten für die Heimautomatisierung, Zustand des Fahrzeugs	Sensoren / Infotainmentsystem → Anbieter Backend

3.4.4. Konkrete Beispiele (A)

Beispiel 1: Ein Kunden möchte regelmäßig darüber informiert werden, ob es in seiner Nähe Geocaching-Orte gibt. Er registriert sich bei dem Geocaching-Dienst und verknüpft den Account mit dem Infotainmentsystem seines Autos. Er stellt in der Konfiguration ein, dass er bei der Fahrt auf der Karte alle Geocaching-Orte angezeigt bekommt die sich in einem Umkreis von 2km um sein Auto herum befinden. Als weitere Bedingungen gibt er ein, dass diese Informationen nur am Wochenende angezeigt werden sollen. Alle Geocaching-Orte im Umkreis von ca. 100km sollen dabei lokal im Fahrzeug gespeichert werden, so dass keine permanente Internetverbindung nötig ist. Wird ein Ort ausgewählt, sollen jedoch soweit möglich die Informationen auf Aktualität geprüft werden.

Beispiel 2: Ein Kunde möchte seine Heimautomatisierung mit dem Auto verknüpfen. Er hinterlegt im Fahrzeug den Account bei seinem Heimautomatisierungsanbieter. Als Konfiguration stellt er ein, dass wenn sich sein Auto mehr als 50km von seinem Haus entfernt hat und seit mehr als einer Stunde kein Bewegungsmelder ausgelöst wurde, sich die Alarmanlage scharf schaltet und die Heizung heruntergeregelt werden soll. Wenn sich das Auto wieder dem Haus nähert, soll die Heizung wieder die übliche Temperatur einstellen.

3.4.5. Textuelle Beschreibung (B)

1. **Registrierung und Login:** (optional) Der Kunde registriert sich bei dem Anbieter und erhält Zugangsdaten. Mit diesen loggt er sich beim Anbieter ein, um den Service zu nutzen.
2. **Konfiguration:** Der Kunde konfiguriert seine Parameter und Präferenzen für die Aktionen (z.B. Suchradius und Suchpräferenzen). Dies kann entweder lokal im Fahrzeug oder online beim Dienstanbieter geschehen.
3. **Lokalisierung:** Die Position des Fahrzeugs wird beim Auslösen einer Aktion unter Verwendung der im Fahrzeug vorhandenen Sensoren (z.B. GPS, Koppelnavigation) bestimmt. Optional kann auch eine geplante Navigationsroute berücksichtigt werden.
4. **Ausführen der Aktionen:** Die mit den Bedingungen verknüpften Aktionen werden ausgeführt. Dies kann gegebenenfalls auch mit der Übertragung von Informationen aus dem Fahrzeug ins Internet oder mit dem Abruf zusätzlicher Informationen einhergehen
   a) **Option:** Die Position/Navigationsroute wird an den Dienstanbieter zusammen mit den Einstellungen und den Funktionsparametern (z.B. der POI-Anfrage) zur weiteren Analyse übermittelt. Die Ergebnisse werden dann an das Fahrzeug gesendet welches diese dem Fahrer anzeigen und ggf. weitere Aktionen ausführen kann.
   b) **Option:** Die Position/Navigationsroute und die Parameter werden lokal im Fahrzeug verarbeitet und verlassen das Fahrzeug nicht. In diesem Fall muss das Fahrzeug alle Informationen lokal vorhalten, die für die

Durchführung der Aktion erforderlich sind.

c) **Option:** Wie Option 2, nur noch zusätzlich mit der Möglichkeit einzelne Informationen online zu validieren oder zu aktualisieren.

3.4.6. Datenfluss-basierte Beschreibung (B)

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Login	1. Beschränkung des Dienstes auf registrierte Kunde; 2. Online-Profil, in dem Einstellungen und Präferenzen verwaltet werden; 3. Verknüpfung mit weiteren Systemen	Identifizierende oder pseudonyme Daten, die eine Verknüpfung mit einem Profil erlauben	Infotainmentsystem / Nutzer-Endgerät → Anbieter Backend
Konfiguration	Verwalten von Parametern und Präferenzen	Vom Nutzer eingegebene Informationen	Infotainmentsystem / Nutzer-Endgerät → Anbieter Backend
Lokalisierung	Ortsinformationen als Parameter für die Aktionen	Fahrzeugposition, (Navigationsroute)	(Sensoren → Infotainmentsystem)
Ausführen der Aktionen	Notwendige Daten, um die festgelegten Aktionen ausführen zu können	Beispiele: Fahrzeugposition, POI-Typ, Parameter und Präferenzen	Sensoren / Infotainmentsystem -→ Anbieter Backend

3.4.7. Konkrete Beispiele (B)

Beispiel 1: Ein Kunde möchte sich alle Restaurants im Umkreis von 5km anzeigen lassen, die Schnitzel im Angebot und gerade geöffnet haben. **Beispiel 2:** Ein Kunde bekommt bei der Fahrt angezeigt, dass sein der Füllstand seines Benzintanks so niedrig ist, dass das Auto nur noch eine Reichweite von 30km hat. Er klickt auf die Warnmeldung und wählt die Option alle Tankstellen entlang seiner Navigationsroute anzuzeigen, die innerhalb der noch verbleibenden Reichweite sind. Die Tankstellen sind zwar auch lokal im Fahrzeug gespeichert, aber der Nutzer möchte gerne zusätzlich die aktuellen Spritpreise angezeigt bekommen. **Beispiel 3:** Um sich den Parkplatz seines Autos zu merken, übermittelt der Nutzer die aktuelle Position des Autos an eine Smartphone-App. Da er das Auto an eine elektrische Ladesäule gehängt hat, wird zusätzlich auch die Information übertragen, zu welcher Uhrzeit das Auto voraussichtlich vollständig geladen ist.

3.4.8. Textuelle Beschreibung (C)

1. **Registrierung und Login:** (optional) Der Kunde registriert sich bei dem Anbieter und erhält Zugangsdaten. Mit diesen loggt er sich beim Anbieter ein, um den Service zu nutzen bzw. um weiteren Nutzern einen Zugang zu gewähren.
2. **Konfiguration:** Der Kunde konfiguriert die Parameter und Einschränkungen für die Aktionen (z.B. Bedingungen unter denen eine Lokalisierung erlaubt ist). Dies kann entweder lokal im Fahrzeug oder online beim Dienstanbieter geschehen.
3. **Lokalisierung:** Eine externe Person oder ein externes System initiiert eine Lokalisierung des Fahrzeuges. Die Position des Fahrzeugs wird unter Verwendung der im Fahrzeug vorhandenen Sensoren (z.B. GPS, Koppelnavigation) bestimmt. Optional kann auch eine geplante Navigationsroute berücksichtigt werden.
4. **Ausführen der Aktionen:** Die Bedingungen werden geprüft und die Aktion wird nach erfolgreicher Prüfung ausgeführt. Das Ergebnis der Aktion enthält neben möglichen weiteren Informationen aus dem Fahrzeug entweder direkt die Position des Fahrzeuges oder indirekt mit der Position zusammenhängende Aussagen wie z.B. ob sich das Fahrzeug in einem definierten Gebiet befindet.
   a) **Option:** Die Position des Fahrzeugs wird an die externe Person bzw. das externe System zusammen mit weiteren zuvor definierten Parametern übermittelt. Gegebenenfalls kann noch eine Vorverarbeitung bei einem Dienstanbieter stattfinden.
   b) **Option:** Die Position wird lokal im Fahrzeug verarbeitet und verlässt das Fahrzeug nur als indirekt mit der Position zusammenhängenden Aussage. In diesem Fall muss das Fahrzeug alle Informationen lokal vorhalten, die für Verarbeitung erforderlich sind.
   c) **Option:** Wie Option 2, nur noch zusätzlich mit der Möglichkeit einzelne Informationen online zu validieren oder zu aktualisieren.

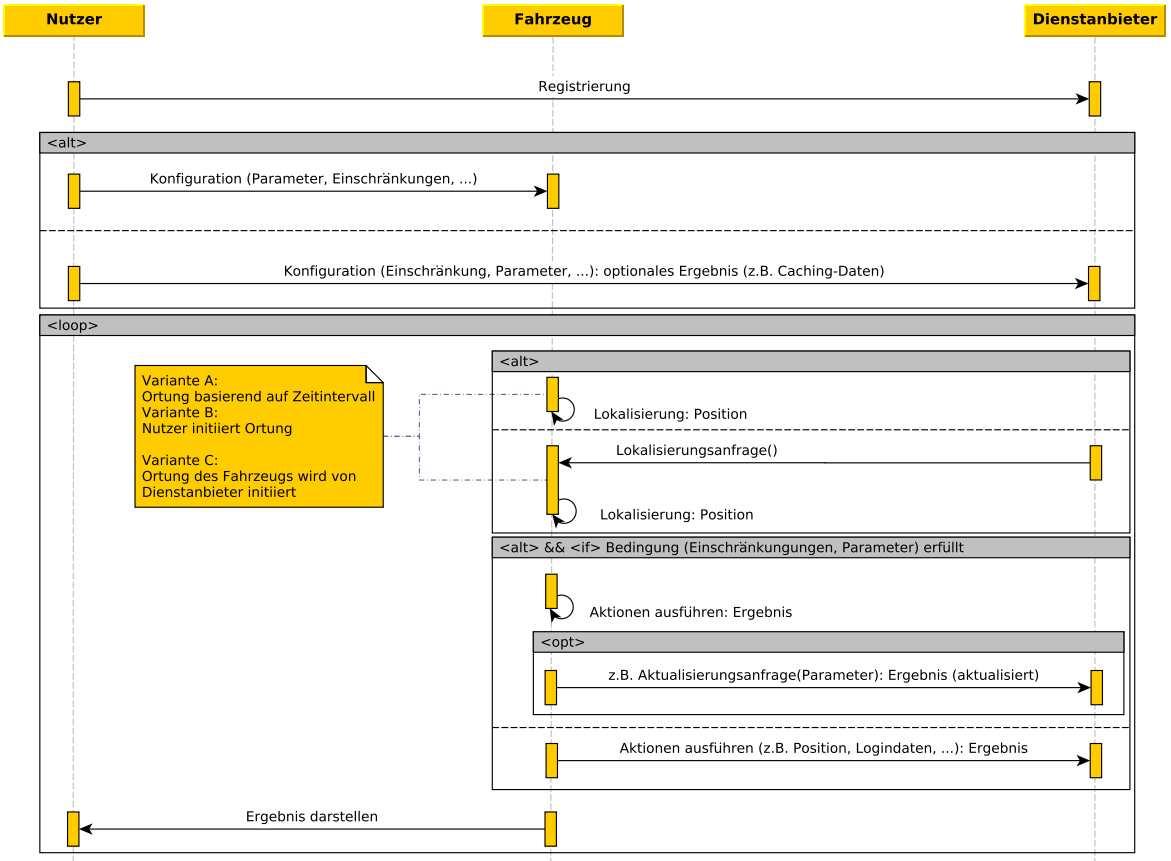
3.4.9. Datenfluss-basierte Beschreibung(C)

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Login	1. Beschränkung des Dienstes auf registrierte Kunde; 2. Online-Profil, in dem Einstellungen und Präferenzen verwaltet werden; 3. Verknüpfung mit weiteren Systemen	Identifizierende oder pseudonyme Daten, die eine Verknüpfung mit einem Profil erlauben	Infotainmentsystem / Nutzer-Endgerät → Anbieter Backend
Konfiguration	Verwalten von Parametern und Einschränkungen, sofern eine Vorabfilterung von Anfragen beim Diensteanbieter stattfindet	Vom Nutzer eingegebene Informationen	Infotainmentsystem / Nutzer-Endgerät → Anbieter Backend
Lokalisierung	Ortsinformationen als Parameter für die Aktionen	Fahrzeugposition	(Sensoren → Infotainmentsystem)
Ausführen der Aktionen	Notwendige Daten, um die festgelegten Aktionen ausführen zu können	Beispiele: Fahrzeugposition, Fahrzeugstatus, abstrahierte Aussage mit Positionsbezug	Sensoren / Infotainmentsystem → Anbieter Backend

3.4.10. Konkrete Beispiele (C)

Beispiel 1: Ein Kunde hat seinen volljährigen Kindern erlaubt sein Auto auszuleihen. Dabei möchte er überprüfen, ob sich das Fahrzeug innerhalb des erlaubten Gebietes aufhält. Die Antwort auf die Anfrage ist “Ja” oder “Nein”. **Beispiel 2:** Ein Heimautomatisierungssystem möchte wissen, ob es das Hoftor schließen kann. Dies ist nur vorgesehen, wenn sich das Fahrzeug des Nutzers auf dem Grundstück befindet und sich seit mindestens 10 Minuten nicht bewegt hat. Das System kontaktiert das Fahrzeug und erhält die Antwort ob die Parameter erfüllt sind. **Beispiel 3:** Der Kunde hat vergessen, wo er sein Fahrzeug geparkt hat. Er schickt per Smartphone eine Anfrage an das Fahrzeug und bekommt die Position mitgeteilt.

3.4.11. UML-basierte Beschreibung (ABC)



3.5. Android Auto

In diesem Anwendungsfall wird das Szenario der Nutzung von mobilen Endgeräten (i.d.R. Smartphone) im Fahrzeug mit Hilfe von dem Google-Produkt “Android Auto” betrachtet. Android Auto bildet die Schnittstelle zwischen einem mobile Android Gerät (im Folgenden “Mobile Device”) und dem Infotainmentsystem des PKWs.

Die Rechenleistung für die Apps verbleibt im Mobile Device, während die fürs Auto optimierte Anzeige in den integrierten Display des Fahrzeugs gespiegelt wird. Für Spracherkennung und Audiowiedergabe wird ebenfalls auf die Hardware des Fahrzeugs zugegriffen. Gleichzeitig nutzt Google im Fahrzeug gewonnen Informationen, wie z.B. GPS-Daten.

Die Verbindung kommt durch USB zustande. Für die Telefonie bzw. HFP wird zusätzlich eine Bluetooth-Verbindung benutzt. Alle anderen Funktionen wie die Übertragung von Bildern und Videos, Bedienereignisse, oder auch alle Audio-Daten wie beispielsweise das Mikrofon-Signal für Google Now fließen dagegen über das USB-Kabel.

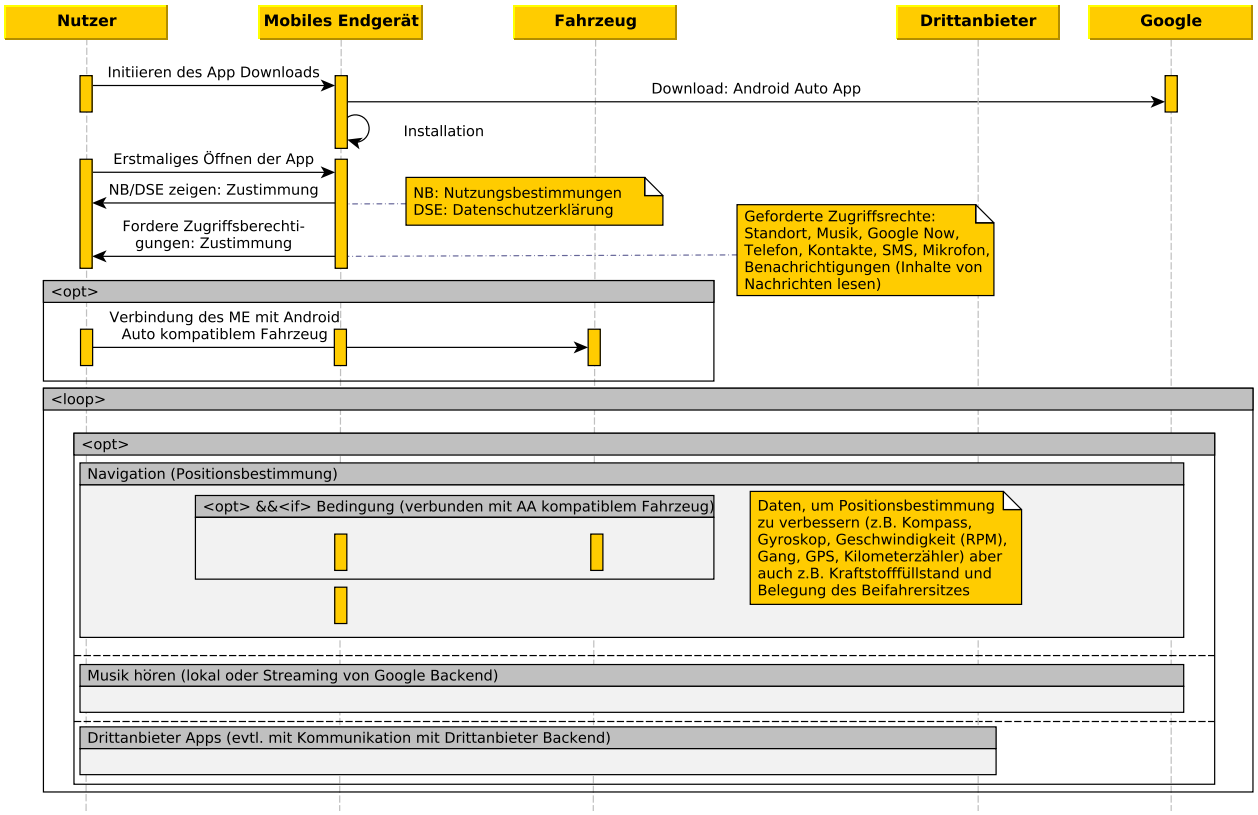
Aus Datenschutz-rechtlicher Sicht ist in diesem Anwendungsfall insbesondere die Bereitstellung von Fahrzeugdaten an das Mobile Device kritisch zu sehen, da die Daten in jedem Fall dem unvermeidbaren Google-Konto des Nutzer zugeordnet werden können. Weiterhin existieren nur wenige genaue Angabe, welche Daten wirklich vom Fahrzeug bereitgestellt werden und wie diese durch Google anschließend genutzt werden. Auch die Datenspeicherung im Fahrzeug ist nicht nachvollziehbar. Ob das Fahrzeug beispielsweise speichert, wie häufig Android Auto genutzt wurde oder welche Anwendungen genutzt wurden, ist unklar.

Der Anwendungsfall Android Auto enthält verschiedene Nutzungsszenarien.

3.5.1. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Registrierung Google: Um Google-Anwendungen, hier den Google Playstore und Android Auto nutzen zu können- wird ein Google-Konto benötigt	Kunde, Google	Einwilligung Google DSE	Vor- & Nachname, E-Mail, Geburtstag, Geschlecht, Standort (Land), Geräteinformationen
2. Download Android Auto: Der Kunde besucht den Google Playstore und lädt die Android Auto App.	Kunde, Mobile Device, Google	Zustimmung zu von der App geforderten Zugriffsrechten erforderlich	
3. Verbindung Mobile Device und Fahrzeug: Durch die USB-Schnittstelle des Fahrzeugs wird eine Verbindung mit dem Mobile Device hergestellt. Bluetooth wird eingeschaltet, damit Telefonie (HFP) unterstützt werden kann.	Kunde, Mobile Device, Fahrzeug, Google		
4. Nutzung von Android Auto: Mit der Nutzung von Android Auto werden im Fahrzeugdaten gewonnen an das Mobile Device bereitgestellt und stehen damit prinzipiell Google zur weiteren Nutzung zur Verfügung.	Kunde, Mobile Device, Fahrzeug, Google		GPS, Geschwindigkeit, ...

3.5.2. UML-basierte Beschreibung



3.5.3. Datenfluss-basierte Beschreibung

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Nutzung von Fahrzeugdaten	Die Fahrzeugdaten werden genutzt, um Funktionalitäten wie Navigation sicherzustellen bzw. zu optimieren. Der Nutzer sollte hierüber allerdings aufgeklärt sein. Dass die Fahrzeuggeschwindigkeit erfasst wird, erfährt der Nutzer allerdings erst nach langwieriger Auseinandersetzung mit den Zugriffsrechten der Anwendung, da sich diese Information hinter dem Zugriffsrecht “Standort” versteckt. Grundsätzlich sollte hier das Prinzip der Datensparsamkeit greifen, sodass nicht alle Daten ständig erfasst werden, sondern nur im konkreten Bedarfsfall. Insgesamt ist der Datenverkehr über Android Auto als intransparent zu bewerten. Inwiefern eine Zuordnung der Daten zum Google-Konto stattfindet, ist ebenfalls nicht transparent kommuniziert.	GPS, Fzg.-Geschwindigkeit,...	Fahrzeug → Mobile Device → Google Datenbank

3.6. Laden und Bezahlen

3.6.1. Abstrakte Beschreibung

In diesem Anwendungsfall wird das elektrische Laden eines Elektrofahrzeugs an einer Ladestation und der damit verbundene Bezahlvorgang beschrieben. Für den Datenschutz relevant sind dabei die Authentisierung und Autorisierung an der Ladestation sowie die anschließende Abrechnung der geladenen Energie.

Abgesehen von Prepaidlösungen (bspw. in Form einer Prepaid-RFID-Karte) oder Direktbezahlverfahren (z.B. via Kreditkarte oder Paypal) muss die geladene Energie einem Kunden für Abrechnungszwecke eindeutig zugeordnet werden können. Aufgrund der ohnehin hohen Kosten einer Ladestation scheidet ein Münzeinwurfautomat für anonymes Bezahlen aus und auch kein Ladestationshersteller führt eine solche Lösung im Sortiment. In diesem Anwendungsfall sind neben dem Kunden noch vornehmlich drei weitere Marktakteure beteiligt, die datenschutzrelevante Daten übertragen. Zu diesen gehören:

- der Ladestationsbetreiber (auch CPO für Charge Point Operator)
- der (Elektro-) Mobilitätsanbieter (auch EMP für E-Mobility Provider bzw. EMSP für E-Mobility Service Provider)
- die Clearingstelle als B2B-Plattformbetreiber für gebündelte Roamingverträge zwischen CPOs und EMPs (auch CH für Clearinghaus)

Im Allgemeinen autorisiert sich der Kunde an der Ladestation mittels eines geeigneten Mediums (RFID-Karte, Smartphone-App, direkte Kommunikation über das Ladekabel (ISO 15118, Plug&Charge)), welche die Autorisierungsanfrage an das Backend des Ladestationbetreibers (CPOs) weiterleitet. Der CPO muss dann - falls keine Prepaid- oder Direktbezahllösung via Kreditkarte bzw. Paypal gewählt wird - die Freischaltungsanfrage für diesen Ladevorgang an das Backend des Energielieferanten, mit welchem der Kunde zuvor einen Vertrag abgeschlossen hat (EMP), weiterleiten. Dies kann entweder in direkter Kommunikation mit dem EMP oder über eine Clearingstelle (CH) abgewickelt werden, die als gemeinsame Schnittstelle zwischen CPOs und EMPs agiert. Für eine erfolgreiche Autorisierung muss es einen gültigen Vertrag für Abrechnungszwecke zwischen EMP des Kunden und dem CPO sowie ein ebenfalls gültiges Vertragsverhältnis zwischen EMP und Kunden geben, ansonsten wird die Autorisierungsanfrage bei vertragsbasierten Verfahren abgelehnt.

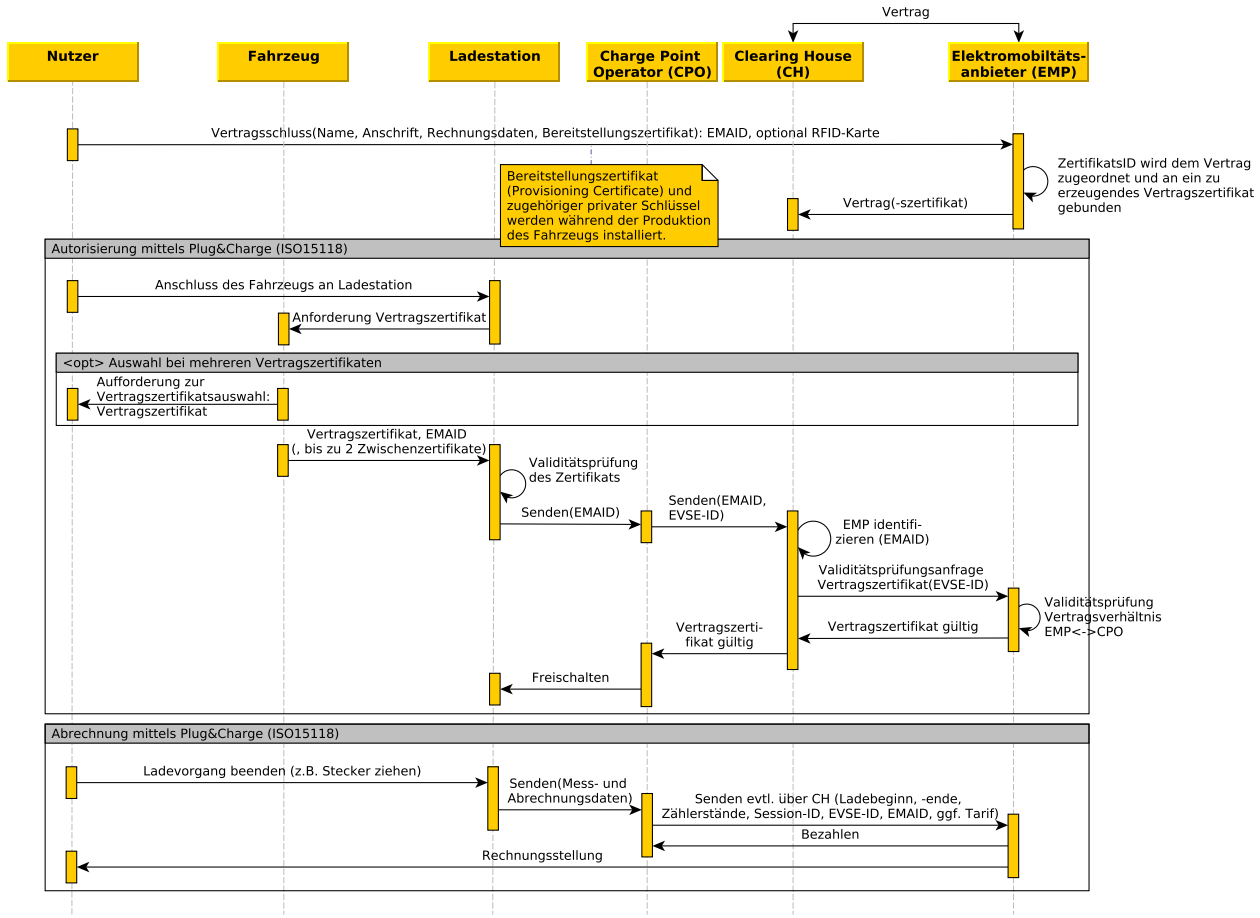
Derzeit laufen vertragsbasierte Verfahren über eine sogenannte externe Autorisierung durch den Kunden mittels RFID-Karte bzw. Smartphone-Applikation an der Ladestation ab. Das Kommunikationsprotokoll ISO 15118 ermöglicht hingegen das komfortable Laden des Elektrofahrzeugs inklusive Abrechnung ohne die Interaktion des Fahrers mit der Ladestation und stellt somit den zukünftigen Trend diesen Anwendungsfall betreffend dar. Hierfür wird auf eine Public-Key-Infrastruktur mit digitalen Zertifikaten gesetzt, in welche die oben aufgeführten Akteure eingebunden sein müssen.

Aus datenschutzrechtlicher Sicht sind in diesem Anwendungsfall sowohl die Vertrags-ID bzw. Authentisierungs-ID des Kunden (auch EMAID für E-Mobility Account Identifier bzw. E-Mobility Authentication Identifier) als auch die Ladestations-ID (auch EVSE-ID für Electric Vehicle Supply Equipment Identifier), die mit dem Standort verknüpft ist, relevante Daten, welche die Erstellung eines Bewegungsprofils ermöglichen.

3.6.2. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz
1. Nutzer schließt einen Vertrag mit einem EMP ab	Kunde, EMP, CH	Details siehe PDF-Dokument	Name, Anschrift und Rechnungsdaten des Kunden; EMAID vergeben durch EMP
2. Nutzer autorisiert sich an der Ladestation mittels Vertrag durch externe Identifikation	Kunde, Ladestation, CPO, EMP, CH	Details siehe PDF-Dokument	EMAID im Falle von RFID Mifare Desfire EV1; UUID der RFID-Karte im Falle von RFID Mifare Classic; Standortabhängige EVSE-ID des vom Kunden ausgewählten Ladepunkts
3. Nutzer autorisiert sich an der Ladestation mittels adhoc-Bezahlverfahren	Kunde, Bezahldienstleister (z.B. VISA, MasterCard, American-Express, PayPal), CPO, Ladestation	Details siehe PDF-Dokument	Kreditkartendaten oder Paypal-Accountdaten des Kunden; Standortabhängige EVSE-ID des vom Kunden ausgewählten Ladepunkts
4. Nutzer autorisiert sich an der Ladestation mittels Prepaid-Karte	Kunde, CPO, EMP, Ladestation	Details siehe PDF-Dokument	Anschlussdauer, Kosten für Ladevorgang, verbleibendes Restguthaben
5. Nutzer autorisiert sich an der Ladestation mittels Vertrag durch Plug&Charge-Identifikation über ISO 15118	E-Fahrzeug, Ladestation, CPO, EMP, CH	Details siehe PDF-Dokument	Digitales Vertragszertifikat; Digitale Sub-CA Zertifikate (zur Überprüfung der Signaturkette von Blattzertifikat – also Vertragszertifikat – bis hin zu einem Wurzelzertifikat); EMAID des im Fahrzeug gespeicherten Ladevertrags; EVSE-ID des gewählten Ladepunkts
6. Vertragszertifikat wird in das E-Fahrzeug installiert	E-Fahrzeug, Ladestation, CPO, EMP, CH	Details siehe PDF-Dokument	Digitales Vertragszertifikat; Digitale Sub-CA Zertifikate (zur Überprüfung der Signaturkette von Blattzertifikat – also Vertragszertifikat – bis hin zu einem Wurzelzertifikat); Digitales Bereitstellungszertifikat des E-Fahrzeugs; Privater verschlüsselter Schlüssel des Vertragszertifikats
7. Im E-Fahrzeug gespeichertes Vertragszertifikat wird aktualisiert	E-Fahrzeug, Ladestation, CPO, EMP, CH	Details siehe PDF-Dokument	Digitales Vertragszertifikat; Digitale Sub-CA Zertifikate (zur Überprüfung der Signaturkette von Blattzertifikat – also Vertragszertifikat – bis hin zu einem Wurzelzertifikat); Privater verschlüsselter Schlüssel des Vertragszertifikats
8. Nutzer beendet den Ladevorgang, Messdaten für Abrechnung werden erhoben	Kunde, CPO, EMP, CH, Ladestation	Details siehe PDF-Dokument	Messwerte des Smart-Meters der Ladestation: Start und Ende des Ladevorgangs, geladene Energie, ggf. Zählerstand des Smart-Meters zu Beginn und zum Ende des Ladevorgangs; EVSE-ID des vom Kunden gewählten Ladepunkts; EMAID oder UUID der RFID-Karte; Transaktionsnummer der Ladesession (Session-ID); EMP-ID (auch Provider-ID genannt, siehe Definition der EMAID)

3.6.3. UML-basierte Beschreibung



3.6.4. Datenfluss-basierte Beschreibung

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Vertragsabschluss	Kunde benötigt ein gültiges Vertragsverhältnis mit EMP, um tanken zu können. Der EMP wiederum braucht einen Vertrag mit CPO und evtl. CH, um Abrechnungsdaten von den Ladesäulen weitergeleitet zu bekommen.	Name, Anschrift und Rechnungsdaten des Kunden, EMAID, OEM Provisioning Certificate im Fall von Plug&Charge	Kunde → EMP, EMP → CPO (, EMP → CH)
Autorisierung durch externe Identifikation	Nutzer will E-Fahrzeug laden und muss ein gültiges Vertragsverhältnis mit EMP nachweisen. Für Abrechnungszwecke ist der mit der EVSE-ID verknüpfte Standort bisher ein notwendiges Datum.	EMAID (Vertrags-ID), EVSE-ID (Ladestations-ID), UUID (Mifare Classic)	(Fahrzeug →) Ladestation → CPO (→ CH) → EMP bzw. Smartphone (→ CH oder CPO) → EMP bzw. RFID-Karte → Ladestation → CPO (→ CH) → EMP
Autorisierung Adhoc	Nutzer will E-Fahrzeug laden und bezahlt mittels adhoc-Bezahlverfahren (Kreditkarte, Paypal)	Bezahldaten (Kreditkarte, Paypal), EVSE-ID	(Smartphone oder HMI der Ladestation → CPO) → Backend Bezahldienstleister (Auswahl- und Bezahlprozess) → CPO (Freischaltung des Ladepunkts)
Autorisierung Prepaid	Nutzer will E-Fahrzeug laden und bezahlt mittels Prepaid Karte	Kosten, Restguthaben	Keine, falls Guthaben kryptographisch gesichert auf Karte oder Ladestation → CPO (→ CH) → EMP falls Online Verwaltung des Guthabens erforderlich
Autorisierung Plug&Charge	Der Abrechnungsvorgang erfolgt automatisch über das Ladekabel mittels des im Fahrzeug hinterlegten und mit der EMAID verknüpften OEM Provisioning Certificates	Provisioning Certificate, Sub-CA Zertifikate, EMAID, EVSE-ID	Fahrzeug → Ladestation → CPO (→ CH) → EMP bzw. Fahrzeug → Ladestation → OCSP-Responder → Ladestation

3.7. Paketauto

In diesem Anwendungsfall wird ein Szenario betrachtet, in welchem externen Paketzustelldiensten die Erlaubnis erteilt wird, Pakete in den Kofferraum eines Fahrzeuges zuzustellen. Beispielhaft kann sich ein Kunde seine nächste Katalogbestellung während seiner Arbeitszeit in sein auf dem Firmenparkplatz stehendes Fahrzeug zustellen lassen.

Hierfür ist sowohl eine Planungs- als auch eine Betriebsphase zu betrachten. In der Planungsphase legt der Kunde am Ende der Bestellung fest, wann und wo er sein Fahrzeug über einen längeren Zeitraum abstellen wird. Dies kann entweder direkt eingegeben oder aus dem digitalen Kalender des Kunden ausgelesen werden. Auf Basis dieser Information kann der betroffene Paketzustelldienst die Routen der eigenen Zusteller planen.

In der Betriebsphase nähert sich der Paketbote der geplanten Position des Fahrzeuges und erfragt über ein Mobilteil mit Internetanbindung den exakten Parkplatz. Sobald er am gewünschten Fahrzeug angekommen ist, fragt er über sein Mobilteil die Öffnung des Kofferraumes des Fahrzeuges an. Der Kofferraum wird entriegelt, das Paket wird eingelegt und der Paketbote verschließt das Fahrzeug. Somit ist die Auslieferung abgeschlossen.

Während der Betriebsphase kann der Kunde sich auf seinem Smartphone über den aktuellen Stand der Auslieferung

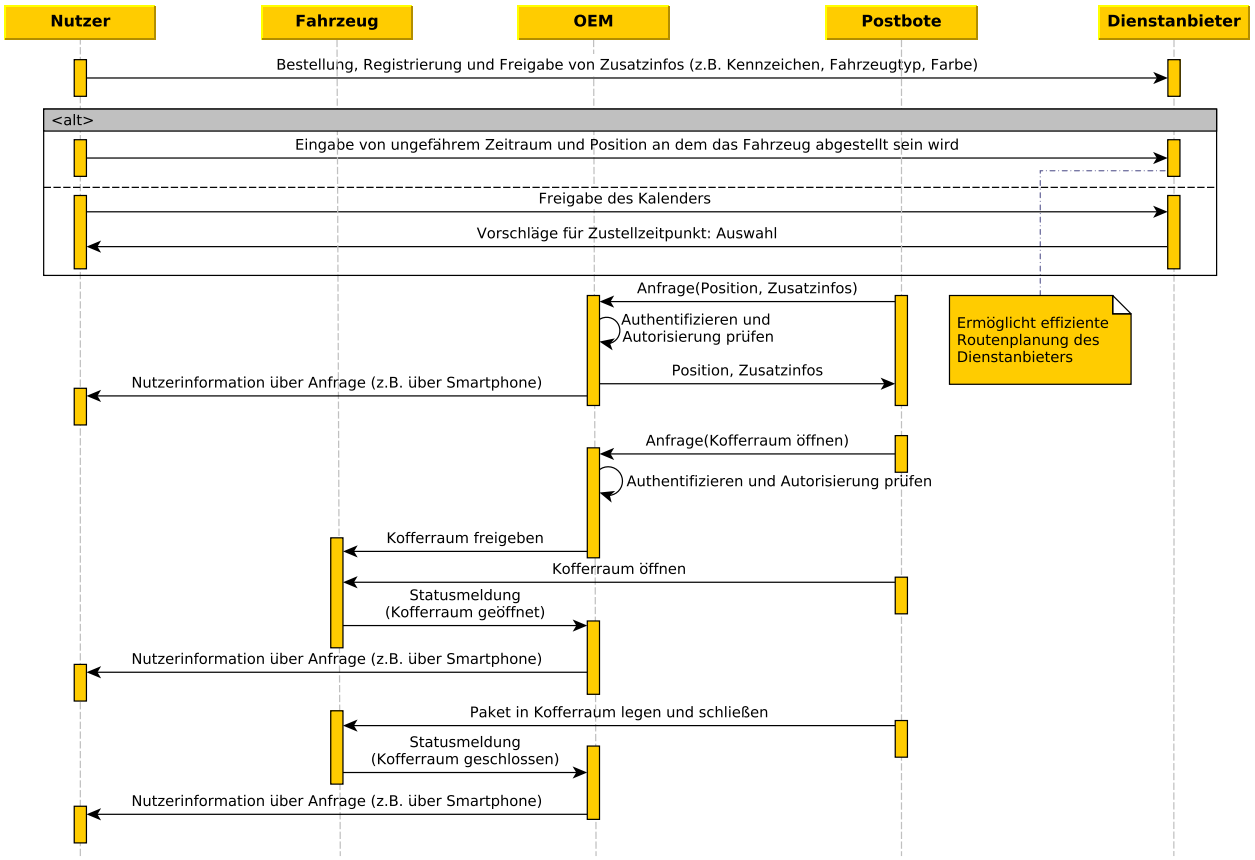
informieren lassen. Sowohl die Lokalisierung und die Öffnung als auch die abschließende Verriegelung des Fahrzeuges werden ihm jeweils mitgeteilt, um ihn über den Zustand seines Fahrzeuges zu informieren.

3.7.1. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Bestellung und Freigabe: Der Kunde bestellt seine Ware und registriert sich im Anschluss mit bei dem Paketzustelldienst. Er wird hierzu auf die Internetseite des Paketzustelldienstes weitergeleitet, um die Zulieferung zu planen.	Kunde, Internetshop, Paketzustelldienst	Keine Interaktion mit dem Fahrzeug	—
2.1. Eingabe des Zeitraums und der Position: Der Kunde legt auf der Seite des Paketzustelldienstes fest wann und wo er sein Fahrzeug über einen längeren Zeitraum abstellen wird.	Kunde, Paketzustelldienst	Keine Interaktion mit dem Fahrzeug	—
2.2. Freigabe des Kalenders: Der Kunde erlaubt dem Paketzustelldienst den Zugriff auf seinen persönlichen digitalen Kalender. Der Paketzustelldienst kann Vorschläge für einen Zustellzeitpunkt machen.	Kunde, Paketzustelldienst	Keine Interaktion mit dem Fahrzeug	privater Kalender des Kunden
3. Beginn der Zulieferung: Der Paketbote erfragt über ein Mobilteil die aktuelle Position des Fahrzeuges. Zusätzlich werden ihm weitere Informationen angezeigt, um das Fahrzeug besser finden zu können (z.B. Kennzeichen, Farbe, Hersteller, Modell). Das Recht zu diesem Abruf hat er in *Bestellung und Freigabe* erteilt. Der Kunde wird auf seinem Smartphone über diesen Abruf informiert.	Paketbote, OEM-Server, Fahrzeug(, Kunde)	Das Fahrzeug muss hierfür Mobilfunkempfang zum Zeitpunkt der Abfrage haben. Der Abruf erfolgt über den OEM-Server. Das Mobilteil spricht nicht direkt mit dem Fahrzeug.	Position und Zustand (abgestellt und verschlossen) des Fahrzeuges, identifizierende Merkmale des Fahrzeuges (z.B. Kennzeichen, Farbe, Hersteller, Modell)

4. Zugriff auf das Fahrzeug: Der Paketbote nähert sich auf wenige Meter dem Fahrzeug. Er fragt über sein Mobilteil die Öffnung des Kofferraumes an. Der OEM-Server überprüft die Rechte und die Position des Paketboten und gibt bei erfolgreicher Prüfung den Kofferraum frei. Das Fahrzeug meldet an das OEM-Backend das Öffnen des Schlosses des Kofferraumes. Der Kunde wird auf seinem Smartphone über diesen Schritt informiert.	Paketbote, Fahrzeug, OEM-Server(, Kunde)	s. *Beginn der Zulieferung*	Zustand des Fahrzeuges (Schließstatus des Kofferraumes)
5. Zustellung: Der Paketbote öffnet den Kofferraum, legt das Paket hinein und verschließt den Kofferraum wieder. Das Fahrzeug meldet das Verschließen des Kofferraumes an das OEM-Backend. Der Kunde wird auf seinem Smartphone über diesen Schritt informiert.	Paketbote, Fahrzeug, OEM-Server(, Kunde)	s. *Beginn der Zulieferung*	Zustand des Fahrzeuges (Schließstatus des Kofferraumes)

3.7.2. UML-basierte Beschreibung



3.7.3. Datenfluss-basierte Beschreibung

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Kalenderzugriff	Für die Planung der Zustellung muss ein Zeitraum für die Zulieferung bekannt sein. Der Kunde kann hierzu dem Paketzustelldienst Zugriff auf den privaten Kalender gewähren. Dieser Kalender könnte auch auf dem OEM-Server liegen.	persönlicher Kalender des Kunden	Smartphone/Tablet/PC → Paketzustelldienst; Server des Kalenderbetreibers → Paketzustelldienst
Lokalisierung	Der Paketbote muss über die Position des Fahrzeuges informiert sein. Allerdings sollte dies nicht möglich sein, wenn das Fahrzeug gerade benutzt wird oder wenn die Abfrage außerhalb des geplanten Zeitraums erfolgt.	Fahrzeugposition	Telemetrik-Einheit → (OEM-Backend →) Paketbote und Benachrichtigung an Smartphone des Kunden
Fahrzeugstatus	Der Zustand des Fahrzeuges muss abrufbar sein, damit der Zustellprozess eingeleitet und beobachtet werden kann. Eine Bestätigung über eine erfolgreiche Öffnung und eine zusätzliche Bestätigung über das Wiederverschließen geht an das Smartphone des Kunden.	Zustand des Fahrzeuges (geparkt/fahrend, verschlossen/geöffnet)	Telemetrik-Einheit → (OEM-Backend →) Paketbote und Benachrichtigung an Smartphone des Kunden
Kofferraum öffnen	Der Befehl den Kofferraum einmalig freizugeben wird an das Fahrzeug gesendet. Beim nächsten Verschließen wird das Schloss wieder verriegelt.	Befehl zur Freigabe des Kofferraums	Paketbote (→ OEM-Backend) → Telemetrik-Einheit

3.8. Statistische Analyse der Umgebung (Parkdienst)

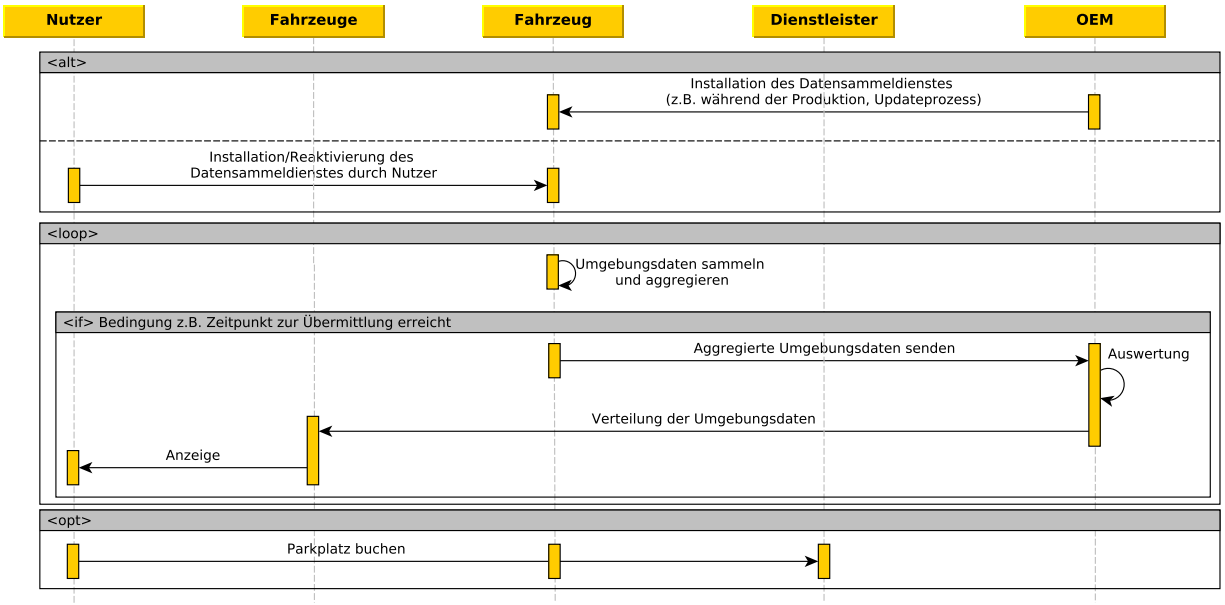
In diesem Szenario wird sich die Umgebungswahrnehmung des Fahrzeugs zu Nutze gemacht. Unterhalb einer gewissen Geschwindigkeit (z.B. 50km/h) aktivieren sich die Parkdistanzsensoren des Fahrzeugs und erfassen die Abstände des Fahrzeugs zu seiner Umgebung. Mit einer Erkennungslogik werden so Parkplätze am Rand der Straße erkannt und an ein Backend-System übermittelt. Das Backend-System sammelt diese Daten und stellt sie anderen Fahrzeugen zum Download bereit. Auf diese Weise können in der Navigationseinheit/Head-Unit des Fahrzeugs Parkplatzwahrscheinlichkeiten oder existierende Parkplätze angezeigt werden. Bei einer statistischen Auswertung kann so auch die Wahrscheinlichkeit für einen Parkplatz zu einer bestimmten Zeit an einem bestimmten Ort berechnet und angezeigt werden.

3.8.1. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Installation des Datensammelauftrags: Das Fahrzeug erhält den Auftrag die Parkplätze in seiner Umgebung zu erfassen und diese Daten an das Backend zu senden.	Fahrzeug, OEM	Dies kann bereits während der Produktion geschehen oder nachträglich bei einem spezifischen Anlass ausgelöst werden. Verschiedene Anlässe wären: Es wurde ein Bedarf an Daten in einer bisher nicht analysierten Region festgestellt, der Kunde installiert sich den gleichnamigen Dienst um den Dienst zu nutzen, der Dienst wird neu vom OEM ausgerollt, der Dienst wurde nach voriger Deaktivierung wieder aktiviert, ...	Datensammelauftrag

2. Fahrzeug sammelt Daten: Das Fahrzeug fährt durch die Gegend und analysiert ständig die Umgebung. Gefundene Parkplätze werden in einem Zwischenspeicher aggregiert.	Fahrzeug	Eine ständige Übermittlung in das OEM-Backend ist zu aufwändig, daher muss eine Aggregation im Fahrzeug erfolgen.	Gefundene Parkplätze auf zurückgelegten Strecken
3. Übermittlung an den Hersteller: Die aggregierten Umweltdaten werden an den Hersteller zur Auswertung übermittelt.	Fahrzeug, OEM-Backend	Die genaue Ausprägung der Daten ist ungewiss. Es können spezifische Parkplätze übermittelt werden oder nur die Anzahl gefundener Parkplätze je Streckenabschnitt. Der Typ des Parkplatzes kann auch eine optionale Detaillierung sein.	Erfasste Parkplatzdaten
4. Auswertung im OEM-Backend: Die übermittelten Daten werden im Backend verarbeitet und zusätzliche Informationen werden extrahiert/erzeugt.	OEM-Backend	Hier kann auch eine Verringerung des Informationsgehalts erfolgen um die Handhabbarkeit zu erhöhen.	Erfasste und verarbeitete Parkplatzdaten
5. Verteilung der Parkplatzdaten an Andere: Die im Backend hinterlegten Daten werden an andere Fahrzeuge zur Anzeige übermittelt. Die Abfrage erfolgt hierbei auf Basis von anzuzeigenden Kartenausschnitten.	OEM-Backend, andere Fahrzeuge	Form und Inhalt der Daten ist weiterhin ungewiss.	Verarbeitete Parkplatzdaten
6. Nutzung des Dienstes: Die Fahrer der anderen Fahrzeuge nutzen die übermittelten Daten um leichter einen Parkplatz zu finden.	andere Fahrzeuge, andere Nutzer	—	Verarbeitete Parkplatzdaten

3.8.2. UML-basierte Beschreibung



3.8.3. Datenfluss-basierte Beschreibung

Use Case	Beschreibung	Betroffene Daten	Datenfluss
Datensammelauftrag installieren	Der Auftrag die spezifischen Daten zu sammeln und zu senden wird im Fahrzeug installiert.	Datensammelauftrag	OEM → Telemetrik-Einheit
Gesammelte Daten hochladen	Die im Laufe der Zeit gesammelten Daten über gefundene Parkplätze werden in das Backend übertragen.	erfasste Parkplatzdaten	Telemetrik-Einheit → OEM-Backend
Parkplatzdaten herunterladen	Die im Backend aggregierten und verarbeiteten Daten werden von anderen Fahrzeugen heruntergeladen und zur Anzeige verwendet.	verarbeitete Parkplatzdaten	OEM-Backend → andere Fahrzeuge
Parkplatzbuchung	Ein Fahrer bucht einen Parkplatz für eine spätere Nutzung.	Parkplatzbuchungsdaten, Bezahlinformationen	Fahrzeug → OEM-Backend → Parkplatzdienstleister

3.9. Verschleißanalysen OEM/Zulieferer

Bei der Verschleißanalyse werden Daten über Fahrzeugkomponenten wie Motor, Batterie, Steuergeräte, etc. gesammelt und ausgewertet. Der Zweck kann dabei von Produktanpassungen in Nachfolgemodellen über marketingrelevante Analysen (z.B. “Wie oft wird in einem Sportwagen die Sport-Fahrwerkseinstellung verwendet?”) bis hin zur Abschätzung über den Bedarf einer Rückrufaktion variieren. In der Regel spielt es keine Rolle, welches Fahrzeug genau die Daten liefert, sofern die nötigen Metadaten (z.B. das Fahrzeugmodell und das Baujahr) bekannt sind. Für langfristige Analysen eines Sachverhaltes kann es auch nötig sein, mehrere Datensätze einer Komponente miteinander zu verknüpfen.

Eine statistische Verschleißanalyse wird in der Regel von OEMs oder Zulieferern durchgeführt.

3.9.1. Textuelle Beschreibung

1. **Konfiguration:** Der OEM oder Zulieferer konfiguriert das Fahrzeug bzw. die relevanten Komponenten so, dass die gewünschten Daten erhoben werden können. Weitere Einstellungen betreffen die Verarbeitung und Übertragung der Daten. Eine nachträgliche Anpassung und Erweiterung der Konfiguration ist möglich.
2. **Erhebung der Daten:** Die Erhebung der Daten kann entweder regelmäßig erfolgen oder wenn definierte Rahmenbedingungen (inklusive gezielter Abfragen) erfüllt sind.
3. **Sammlung und Verarbeitung der Daten:** Die Daten werden von Steuergeräten mit ausreichender Rechenleistung zusammengetragen. Je nach Einstellung werden die Daten entweder unverarbeitet gesammelt, oder lokal verarbeitet und die Ergebnisse gespeichert.
4. **Übertragung der Daten:** Die Daten werden an den OEM oder Zulieferer übertragen.
5. **Auswertung der Daten:** Die Daten werden entweder selektiv oder im "Big-Data"-Stil analysiert.

3.9.2. Datenfluss-basierte Beschreibung

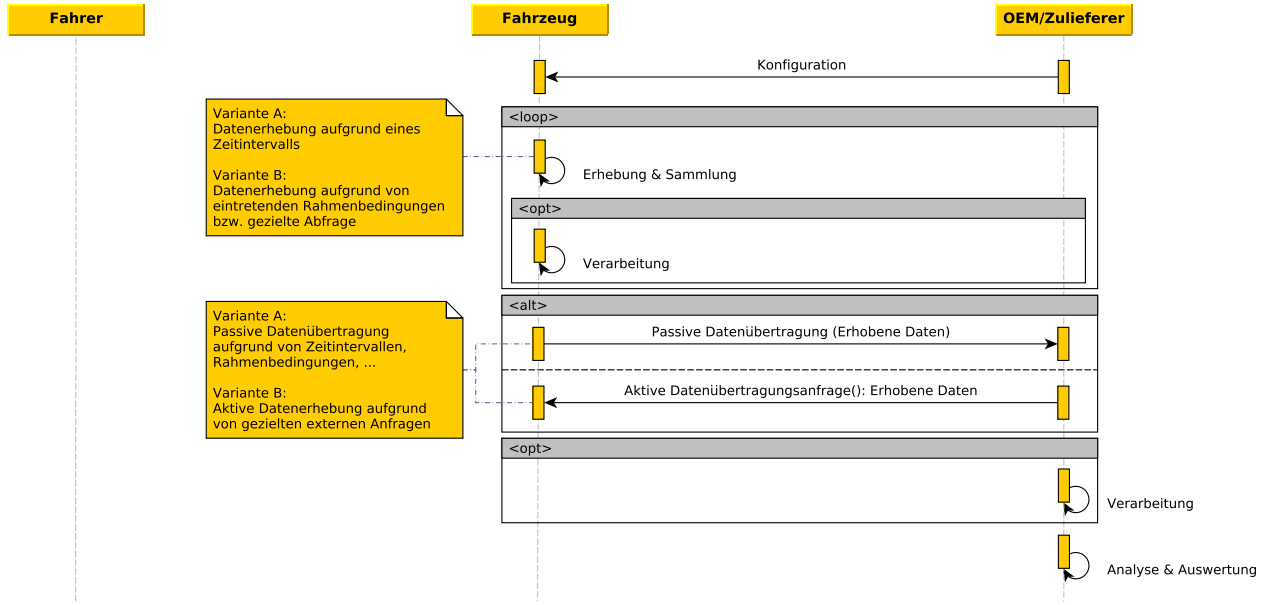
Use Case	Beschreibung	Betroffene Daten	Datenfluss
Sammung und Verarbeitung der Daten	Vorbereitung für die Verarbeitung und Übermittlung	Diverse Daten von Sensoren und Steuergeräten im Fahrzeug	(Infotainmentsystem / Sensoren / Steuergeräte → Zentrale Steuergeräte / Infotainmentsystem)
Übertragung der Daten	Statistische Analysen, Produktoptimierung	Diverse Daten von Sensoren und Steuergeräten im Fahrzeug	Infotainmentsystem / Zentrale Steuergeräte → Anbieter Backend

3.9.3. Konkrete Beispiele

Beispiel 1: Ein Batteriezulieferer eines Elektrofahrzeuges möchte das Produkt verbessern und benötigt dafür Daten aus der realen Nutzung. Der OEM erhebt für den Zulieferer die Daten der Batteriesteuergeräte und leitet diese an ihn weiter. Die Daten werden sowohl regelmäßig erhoben als auch separat zusätzlich unter besonderen Witterungsbedingungen.

Beispiel 2: Bei einem Bauteil hat ein OEM von den Werkstätten die Rückmeldung erhalten, dass es unerwartet oft ausgetauscht werden muss. Da dieses Bauteil mit einer Safety-Funktion verknüpft ist, möchte der Hersteller wissen, welche Modelle und wie viele Fahrzeuge wahrscheinlich betroffen sind und ob es dabei Wechselwirkungen mit anderen Bauteilen gibt. Die mit den Bauteilen zusammenhängenden Sensoren sollen nun für einen Zeitraum von einem Monat regelmäßig Daten sammeln, so dass über Konsequenzen entschieden werden kann. Um Umweltfaktoren ebenfalls berücksichtigen zu können, sollen auch die Daten des Regensensors und des Temperatursensors übermittelt werden.

3.9.4. UML-basierte Darstellung



3.10. Fahrverhalten

In diesem Anwendungsfall wird das Fahrverhalten eines Fahrers überwacht, um ihm Rückmeldung über sein Fahrverhalten zu geben. Dies wird unter anderem von o2 mit dem Produkt “Connected Drive” Angeboten. Hier soll der Nutzer sich auch mit anderen Nutzern vergleichen können und zusätzlich seinen Benzinverbrauch reduzieren.

Weiterhin erfolgt eine Überwachung in verschiedener Form bei den sogenannten “Pay-As-You-Drive”-Versicherungsverträgen. Es wird hierbei entweder ein OBD-Adapter verbaut der Fahrzeugdaten an die Versicherung überträgt (z.B. “AppDrive” von Signal Iduna oder über eine Black Box (z.B. Sparkassen Versicherung) erhoben, die direkt in das Fahrzeugnetz verbaut wird. In diesem Use Case wird aufgrund der aktuellen Relevanz Pay-As-You-Drive näher betrachtet, wobei andere Fahrerüberwachungsdaten äquivalent zu betrachten sind.

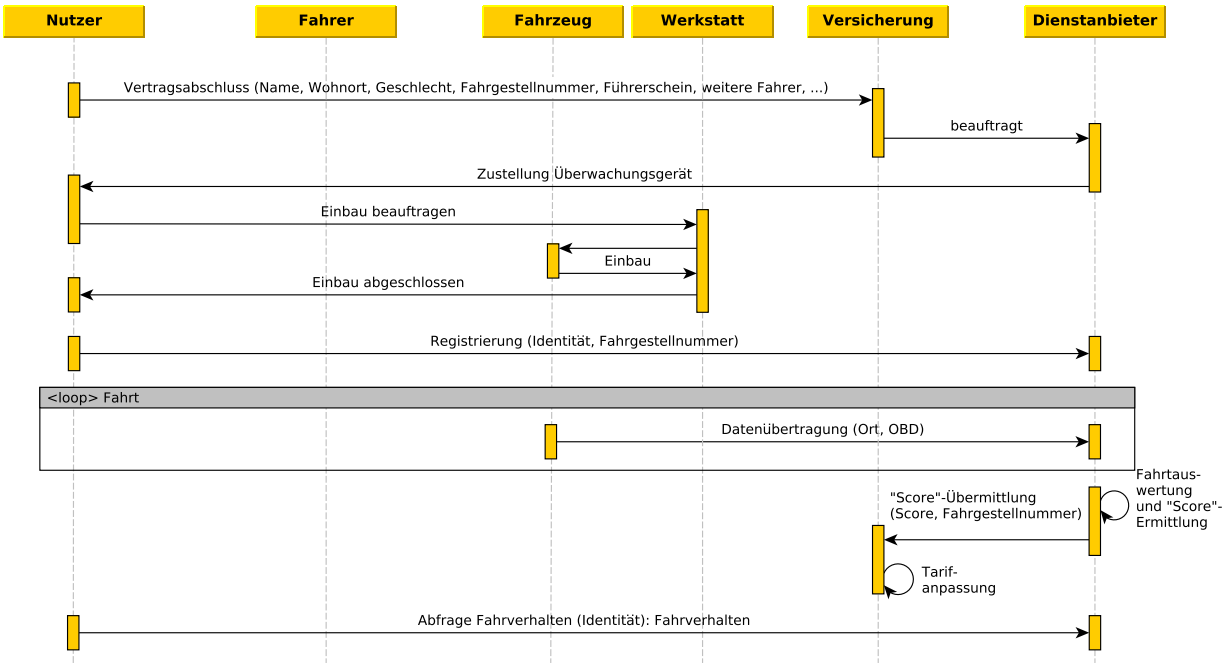
3.10.1. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Vertragsabschluss: Autobesitzer schließt einen “Pay-As-You-Drive”-Versicherungsvertrag ab.	Fahrzeughalter, Versicherung		Vor- & Nachname, Wohnort, Geburtstag, Geschlecht, Fahrgestellnummer, Führerschein, Informationen über weitere Fahrer
2. Integration: Der Kunde erhält ein Überwachungsgerät vom Anbieter.	Fahrzeughalter, Dienstanbieter, (Versicherung), (Werkstatt)	Das Überwachungsgerät kann sowohl eine Blackbox oder ein OBD-Adapter sein. Der Einbau kann auch durch eine Werkstatt erfolgen. Das Überwachungsgerät muss nicht von der Versicherung stammen.	Anschrift des Kunden
3. Registrierung: Kunde registriert sein Auto auf der Seite des Anbieters.	Fahrzeughalter, Dienstanbieter, (Versicherung)		Identität des Fahrers
4. Fahrt: Ein Fahrer fährt mit dem Auto.	Fahrer, Überwachungsgerät		z.B. OBD-Daten, Ort
5. Score: Auswertung der Fahrdaten und Erstellung und Errechnung eines Score-Wertes.	Überwachungsgerät, Dienstanbieter, (Versicherung)		OBD-Daten, Ort, Score Wert
6. Score-Weitergabe: Der Score wird an die Versicherung weitergegeben um den Versicherungstarif anzupassen.			Score
7. Information: Kunde informiert sich über seinen Score und Verhalten auf der Straße.	Fahrzeughalter, Dienstanbieter		Fahrtdaten (inklusive Geschwindigkeit und Position)

OBD-Daten

Hierzu gehören unter anderem Füllstand, Geschwindigkeit, Motorumdrehungen, Brems- und Gaspedalstellung, Motortemperatur, Fehlerspeicher und Abgaswerte.

3.10.2. UML-basierte Beschreibung



3.10.3. Datenfluss-basierte Beschreibung

Use Case	Grund	Betroffene Daten	Datenfluss
Kunde registriert sein Auto auf der Seite des Anbieters.	Vertragsabschluss	Identität des Fahrzeughalters, VIN des Fahrzeugs	Fahrzeughalter zum Dienstanbieter
Ein Fahrer fährt mit dem Auto.	Datenübertragung von Daten aus dem Fahrzeugnetz	OBD-Daten, Zeit, u.U. GPS	Fahrzeug zum Dienstanbieter
Der Score wird an die Versicherung weitergegeben, um den Versicherungstarif anzupassen.	Übermittlung des Score-Wertes	Score, Fahrzeughalter	Dienstleister zu Fahrzeughalter

3.11. Fahrerüberwachung

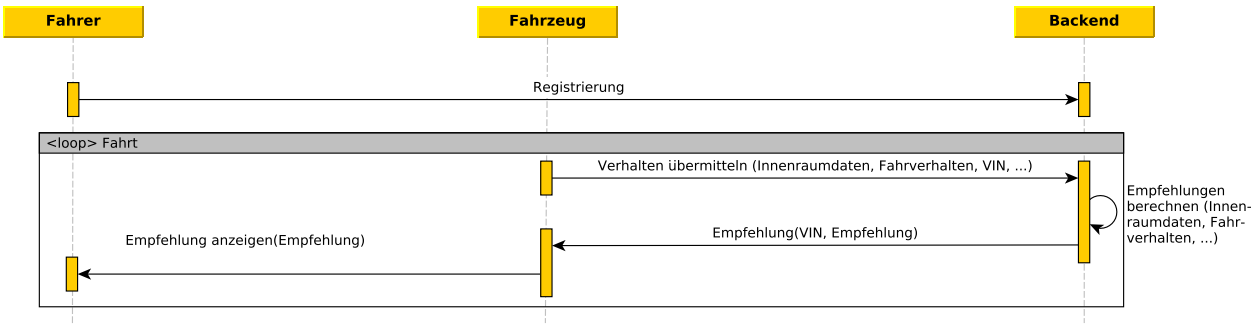
In diesem Anwendungsfall wird der Fahrer durch geeignete Sensoren im Fahrzeug überwacht. Zu diesen Sensoren zählen Sensoren zur Müdigkeitserkennung, Innenraumkameras, Luftanalyse (Diabetes, Alkohol, etc.).

Erhobene Daten werden entweder im Fahrzeug ausgewertet und gespeichert oder auf einem Server ausgewertet.

3.11.1. Textuelle Beschreibung

Beschreibung	Beteiligte Entitäten	Bemerkung	Relevante Daten für den Selbstdatenschutz im Fahrzeug
1. Datenaufnahme: Aufnahme von Daten aus dem Fahrerraum	Fahrzeug, Fahrer		Augenbewegungen, Lenkradwinkel, Luftzusammensetzung, Innenraumbild
2.1. (Optional) Datenübertragung: Übertragung von Daten an einen Server	Fahrzeug, Server	Optionale Datenweitergabe	Augenbewegungen, Lenkradwinkel, Luftzusammensetzung, Innenraumbild, VIN
2.2. Auswertung: Daten werden ausgewertet.	Server oder Fahrzeug	Je nachdem wo die Auswertung ausgeführt wird.	Rückschlüsse auf den Fahrer (z.B. Müdigkeit)
3. Rückspiegelung: Auswertung wird vom Fahrzeug zur Verfügung gestellt.	Fahrzeug		Alkoholerkennung, Müdigkeitsanzeige, Diabeteswarnung, etc.
4. Reaktion: Fahrzeug reagiert, in dem es dem Fahrer eine mögliche Verhaltensweise empfiehlt.	Fahrzeug, Fahrer	Hier sind verschiedene Reaktionen möglich.	Daten zum Zustand des Fahrers (s.o.)

3.11.2. UML-basierte Beschreibung



3.11.3. Datenfluss-basierte Beschreibung

Use Case	Grund	Betroffene Daten	Datenfluss
Datenauswertung	Assistenz für die sichere Fahrt	VIN, Innenraumdaten (Bild, Ton, Lenkradbewegung, etc.)	Fahrzeug zu Server

4. Datentaxonomie

4.1. Definition des Begriffes Datum

Jede Information wird in IT-Systemen in Form von Bit-Folgen repräsentiert. Diese Bit-Folgen haben in der natürlichen/realen Welt eine spezifische Bedeutung. Zum Beispiel kann die Bit-Folge `00101010` eine `Temperatur` repräsentieren (42 in diesem Fall). Diese Bedeutung der Bit-Folge soll im Folgenden den Begriff `Datum` oder `Daten` prägen - nicht die dahinterstehende Bit-Folge und der spezifische Wert. Wenn von dem Datum `Temperatur`gesprochen wird, steht dieses Datum symbolisch für alle möglichen Bit-Folgen, die dieses Datum annehmen kann. Somit sollen sich die Klassifikationen und die Taxonomie nicht auf die repräsentierten Werte, also die Bit-Folgen, beziehen, sondern auf die Bedeutung, die Relevanz oder den Zweck des Datums. Somit wird auch, von den verschiedenen Möglichkeiten einen spezifischen Wert mit einer Bit-Folge zu repräsentieren, abstrahiert.

Da es jedoch sein kann, dass der Inhalt oder Wert eines Datums über die Relevanz für den Datenschutz entscheidet, wird im Folgenden die `Klassifikation nach Relevanz` zusätzlich zu denen im Projekt festgeschriebenen Perspektiven Recht, Technik und Nutzersicht aufgenommen.

4.2. Ziele der Datentaxonomie

- Verständlichkeit/Transparenz (jeder soll eine sinnvolle Vorstellung der Bedeutung haben)
- Sinnvolle Granularität (nicht zu viele und nicht zu wenig Klassen)
- Umfassend (alle Daten sollen durch das Modell erfasst werden)
- Darstellung der gesetzlichen Realität (gesetzlich geregelte vorgeschriebene Datenerhebung soll als solche erkennbar sein)

4.3. Perspektiven der Datentaxonomie

Im Projekt soll Selbstdatenschutz aus rechtlicher, technischer und Nutzerperspektive betrachtet werden. Diese Perspektiven lassen sich zu Beginn auch für eine erste Kategorisierung verschiedener Klassifikationen nutzen. Zusätzlich muss noch die Perspektive der Datenschutzrelevanz - also der Notwendigkeit der Betrachtung im Datenschutzkontext - als Kategorie aufgenommen werden wie im vorigen Abschnitt ausgeführt.

Ziel einer Taxonomie ist ein Regelwerk zur Einordnung verschiedener Daten in spezifische verschiedene distinkte Klassen. Ein mögliches Ergebnis, dass bei der Betrachtung verschiedener Perspektiven auftritt, ist dabei allerdings, dass die verschiedenen genannten Perspektiven orthogonal sind und gleichzeitig angewendet werden können. Da ein Datum allein für eine Perspektive schon in mehrere Kategorien gleichzeitig fallen kann, wird, wenn nun mehrere Perspektiven gleichzeitig betrachtet werden, ein Datum somit möglicherweise Mitglied einer Vielzahl verschiedener Klassen.

Hier wäre es nun zwar möglich wiederum nach häufig wiederkehrenden Kombinationen von Klassen zu suchen um eine erneute Gruppierung/Klassifikation nach diesen Kombinationen durchzuführen. Dies wird aber erst nach Fertigstellung der Betrachtung der verschiedenen Anwendungsfälle möglich sein. Diese Aufgabe wird daher auf einen späteren Zeitpunkt des Projektes verlagert.

4.3.1. Klassifikationen aus rechtlicher Perspektive

Aus rechtlicher Perspektive werden folgende Begriffe in die Klassifikation aufgenommen:

- `"Personenbeziehbarkeit"` (untergliederbar in Daten zu einer *"bestimmten Person"* und einer *"bestimmbaren Person"*). Personenbezogene Daten sind es dann, wenn der Verantwortliche sie einer Person zuordnen kann. Das ist z.B. der Fall, wenn es sich um eine anwesende Person handelt oder andere Identifikationsmerkmale bekannt sind. Daher sind die Use Cases personenbezogen, in denen z.B. Abrechnungs- oder Registrierungsdaten auftauchen. Personenbeziehbar sind Daten dann, wenn irgendjemand die Daten nicht nur sehr unwahrscheinlich einer Person

zuordnen kann. Das könnte z.B. über Driver Fingerprinting geschehen und ist auch der Fall bei einer Pseudonymisierung.

- `"Daten besonderer Kategorie"`, im Folgenden als **Projekt-internes Kunstwort** synonym verwendet für die gesetzlich fest definierten Begriffe *"besondere Arten personenbezogener Daten"* (Begriff aus § 3 Abs. 9 BDSG) bzw. *"besondere Kategorien personenbezogener Daten"* (Begriff aus Art. 9 DSGVO). Solche Daten liegen vor, wenn aus ihnen *"die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung"* erfolgt.

  Im Hinblick auf die Schutzbedarfsfeststellung wird eine weitere Kategorie `"Profilbildungseignung"` in die Klassifikation aufgenommen um Daten zu beschreiben, die einen tiefgreifenden Einblick in persönliche Gewohnheiten und Verhaltensmuster erzeugen können. Beispiele hierfür sind Positionsdaten und Daten aus denen sich Bewegungsprofile ableiten lassen. Die dahinterstehende Wertung kann im Rahmen einer Abwägung berücksichtigt werden, ist jedoch nicht ohne Vorbehalt anzuwenden. Gesetzlich gibt es keine gesonderten Regelungen zu "profilbildungsgeeigneten Daten".

  In der Betrachtung der rechtlichen Einordnung wird zwischen den zwei Perspektiven,

- der `isolierten Betrachtung` des jeweiligen Datums und
- der `kombinierten Betrachtung` aus der Sicht des gesamten Verfahrens, bestehend aus Daten, Systemen und Prozessen

unterschieden, da sich in Kombination von Daten, d.h. aus den Kriterien der Schutzbedarfsfeststellung, sich ggf. eine andere Einschätzung ergeben kann. Bei der möglichen Beurteilung abstrakter Use-Cases (Kapitel 3) auf datenschutzfreundliche und nicht datenschutzfreundliche Weise eine "pessimistische Sicht" eingenommen.

4.3.1.1. Klassifikationen aus technischer Perspektive

Auf technischer Ebene kann man hauptsächlich zwischen zwei unterschiedlichen Granularitäten der Klassifikation unterscheiden. Einerseits hat jedes Datum eine `direkte Bedeutung` - also einen repräsentierten Wert bzw. interpretierbare Bedeutung wie eine Temperatur oder ein Name - oder andererseits kann jedes Datum seinem `Zweck und der darauf beruhenden Funktionalität` zugeordnet werden. Eine ähnliche Klassifikation nimmt die Landkarte der Daten-Kategorien beim vernetzten Fahrzeug[1] ebenfalls vor, daher wurde diese Klassifikation zusätzlich aufgenommen.

4.3.1.2. Klassifikationen aus Nutzersicht

Bei der Klassifikation aus Nutzersicht wird es insbesondere wichtig die Bedeutung der Daten in Beziehung zu dem Nutzer zu beschreiben. Also gibt ein Datum Informationen über den Nutzer an sich preis oder werden Objekte in seiner möglicherweise direkten Umgebung beschrieben. Daher wird für die Nutzersicht eine Klassifikation eingeführt, die beschreibt auf welches Objekt sich ein Datum bezieht (den Nutzer eingeschlossen). Zusätzlich kann die unter der technischen Perspektive eingeführte Klassifikation nach dem `Zweck und der darauf beruhenden Funktionalität`auch aus der Nutzerperspektive betrachtet werden, was diese Klassifikation als besonders hilfreich erscheinen lässt.

4.3.1.3. Hinweis zu den exemplarischen Klassen

Die im Folgenden eingeführten Klassen sollen lediglich exemplarisch die Klassifikationen erläutern. Sie müssen für eine finale Datentaxonomie erneut und mit mehr Gründlichkeit definiert und gewählt werden.

4.4. Aufzählung möglicher Klassifikationen

Im Folgenden werden die identifizierten Klassifikationen aufgezählt. Diese werden jeweils den betroffenen Perspektiven zugeordnet.

[1] Verband der Automobilindustrie (VDA) Datenschutz-Prinzipien für vernetzte Fahrzeuge. 2014 ⟨URL: https://www.vda.de/dam/vda/Medien/DE/Themen/Innovation-und-Technik/Vernetzung/Datenschutz-Prinzipien/VDA-Datenschutz-Prinzipien-2014/vda-datenschutzprinzipien-2014.pdf⟩.

4.4.1. Klassifikation nach Datenschutzrelevanz (generelle Perspektive)

Die triviale Lösung: Wenn ein Datum über einen beliebigen Weg personenbeziehbar ist, dann ist es ein `personenbezogenes Datum`, ansonsten nicht.

personenbeziehbar	Klasse des Datums
Ja	personenbezogenes Datum
Nein	nicht personenbezogenes Datum

Da zu Beginn die Unterscheidung zwischen verschiedenen Werten, die ein Datum annehmen kann, ausgeschlossen wurde, kann es schwer fallen für ein Datum zu entscheiden ob es personenbeziehbar ist oder nicht. Gerade der Inhalt eines Datums kann die Personenbeziehbarkeit hervorrufen. Beispielsweise könnte in einem Datum namens **Name** entweder der echte Name einer Person stehen oder doch nur ein anonymer Zufallswert. In diesem Sinne wird an dieser Stelle eine Überabschätzung notwendig, sodass alle Werte, die personenbeziehbar sein *könnten*, als personenbezogene Daten klassifiziert werden müssen. Dies ist insofern auch vertretbar als dass das Eintragen von anonymen Zufallswerten oder Pseudonymen sowie das Verschleiern von Werten durch Verschleierungsfunktionen schon als Maßnahme für den Datenschutz gewertet werden kann. Und diese Maßnahmen werden an dieser Stelle der Untersuchung noch nicht betrachtet - sie werden erst später auf Basis der Anforderungen definiert.

4.4.2. Klassifikation nach Datenschutzrelevanz und Profilbildungseignung (generelle Perspektive)

Zusätzlich zu der Personenbeziehbarkeit wird im Datenschutz (siehe Definition des Begriffs oben unter 4.3.1 für dieses Projekt) im Rahmen des Projekts auch zwischen Daten “besonderer Kategorie” und “Daten nicht besonderer Kategorie” (*Hinweis: Projekt-internes Kunstwort, kein gesetzlicher Begriff!*) unterschieden. Dieses sind Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben der beschriebenen Person. Durch die besondere Sensitivität dieser Daten ist eine Klassifikation nach eben dieser Sensitivität notwendig. Da zusätzlich auch durch das Sammeln und Auswerten spezifischer Daten ein Ableiten profilbildungsgeeigneter Informationen möglich, wird eine zusätzliche Kategorie der “Profilbildungseignung” mit den Unterbegriffen “profilbildungsgeeignet” / “abgeleitet profilbildungsgeeignet” / “nicht profilbildungsgeeignet” eingeführt.

Zusätzlich zu der Personenbeziehbarkeit wird im Datenschutz auch zwischen sensiblen und nicht-sensiblen personenbeziehbaren Daten unterschieden. Dieses sind Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben der beschriebenen Person. Durch die besondere Sensitivität dieser Daten ist eine Klassifikation nach eben dieser Sensitivität notwendig.

Da zusätzlich auch durch das Sammeln und Auswerten spezifischer Daten ein Ableiten sensibler Informationen möglich wird, wird eine zusätzliche Kategorie der sensibel ableitbaren Daten eingeführt.

Beispieldatum	Klasse des Datums
Außentemperatur	nicht personenbeziehbar, kein Datum besonderer Kategorie, nicht profilbildungsgeeignet
Fahrgestellnummer	personenbeziehbar, kein Datum besonderer Kategorie, nicht profilbildungsgeeignet
Standortverlauf	personenbeziehbar, kein Datum besonderer Kategorie, abgeleitet profilbildungsgeeignet
Nationalität	personenbeziehbar, kein Datum besonderer Kategorie, profilbildungsgeeignet

4.4.3. Klassifikation nach durch ein Gesetz geregelt/vorgeschrieben/gefordert (rechtliche Perspektive)

Rechtlich kann - zusätzlich zur trivialen Relevanz - unterschieden werden, ob die Erhebung, Verarbeitung oder Nutzung `durch ein Gesetz geregelt/vorgeschrieben/gefordert` ist oder `gesetzlich eine bestimmte Zweckbindung vorgeschrieben` ist. Dies ändert nicht die Notwendigkeit, sonstigen rechtlichen Anforderungen der Datenschutzgesetze zu prüfen, insb. der Prüfung des Personenbezugs eines Datums oder der Prüfung des Erfüllens der Voraussetzungen einer datenschutzrechtlichen Rechtsgrundlage (Bsp. Einwilligung zur Erhebung der Daten). Diese Klassifikation dient lediglich als Hinweis für den Grund bzw. Zweck der Datenerhebung.

Datenerhebung und/ oder Zweckbindung durch ein Gesetz geregelt/ vorgeschrieben/ gefordert	Klasse des Datums
Ja	Datum einer durch ein Gesetz geregelten/ vorgeschriebenen/ geforderten und/ oder zweckvorgeschriebenen Datenerhebung
Nein	Datum einer nicht durch ein Gesetz geregelten/ vorgeschriebenen/ geforderten und/oder zweckvorgeschriebenen

4.4.4. Klassifikation auf Signalebene nach Bedeutung (technische Perspektive)

Die direkte Bedeutung oder die repräsentierte Bedeutung kann zur Unterscheidung zwischen verschiedenen Daten genutzt werden. Dies ist insbesondere die grundlegende Definition des Begriffes `Datum` die zu Beginn der Seite eingeführt wurde. Somit entspricht diese Klassifikation der technischen Bedeutung der Daten. Hauptnachteil dieser Klassifikation ist, dass jedes dem System hinzugefügte Datum auch direkt eine neue Klasse erzeugt.

Beispieldatum	Klasse des Datums
Motordrehzahl	Motordrehzahl
Geschwindigkeit	Geschwindigkeit
Name des Fahrers	Name des Fahrers
...	...

4.4.5. Klassifikation nach Übertragungshäufigkeit und zweckmäßiger Profilbildung (technische Perspektive)

Es ist relevant ob ein Datum lediglich einmalig oder mehrmals übertragen wird. Ebenfalls ist interessant welche Übertragungen zusätzlich unter Angabe einer gemeinsamen Entität (wie z.B. einer Person oder einem Fahrzeug) abgespeichert und ausgewertet werden.

Beispieldatum	Klasse des Datums	Beschreibung der Klasse
Status Fenster und Türen abfragen ausgehend von Smartphone-App	einmalig übertragen, ohne Speicherung	einmalige, sehr seltene oder nicht periodische Anfragen mit direkter Weiterleitung/Antwort
erkannte Gefahrenstelle	einmalig übertragen, mit Speicherung in anonymer Datenbank	einmalige, sehr seltene oder nicht periodische Ereignisse, die an einer Stelle anonym gesammelt werden
Softwareupdate	einmalig übertragen, mit Speicherung in Profil über Fahrzeug ohne Bewegungsinformationen	einmalige, sehr seltene oder nicht periodische Ereignisse, die im Sinne der Nachvollziehbarkeit protokolliert werden (exkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)

Beispieldatum	Klasse des Datums	Beschreibung der Klasse
Pannenmeldung	einmalig übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen	einmalige, sehr seltene oder nicht periodische Ereignisse, die im Sinne der Nachvollziehbarkeit protokolliert werden (inkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)
Online-Shopping	einmalig übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungsinformationen	einmalige, sehr seltene oder nicht periodische Ereignisse, die im Sinne der Nachvollziehbarkeit protokolliert werden (exkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)
Restaurantbuchung	einmalig übertragen, mit Speicherung in Profil über Fahrer mit Bewegungsinformationen	einmalige, sehr seltene oder nicht periodische Ereignisse, die im Sinne der Nachvollziehbarkeit protokolliert werden (inkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)
Positionsdaten für online-optimierte Route	mehrmals übertragen, ohne Speicherung	häufig oder periodisch übertragene Anfragen mit direkter Weiterleitung/Antwort
Außentemperatur oder Verkehrsinformationen	mehrmals übertragen, mit Speicherung in anonymer Datenbank	häufige oder periodische Ereignisse, die an einer Stelle anonym gesammelt werden
Anzahl Türöffnungen (QS)	mehrmals übertragen, mit Speicherung in Profil über Fahrzeug ohne Bewegungsinformationen	häufige oder periodische Ereignisse, die an einer Stelle gesammelt und ausgewertet werden (exkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)
Durchschnittsverbrauch	mehrmals übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen	häufige oder periodische Ereignisse, die an einer Stelle gesammelt und ausgewertet werden (inkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)
Gewicht des Fahrers	mehrmals übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungsinformationen	häufige oder periodische Ereignisse, die an einer Stelle gesammelt und ausgewertet werden (exkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)
erkannte Gefahrenbremsung	mehrmals übertragen, mit Speicherung in Profil über Fahrer mit Bewegungsinformationen	häufige oder periodische Ereignisse, die an einer Stelle gesammelt und ausgewertet werden (inkl. Ortsdaten, die ein Bewegungsprofil ermöglichen würden)

4.4.6. Klassifikation durch Zuordnung zu einer Funktionalität oder einem funktionalen Bereich (technische Perspektive und Nutzersicht)

Auf technische Ebene können die Daten anhand ihrer Funktionalität bzw. ihres funktionalen Bereichs zusammengefasst werden. Ein Datum kann daher Mitglied mehrerer Klassen sein kann, wenn es für mehrere Funktionen benötigt wird.

Beispieldatum	Klassen des Datums
Motordrehzahl	Daten des Fahrbetriebs
Geschwindigkeit	Daten des Fahrbetriebs; Daten zur Berechnung der Lautstärke des Radios; Daten für die Navigation
GPS-Position	Daten für die Navigation; Daten zur Optimierung der Fahrerassistenzsysteme

Beispieldatum	Klassen des Datums
Name des Fahrers	Daten zur Identifikation des Fahrers

Da hier erstmals mehrere Klassen je Datum möglich sind, folgt zur Vollständigkeit eine Tabelle mit invertierter Zuordnung, welche möglicherweise im Sinne der Verständlichkeit vorzuziehen wäre.

Klasse der Daten	Daten
Daten des Fahrbetriebs	Motordrehzahl; Geschwindigkeit; Position des Gaspedals; Öltemperatur; ...
Daten für die Navigation	GPS-Position; Geschwindigkeit; Lenkwinkel; POIs des Fahrers; ...
Daten zur Identifikation des Fahrers	Name des Fahrers; Bremsverhalten; Lenkverhalten; Fingerabdruck des Fahrers; ...

4.4.7. Klassifikation nach der Landkarte der Daten-Kategorien beim vernetzten Fahrzeug (VDA 2014, technische Perspektive)

Diese Klassifikation ähnelt der Zuordnung nach einem funktionalem Bereich. Sie entspricht dabei dem VDA-Vorschlag aus 2014, ist aber auf eine kleinere Anzahl an Kategorien beschränkt. Eine eindeutige Zuordnung zu allein einer Klasse ist hier auch nicht möglich.

Beispieldatum	Klassen des Datums
Motordrehzahl	im Fahrzeug erzeugte, dem Fahrer angezeigte Kfz-Betriebswerte; im Fahrzeug erzeugte aggregierte Fahrzeugdaten; im Fahrzeug erzeugte technische Daten
Öltemperatur	im Fahrzeug erzeugte, dem Fahrer angezeigte Kfz-Betriebswerte; im Fahrzeug erzeugte technische Daten
Name des Fahrers	nutzereigene/eingebrachte Daten

4.4.8. Klassifikation durch beschriebenes Objekt/Person (Nutzersicht)

Für den Nutzer kann es wichtig sein zu erfahren, über welches Objekt oder welche Person Informationen in einem Datum enthalten sind.

Beispieldatum	Klasse des Datums
Erkanntes Verkehrsschild	Umwelt
Außentemperatur	Umwelt
Kilometerstand	Fahrzeug
Geschwindigkeit	Verkehrsinformationen; Fahrverhalten (Fahrzeug + Fahrer)
Name des Fahrers	Fahrer

4.4.9. Klassifikation durch enthaltene Information (Nutzersicht)

Für den Nutzer ist es insbesondere wichtig ein Verständnis davon zu bekommen, welche Art von Information erhoben wird. Dies bedeutet dass zusätzlich zu dem beschriebenen Objekt bzw. der beschriebenen Person auch die enthaltene erhobene Information genannt werden muss. Da dies inhaltlich identisch zu der Klassifikation durch Zuordnung zu einer Funktionalität oder einem funktionalen Bereich ist, wird diese Klassifikation hier nicht wiederholt.

4.5. Zusammenführen der Klassifikationen

Da nun eine Aufzählung der möglichen Klassifikationen erfolgt ist, kann nun damit begonnen werden diese sinnvoll einzusetzen oder zu kombinieren. Hierzu müssen aber vorher einige Überlegungen angestellt werden.

4.5.1. Notwendigkeit der verschiedenen Perspektiven

Die rechtliche Perspektive ist für die Bewertung der Datenschutzmaßnahmen unerlässlich. Nur auf diese Weise lässt sich eine Erfüllung der rechtlichen Anforderungen bestimmen. Allerdings verliert die rechtliche Perspektive insbesondere aus der Nutzerperspektive an Relevanz. Für einen Nutzer kann die empfundene Datenschutzrelevanz eines Datums unabhängig von der rechtlichen Relevanz und der Personenbeziehbarkeit sein. Insofern sollten bei einer nutzerzentrischen Lösung alle Daten unabhängig ihrer Bewertung nach der rechtlichen Perspektive gleich behandelt werden. Allerdings kann die Klassifikation nach der “Profilbildungseignung” für den Nutzer einen Hinweis für eine grobe Einordnung der erhobenen Daten ermöglichen.

Die technische Perspektive setzt ein Verständnis der technischen Vorgänge des Systems voraus. Diese technischen Vorgänge sollen nach den Zielen des Projektes zwar nachvollziehbar sein, jedoch wird dies nur technisch versierten Nutzern möglich sein. In diesem Sinn muss dem Nutzer zwar eine technische Klassifikation angeboten werden, diese muss allerdings zuerst die technisch weniger versierten Nutzer adressieren indem beispielsweise eine technisch stark vereinfachte Darstellung gewählt wird. Für den versierten Nutzer kann eine detailliertere Beschreibung auf Abruf (z.B. in einer tieferen Menüebene) zur Verfügung stehen.

Die Nutzerperspektive ist bei einer nutzerzentrischen Lösung selbstverständlich im Fokus. Hier wird es insbesondere wichtig, dass das Ziel der Verständlichkeit/Transparenz erfüllt wird. Um dies für jeden Nutzer erreichen zu können, werden abschätzbar Kompromisse bei der Granularität der Klassifikation notwendig sein. Dies muss aber nicht im Widerspruch zu den Zielen der Datentaxonomie stehen, wenn wie im vorigen Abschnitt eingeführt, eine Möglichkeit besteht zusätzliche Informationen abzurufen. Über diese zusätzlichen Informationen müssen so nicht nur die technischen Informationen transportiert, sondern auch die verbliebenen Ungenauigkeiten einer ersten vereinfachten Darstellung beseitigt werden.

4.5.2. Vorschlag zur Verwendung

Die rechtliche Perspektive wird dazu verwendet eine Prüfung der finalen SeDaFa-Architektur auf Erfüllung der rechtlichen Anforderungen vorzunehmen und um einen Anhaltspunkt für die Sensitivität eines Datums zu liefern. Die technische Perspektive und die Nutzerperspektive werden ebenfalls durch verschiedene Datentaxonomien vertreten. Das heißt dass hierarchisch zuerst alle Daten aus einer vereinfachten Nutzerperspektive klassifiziert werden indem der Bezug zu den beschriebenen Objekten hergestellt wird. Innerhalb dieser Klassen wird dann eine genauere technische Klassifikation nach der Funktion oder dem funktionalen Bereich durchgeführt um sowohl alle Ziele erfüllen zu können als auch um die technische Perspektive generell zu platzieren. Dies erfolgt durch die Zuordnung zu einem Funktionalem Bereich und einer Beschreibung der Verkettung der Daten bzw. wie häufig ein Datum übertragen wird.

4.5.2.1. (vorläufiges) Beispiel Parkdienst - Klassifikation durch beschriebenes Objekt/Person gefolgt von Klassifikation durch Zuordnung zu einer Funktionalität oder einem funktionalen Bereich inkl. Sensitivität

Vorläufige Liste der Daten im Anwendungsfall: Position, Zeit, erkannte Parklücken, erkannte Parkhausinformationen, Reiseziel, Reiseroute, Kennzeichen des Fahrzeuges, Name des Fahres, Bezahlinformationen des Fahrers, Parkplatzbuchung

Beinhaltete Funktionen: Erkennen und Hochladen von Parklücken und Parkhausinformationen, Herunterladen und Betrachten von Parkplatzdaten, Navigation zu einem freien Parkplatz, Reservieren und Bezahlen eines Parkplatzes

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit/ Daten besonderer Kategorie/ Profilbildungseignung	Übertragung/ Profilbildung	enthaltene Daten
Ortungs- und Routendaten	Fahrzeug, Fahrer	personenbeziehbar, keine Datum besonderer Kategorie, abgeleitet profilbildungsgeeignet	mehrmals übertragen, ohne Speicherung	Position, Zeit, Reiseziel, Reiseroute
Parkplatzinformationen	Umgebung	nicht personenbeziehbar, kein Datum besonderer Kategorie, nicht profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in anonymer Datenbank	erkannte Parklücken, erkannte Parkhausinformationen
Identifizierende Daten	Fahrzeug, Fahrer	personenbeziehbar,keine Datum besonderer Kategorie, nicht profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer	Kennzeichen des Fahrzeugs, Name des Fahrers, Bezahlinformationen des Fahrers (z.B. VISA-Kartennummer)
Bezahlinformationen	Fahrer	personenbeziehbar, keine Datum besonderer Kategorie, nicht profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer	Bezahlinformationen des Fahrers (z.B. VISA-Kartennummer), Parkplatzbuchung

Es wird ersichtlich, dass der funktionale Bereich stark abhängig vom betrachteten Anwendungsfall ist. Dennoch können einige funktionale Bereiche in verschiedenen Anwendungsfällen wiederverwendet werden.

Ebenfalls ist die Personenbeziehbarkeit genauer zu betrachten. Es muss betrachtet werden, welche Daten dem Anwendungsfall nach gemeinsam übertragen werden und somit möglicherweise eine Personenbeziehbarkeit herstellen (z.B. Übertragung eines Parkplatzes zusammen mit der FIN/VIN). In diesem vorläufigen Beispiel wurden die Daten vorerst separat betrachtet.

Weitere Datentaxonomien finden sich im Anhang dieses Dokuments.

5. Risikobewertung und Schutzbedarfsfeststellung nach SDM

Anhand der vorstehenden Übersicht und den in den Anwendungsfällen beschriebenen Verfahren ist eine Risikobewertung vorzunehmen, um den Schutzbedarf festzustellen.

5.1. Risikobewertung und Schutzbedarfsfeststellung nach SDM

Auf der Grundlage der Anwendungsfälle, der Untersuchung der dabei anfallenden Daten und der möglichen Angreifer (siehe AngreifermodellSinner et al.) ist nun eine Risikobewertung vorzunehmen. Eine solche Risikobewertung ist immer anhand der konkreten Umstände eines Einzelfalls durchzuführen. Sie dient dazu, den Schutzbedarf eines personenbezogenen Verfahrens festzustellen. Im Kontext von SeDaFa wurde sich bei der Entwicklung der Anwendungsfälle und der Datentaxonomie darauf verständigt, diese nicht schon von vornherein in der datenschutzfreundlichsten Variante zu betrachten. Dadurch würde der Blick auf die zu lösenden Probleme verstellt. Vielmehr geht es hier darum, deutlich zu machen, welche Risiken bestehen um dann im nächsten Schritt angemessene Maßnahmen zu finden, die diese Risiken so weit wie möglich eindämmen. Sodann wird im Rahmen der Evaluation zu untersuchen sein, ob dies der Fall ist.

5.1.1. Verfassungsrechtliche Grundlagen

Eine Risikobewertung nach SDM hat die Aufgabe den Schutzbedarf eines bestimmten Verfahrens festzustellen. Die Feststellung des Schutzbedarfs ist dann im nächsten Schritt Grundlage für die Entwicklung des Anforderungskatalogs. Je höher der Schutzbedarf ist, desto umfassender müssen nämlich auch die technischen und organisatorischen Anforderungen an ein personenbezogenes Verfahren sein. Dies ist Ausdruck des Verhältnismäßigkeitsgrundsatzes im engeren Sinne: Je tiefer in ein Grundrecht eingegriffen wird, desto schwerer müssen die den Eingriff rechtfertigenden Gründe wiegen. Dies bedeutet, dass schwerwiegende Eingriffe in die informationelle Selbstbestimmung von mindestens ebenso schwer wiegenden Gründen getragen werden müssen. Das Bundesverfassungsgericht hat dazu ausgeführt, der Gesetzgeber habe „organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken“ [1].

Die aus den Anforderungen abgeleiteten Maßnahmen verringern also die Eingriffsintensität auf Seiten der informationellen Selbstbestimmung und ermöglichen auf diese Weise erst eine verhältnismäßige Datenverarbeitung. Anknüpfungspunkt für die Durchführung der Risikobewertung kann daher nur das Risiko für das allgemeine Persönlichkeitsrecht der Betroffenen sein.

Diese Vorgehensweise nach SDM für eine Risikobewertung ist klar abzugrenzen von einer Vorgehensweise, die ein Risiko aus Sicht einer Organisation bewertet und dabei im Wesentlichen unmittelbare oder mittelbare finanzielle Risiken bewertet.

Auf abstrakter Ebene ist zu berücksichtigen, dass das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG wegen seiner Anknüpfung an die Menschenwürde einen erhöhten Schutz genießt[2].

5.1.2. Einfachrechtliche Vorgaben

Nach § 9 BDSG sind die erforderlichen technischen und organisatorischen Maßnahmen zur Ausführung des Gesetzes zu treffen, wobei die Erforderlichkeit an dieser Stelle so definiert ist, dass Maßnahmen nur dann erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Anlage zu § 9 S. 1 BDSG nennt, welche Maßnahmen insbesondere zu treffen sind. Wegen der Formulierung „insbesondere“ ist die Aufzählung nicht abschließend. Es können auch darüber hinausgehende Maßnahmen erforderlich sein. Um zu ermitteln, welcher Aufwand angemessen und somit erforderlich ist, ist der Schutzbedarf der personenbezogenen Daten festzustellen. Für die konkrete Schutzbedarfsfeststellung hat sich eine dreistufige Skala etabliert: normal, hoch und sehr hoch. Ein normaler Schutzbedarf ist bei jeder Erhebung, Verarbeitung und Nutzung personenbezogener Daten gegeben, da hiermit immer ein Eingriff in die informationelle Selbstbestimmung der Betroffenen verbunden ist. Es ist daher nicht zu diskutieren,

[1] BVerfG, Urt. v. 15.12.1983, Az.: 1 BvR 209/83 Rn. 175

[2] Fabio, Udo Di Grundgesetz-Kommentar. Maunz/Dürig, 76. EGL 2015, Nr. Art. 2.

ob Schutzmaßnahmen überhaupt getroffen werden müssen. Der Abwägung zugänglich ist aber die Frage, in welchem Umfang Schutzmaßnahmen zu treffen sind.

Die Kategorien hoch und sehr hoch liegen vor, wenn nach Prüfung der Umstände des Einzelfalles eine erhöhte Eingriffsintensität festgestellt wird.

Noch deutlicher wird die Wichtigkeit dieses Aspektes einer datenschutzkonformen Entwicklung und eines datenschutzkonformen Betriebs von Systemen in der Datenschutzgrundverordnung. Art. 24 DSGVO regelt die technischen und organisatorischen Maßnahmen zur Einhaltung der DSGVO. Sie sollen „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ eingesetzt werden. Art. 32 regelt die die Sicherheit der Verarbeitung und formuliert ganz ähnlich wie Art. 24 DSGVO, dass „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verabeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ die geeigneten technischen und organisatorischen Maßnahmen zu treffen sind. Die Risikobewertung ist mithin ein zentraler Bestandteil der Ermittlung der geeigneten technischen Maßnahmen sowohl zur Einhaltung der DSGVO als auch der Sicherheitsanforderungen. Bei der Frage, welche Maßstäbe an eine ordnungsgemäße Risikobewertung anzulegen sind, hilft Art. 1 Abs. 2 DSGVO weiter. Danach dient die Datenschutzgrundverordung dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere dem Recht auf Schutz personenbezogener Daten. Ein „Risko“ in diesem Sinne kann also nur die Eingriffsintensität in das Grundrecht auf Datenschutz nach Art. 8 der Charta der Grundrechte der europäischen Union sein. Im nachfolgenden werden Kriterien skizziert, anhand derer eine erhöhte Eingriffstiefe geprüft werden kann.

5.1.3. Art und Umfang der personenbezogenen Daten

Eine erhöhte Eingriffsintensität kann sich zunächst insbesondere aus Art und Umfang der verarbeiteten personenbezogenen Daten ergeben.

Indizien für eine erhöhte Eingriffsintensität aufgrund der ***Art*** der Daten:

- Verarbeitung nicht veränderbarer personenbezogener Daten, da diese Anknüpfungspunkt für eine weitgehende Verkettung von personenbezogenen Daten sein können (z.B. biometrische Daten)
- Verarbeitung von anderweitig hoch verknüpfbaren Daten (z.B. Kennzeichen, andere Identifier, die nicht häufig wechseln)
- Daten aus der Privat- oder Intimsphäre der Betroffenen (evtl. auch Positionsdaten, zumindest bei privat genutztem Fahrzeug)
- Verarbeitung sensitiver Daten (Rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben)
- Verarbeitung von Daten, die Hinweise auf besondere Kategorien personenbezogener Daten zulassen (z.B. Positionsdaten, die Hinweise auf den Besuch spezialisierter medizinischer Einrichtungen zulassen)

Umfang: Die Eingriffsintensität erhöht sich mit der Anzahl der betroffenen Personen [3]. Das gleiche gilt wegen der daraus entstehenden Verkettungsmöglichkeiten, wenn eine Vielzahl von Daten eines einzelnen Betroffenen verarbeitet wird.

5.1.4. Eingriffsintensive Verfahren

Neben Art und Umfang der zu erhebenden personenbezogenen Daten sind auch Besonderheiten des Verfahrens bei der Bestimmung der Eingriffstiefe zu prüfen.

Eine erhöhte Eingriffsintensität ist darüber hinaus anzunehmen, wenn ein Verfahren aus bestimmten Gründen intransparent gestaltet werden soll oder Eingriffsmöglichkeiten für den Betroffenen nicht vorliegen sollen. Beispiele hierfür finden sich im Rahmen der Datenverarbeitung zur Strafverfolgung und Gefahrenabwehr (z.B. verdeckte Ermittlungsmaßnahmen).

Auch die möglichen Folgen des Verfahrens für den Betroffenen sind bei der Eingriffsintensität zu berücksichtigen:

- Verfahren, die erhebliche finanzielle Folgen für den Betroffenen nach sich ziehen können.
- Verfahren, die Auswirkungen auf die körperliche Unversehrtheit der Betroffenen haben können.
- Verfahren, die Auswirkungen auf die Fortbewegungsfreiheit der Betroffenen haben können.

[3] Vgl. BVerfG, Urt. v. 02.03.2010

- Verfahren, die Einschüchterungseffekte in Bezug auf die Grundrechtsausübung der Betroffenen auslösen können.
- Verfahren, bei denen eine Vielzahl an Personen Zugriff auf die Daten hat.
- Erhöhte Gefahr der Verarbeitung von unrichtigen Daten

Schließlich ist auch zu berücksichtigen, ob der Betroffene selbst durch ein ihm vorwerfbares, zurechenbares Verhalten einen Anlass zur Datenverarbeitung gegeben hat oder ob die Daten anlasslos verarbeitet werden. Liegt ein solcher Anlass nicht vor, so spricht dies für eine sehr hohe Eingriffsintensität [4].

Übertragbar könnten solche Überlegungen des Bundesverfassungsgerichts auf Forderungen sein, wonach in Fahrzeuge eine Blackbox eingebaut werden solle, die drei Jahre speichert, wann das Fahrzeug von einem Menschen und wann vom Computer gesteuert wurde[5].

Aus den bereits genannten Kriterien oder aus anderen Gründen können sich auch eine erhöhte Motivation für Missbrauch der Daten durch die verantwortlichen Stelle oder die sonst erhöhte Gefahr von Missbrauch, Verlust oder unbefugter Kenntniserlangung ergeben. Beides spricht für eine erhöhte Eingriffsintensität.

Es ist nochmals zu betonen, dass die vorstehenden Kriterien in einer Gesamtbetrachtung umfassend zu würdigen sind und die darauf beruhende Schutzbedarfseinstufung im Einzelfall entsprechend zu begründen. Es ist zu beachten, dass die aufgeführten Kriterien nicht abschließend sind.

5.1.5. Anwendung dieser Grundsätze auf das vernetzte Fahrzeug

Die Anwendung dieser Grundsätze auf das vernetze Fahrzeug zeigt, dass es hier um einen für die informationelle Selbstbestimmung sehr sensiblen Bereich geht. Das Auto ist für viele Menschen das zentrale Fortbewegungsmittel. Von Datenverarbeitung im Fahrzeug wird also in naher Zukunft fast jeder Autofahrer zumindest in der westlichen Welt betroffen sein. Im Rahmen des vernetzten Fahrzeugs gibt es eine Vielzahl von denkbaren Anwendungsfällen, bei denen Positionsdaten anfallen. Diese eröffnen die Möglichkeit, tiefgreifende Einblicke in die Lebensgewohnheiten der betroffenen Personen zu erlangen. Auch wenn nicht unmittelbar Daten einer besonderen Kategorie im Sinne von Art. 9 DSGVO erhoben werden, lassen sich aus solchen Positionsdaten Erkenntnisse über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit ableiten. Allein die Möglichkeit solcher Rückschlüsse kann dazu führen, dass betroffene Personen ihr Verhalten ändern, vielleicht doch nicht zu einer politischen Demonstration fahren oder sich nicht zu einer Moschee begeben, für die sie sich interessieren, und mithin ihre Grundrechte aufgrund von Einschüchterungseffekten nicht ausüben.

Es ist auch absehbar, dass Fahrzeugdaten verstärkt in gerichtlichen Verfahren Verwendung finden[6] oder dazu genutzt werden, anhand des Fahrverhaltens die Höhe von Versicherungsbeiträgen zu berechnen Datenverarbeitungsvorgänge, die Richtigkeit der gespeicherten Daten und die Zugriffsmöglichkeiten auf diese Daten werden also erhebliche finanzielle und strafrechtliche Auswirkungen für die betroffenen Personen haben können.

Die in den Anwendungsfällen untersuchten Verarbeitungsvorgänge sind überwiegend anbieterneutral. Es wäre denkbar, dass sie durch eine Vielzahl von Anbietern zur Verfügung gestellt werden oder durch zentrale Anbieter. Je mehr Nutzer ein Dienst hat, umso größer ist die Gefahr, dass es sich lohnt, auch größere Widerstände zu überbrücken, um unbefugt auf dessen Daten zuzugreifen, andererseits ist auch denkbar, dass größere Anbieter höhere Sicherheitsanforderungen erfüllen als kleinere, für die sich ein Aufwand schwer amortisiert. Die Entwicklung des Angreifermodells hat gezeigt, dass es eine Vielzahl von Akteuren gibt, die ein potentielles Interesse an Fahrzeugdaten haben. Werden durch einen Anbieter mehrere Dienste angeboten oder werden durch einen Dienst Daten zu unterschiedlichen Zwecken erhoben, so erhöht sich dadurch die Gefahr, dass Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unbefugt miteinander verkettet werden. Größere Dienstanbieter haben zudem regelmäßig eine größere Anzahl an Mitarbeitern, die Zugriff auf Daten haben oder benötigen. Andererseits kann es bei kleineren Anbietern auch sein, dass eine organisatorische Trennung schwieriger ist. Darüber hinaus können größere Ansammlungen von personenbezogenen Daten auch ein lohnenderes Ziel für unbefugte Angreifer darstellen, die nicht Teil der Organisation sind (z.B.„Hacker“). Zwar gibt es keine gesetzlichen Regelungen, die solche großen Anbieter verhindern, dennoch ergibt sich aus dem erhöhten Risiko für Anbieter die Pflicht, entsprechend zusätzliche und ggf. auch sehr kostenintensive Maßnahmen umsetzen zu müssen.

Die Fahrer können zudem von der Datenverarbeitung besonders stark abhängig sein, wenn von einer korrekten Datenverarbeitung die Funktionsfähigkeit des Fahrzeugs abhängt. Verlässt sich eine betroffene Person beispielsweise darauf, dass die Diagnosesysteme in ihrem Fahrzeug den Bedarf für einen Werkstattbesuch korrekt erkennen, obwohl dies nicht der

[4] Vgl. BVerfG, Urt. v. 02.03.2010, Az.: 1 BvR 256/08, Rn. 210 - Vorratsdatenspeicherung

[5] Wilkens, Andreas Verkehrsminister Dobrindt will fahrerloses Einparken erlauben. 09 2016 ⟨URL: https://heise.de/-3319487⟩.

[6] vgl. in: Souza Soares, Philipp Alvares de BMW liefert Gericht Kundendaten für Bewegungsprofil. 07 2016 ⟨URL: http://www.manager-magazin.de/unternehmen/autoindustrie/bmw-autobauer-liefert-gericht-kundendaten-fuer-bewegungsprofil-a-1104050.html⟩.

Fall ist, kann dies die Mobilität des Betroffenen einschränken. Dies verschärft sich nochmal in ländlichen Gegenden, wenn die betroffene Person nicht die realistische Möglichkeit hat, kurzfristig auf öffentliche Verkehrsmittel auszuweichen.

Soweit datenverarbeitende Systeme im Fahrzeug auch sicherheitsrelevante Funktionen erfüllen, besteht eine Gefahr für Leib und Leben der Insassen. Es sind dann besonders hohe Anforderungen an Integrität und Verfügbarkeit der Verfahren zu stellen. Dies kann z.B. das eCall-System betreffen, welches automatisch bei Detektion eines Unfallereignisses einen Notruf absendet aber auch Müdigkeitssensoren kommen für solche Einstufungen in Betracht.

Ein Risiko für die informationelle Selbstbestimmung, das nicht nur die Datenverarbeitung bei Fahrzeugen betrifft, ist die Komplexität der Verarbeitungsvorgänge und die Möglichkeit ihrer Abänderung[7]. Die informationelle Selbstbestimmung soll der betroffenen Person erlauben, zu wissen, wer was wann über sie weiß[8] . Komplexe technische Datenverarbeitungsvorgänge mit mehreren Beteiligten beinhalten das Risiko, dass diese für die Nutzer nicht mehr nachvollziehbar sind und sie folglich nicht mehr wissen können, wer was wann über sie weiß.

Als besonders kritisch zu bewerten sind auch solche Szenarien, in denen hoch verknüpfbare Daten verarbeitet werden. Hoch verknüpfbar sind beispielsweise biometrische Daten. Werden Fahrzeugidentifikationsnummern bei der Kommunikation mit einem Backend übertragen erzeugt dies eine hohe Verknüpfbarkeit, die die Eingriffstiefe der Datenverarbeitung erhöht. Eine solche hochgradige Verknüpfbarkeit kann sich aber nicht nur aus einzelnen Daten oder bestimmten Daten ergeben, sondern auch aus der Analyse von Daten, die auf den ersten Blick nicht geeignet erscheinen, eine Verknüpfung zu unterstützen. Als Beispiel können hier Daten aus Sensoren aus dem Fahrzeug genannt werden, die zur Profilbildung geeignet sind und miteinander gespeichert oder übertragen werden[9]. Obwohl dort nicht unmittelbar identifizierende Daten vorhanden sind, lassen sich anhand der Sensordaten unterschiedliche Fahrer leicht voneinander unterscheiden.

Auch aus dem Wert der personenbezogenen Daten können Risiken entstehen, wenn dies verantwortliche Stellen dazu motivieren kann, datenschutzrechtliche Restriktionen bei der Übermittlung von personenbezogenen Daten entweder vorsätzlich zu missachten oder fahrlässig fehlerhaft auszulegen.

Nach alledem ist bei Datenverarbeitung im Zusammenhang mit vernetzten Fahrzeugen tendenziell von einer erhöhten Eingriffsintensität und damit von einem erhöhten Schutzbedarf auszugehen. Zwar mögen einzelne Datenverarbeitungsvorgänge für sich betrachtet eher einen normalen Eingriff darstellen, jedoch sind die Datenverarbeitungsverfahren immer im Rahmen einer Gesamtschau zu betrachten. Für die Zukunft gilt, dass mit der Zunahme von im Fahrzeug vorhandenen Datenverarbeitungssystemen und der Zunahme der Vernetzung der Fahrzeuge auch der datenschutzrechtliche Schutzbedarf zunimmt.

[7] vgl. in: Krieger-Lamina, Jaro Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen. 2016 S 54 f..

[8] Urteil v. 15.12.1983 in: BVerfG Urteil. 12 1983 Az. 1BvR 209/83, Rn. 172.

[9] vgl. in: Enev, Miro et al. Automobile Driver Fingerprinting. PoPETs, 2016 2016, Nr. 1 ⟨URL: http://www.degruyter.com/view/j/popets.2016.2016.issue-1/popets-2015-0029/popets-2015-0029.xml⟩.

6. Rechtliche Analyse

Aus rechtlicher Sicht wirft das vernetzte bzw. datenverarbeitende Fahrzeug Fragen auf, die teilweise grundsätzliche datenschutzrechtliche Probleme zum Hintergrund haben und sich teilweise aus spezialgesetzlichen Regelungen ergeben. Aus datenschutzrechtlicher Sicht ist der Personenbezug der Daten zu prüfen und die Herstellung der Transparenz erforderlich, so dass betroffene Personen Kenntnis von der verantwortlichen Stelle und den jeweiligen Verarbeitungshandlung in einfacher und verständlicher Weise erhalten können. Hinsichtlich der spezialgesetzlichen Regelungen stellen sich Fragen nach der Abrechnung von Ladevorgängen und dem Verhältnis zwischen allgemeinem und speziellem Datenschutzrecht.

Die nachfolgenden Untersuchungen beziehen sich im Schwerpunkt auf die Datenschutzgrundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im folgenden Datenschutz-Grundverordnung oder DSGVO)), die ab dem 25.05.2018, und damit kurz nach dem Ende des Projektes SeDaFa Geltung erlangen wird, Art. 99 Abs. 2 DSGVO. Das deutsche Datenschutzrecht wird dann in weiten Teilen nicht mehr anwendbar sein. Es bleibt abzuwarten, wie der deutsche Gesetzgeber von den ihm verbleibenden Umsetzungsspielräumen Gebrauch machen wird[1] . Ein erster Entwurf für ein Datenschutz-Anpassungs-und-Umsetzungsgesetz EU (DSAnpUG-EU) wurde wieder zurückgezogen[2] .

Seine verfassungsrechtliche Grundlage findet das Datenschutzrecht im Grundrecht auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 Grundgesetz (GG) sowie aus den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union [3].

6.1. Allgemeines Datenschutzrecht

Zunächst soll im nachfolgenden Abschnitt auf die allgemeinen datenschutzrechtlichen Problematiken eingegangen werden. Das Datenschutzrecht verfolgt nach § 1 Abs. 1 BDSG den Zweck, die betroffene Person vor einer Beeinträchtigung ihres Persönlichkeitsrechts durch die Verarbeitung von personenbezogenen Daten zu schützen. Auch die Datenschutzgrundverordnung bestimmt nach Art. 1 Abs. 2 DSGVO, dass die Verordnung „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ schützt.

Dieses Rechtsgebiet sieht sich vor dem Hintergrund neuer technologischer Entwicklungen immer wieder mit neuen Herausforderungen konfrontiert und gewinnt in dem Maße an Bedeutung, mit dem datenverarbeitende Technologien Verbreitung finden. Nach der Entwicklung des Internets, der Verbreitung von Smartphones und Wearables ist das vernetzte Fahrzeug eine weitere datenverarbeitende Technologie, mit der fast die gesamte Bevölkerung in ihrem täglichen Leben in Berührung kommen wird. Hinzu kommt die oben erwähnte Einführung der Datenschutzgrundverordnung, die den Rechtsanwender mit 99 Artikeln und 173 Erwägungsgründen vor eine Vielzahl von neuen Regelungen stellt, andererseits aber auch auf bekannte Grundsätze zurückgreift. Sie sollte als modernes Datenschutzrecht in der Lage sein, das in Art. 1 Abs. 2 DSGVO gemachte Versprechen des Grundrechtsschutzes einzulösen, gleichzeitig ein möglichst hohes Maß an Rechtssicherheit gewährleisten und die neuen Herausforderungen angemessenen Lösungen zuzuführen.

6.1.1. Personenbezug

Obwohl das Datenschutzrecht bereits über 20 Jahre alt ist, ist der zentrale Begriff dieses Rechtsgebietes immer noch umstritten. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener)“. Die juristische Diskussion dreht sich um die Frage, wie weit der Begriff der Bestimmbarkeit auszulegen ist. Hinsichtlich der Frage, ob eine dynamische IP-Adresse ein personenbezogenes Datum ist, hat der BGH dies dem EuGH vorgelegt [4]. Der EuGH antwortete [5], dass es sich auch bei

[1] zu den Umsetzungsspielräumen: in: Kühling, Jürgen et al. DIE DATENSCHUTZ-GRUNDVERORDNUNG und DAS NATIONALE RECHT. 2016.

[2] Vgl. in: Becker, Ralf/Kefelja, Tobias/Jacqueline, Bredereck Neuer Entwurf für neues BDSG veröffentlicht (2. und 3. Versuch). https://www.datenschutz-grundverordnung.eu/entwurf-neues-bdsg-veroeffentlicht/.

[3] Zu den grundrechtlichen Spannungsverhältnissen beim vernetzen Fahrzeug: Roßnagel Datenschutz und Datensicherheit - DuD 39 [2015] , DuD 2015, 353 ff.

[4] BGH, Beschluss v. 28.10.2014, Az.: VI ZR 135/13

[5] EuGH, Urteil vom 19.10.2016, Az.: C-582/14

dynamischen IP-Adressen um personenbezogene Daten handelt, wenn „er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen“ [6].

Der bisherige Streit dreht sich im Wesentlichen um die Frage, ob für die Bestimmbarkeit nur Informationen der verantwortlichen Stelle oder auch Informationen von Dritten, die zu einer Identifikation führen können, zu berücksichtigen sind.

Nach der Datenschutzgrundverordnung und dem eben genannten Urteil wird diese Diskussion voraussichtlich entschieden sein. Nr. 26 der Erwägungsgründe stellt klar, unter welchen Voraussetzungen von einer Bestimmbarkeit auszugehen ist: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen `oder einer anderen Person` nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.“ Da ausdrücklich andere Personen genannt werden, kommt es nicht nur auf die Mittel der verantwortlichen Stelle an sondern auch solche Informationen, die Dritten zur Verfügung stehen.[7][8]

Der EuGH hatte in seinem oben genannten Urteil zu den IP-Adressen entschieden, dass es „rechtliche“ Mittel sein müssen, die bei der Beurteilung der Bestimmbarkeit heranzuziehen sind. Es ist fraglich, ob diese Einschränkung unter der Datenschutz-Grundverordnung bestehen bleiben kann. Wie soeben dargestellt, sind nach Erwägungsgrund Nr. 26 „alle Mittel“ für die Beurteilung der Bestimmbarkeit heranzuziehen. Eine Einschränkung auf rechtliche Mittel kann diesem Erwägungsgrund nicht entnommen werden. Prüfungsmaßstab des Erwägungsgrundes Nr. 26 ist lediglich, ob Mittel „nach allgemeinem Ermessen wahrscheinlich“ genutzt werden.

Allerdings schränkt der Erwägungsgrund dann im Weiteren den Begriff der Personenbeziehbarkeit ein. Es ist nicht jede völlig abstrakte, extrem zeitaufwendige und kostenintensive Möglichkeit der Identitätsfeststellung zu berücksichtigen. Vielmehr sollen bei „der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“ Die Frage, wann das Datenschutzrecht überhaupt anwendbar ist, kann damit von einer schwierigen Abwägungsentscheidung abhängen.

Die DSGVO wählt damit einen Mittelweg zwischen zwei Extrempositionen. Es kommt zwar nicht allein auf die Möglichkeiten des Verantwortlichen an, aber es sind auch nicht alle unwahrscheinlichen, besonders kostenintensiven und besonders zeitaufwändigen Mittel zu berücksichtigen.

Ein weiterer interessanter Punkt des Erwägungsgrundes Nr. 26 ist, dass technologische Entwicklungen zu berücksichtigen sind. Nach dem Willen des Verordnungsgebers kann also ein Datum, das zu einem bestimmten Zeitpunkt nicht personenbezogen ist, zu einem späteren Zeitpunkt personenbezogen sein.

Der Verantwortliche muss regelmäßig überprüfen, ob alle nicht personenbezogenen Daten, die sie verwenden, nunmehr nach dem aktuellen Stand der Technik oder durch anderweitig bekannt gewordene Informationen personenbeziehbar geworden sind. Es ist dann nicht ausreichend, dies lediglich festzustellen, sondern der Verantwortliche muss darauf reagieren und sollte idealerweise über Prozesse verfügen, die eine angemessene Reaktion ermöglichen. Dem Verantwortlichen steht es frei, auch nicht personenbezogene Daten so zu behandeln, als wären diese personenbezogen. Sofern Zweifel über die Personenbeziehbarkeit von Daten vorliegen, oder wenn zu erwarten ist, dass sich durch technologische Entwicklung die Beurteilung der Personenbeziehbarkeit ändern wird oder als Alternative zu einem Prüfvorgang, ob die Daten personenbezogen sind, kann es für den Verantwortlichen sinnvoll sein, die Daten von vorneherein als personenbezogen zu betrachten um Risiken zu vermeiden [9].

Die fehlerhafte Verneinung des Personenbezugs kann die betroffenen Personen erheblich beeinträchtigen und dazu führen, dass der Verantwortliche sich rechtswidrig verhält. So z.B. bei der Erhebung von Angaben zum Onlineverhalten durch ein Browser-Plugin zu Bewertung von Webseiten und der anschließenden Weitergabe dieser Daten vom Plugin-Hersteller an Dritte ohne adäquate Anonymisierung der Informationen. In diesem Fall konnte das Surfverhalten deutscher Internetnutzer doch auf Basis der vorgeblich anonymen Daten rekonstruiert werden[10].

Die Frage des Personenbeziehbarkeit ist von der Frage der Pseudonymisierung zu trennen. Eine Pseudonymisierung liegt immer dann vor, wenn personenbezogene Daten so verändert werden, dass ohne Hinzuziehung von zusätzlichen Informationen keine Identifizierung mehr stattfinden kann, Art. 4 Nr. 5 DSGVO. Die Bestimmbarkeit bleibt also über die

[6] EuGH, Urteil vom 19.10.2016, Az.: C-582/14, Rn. 49

[7] Ernst Kapitel I. Allgemeine Bestimmungen. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1.

[8] Schantz, Peter Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016, Nr. 26.

[9] Vgl. Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 38

[10] s. in: Eckert, Svea/Klofta, Jasmin/Strozyk, Jan Lukas Nackt im Netz: Auch intime Details von Bundespolitikern im Handel. https://daserste.ndr.de/panorama/archiv/2016/Nackt-im-Netz-Intime-Details-von-Politikern-im-Handel,nacktimnetz110.html, 11 2016.

zusätzlichen Informationen erhalten.

Eine Untersuchung des Personenbezugs im Zusammenhang mit dem vernetzten Fahrzeug findet sich in der Datentaxonomie.

6.1.2. Verantwortlicher bzw. verantwortliche Stelle

Aus der Bestimmung des „Verantwortlichen“ gemäß der DSGVO bzw. der „verantwortlichen Stelle“ im BDSG ergibt sich, wer Adressat der datenschutzrechtlichen Pflichten ist, also z.B. für die Verarbeitung basierend auf Rechtsgrundlagen und die Sicherheit der Daten einstehen muss oder die Transparenzpflichten zu erfüllen hat. Dabei handelt es sich nach Art. 4 Nr. 7 DSGVO um „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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“.

Maßgeblich ist daher, wer die Entscheidung über die Zwecke und Mittel der Verarbeitung trifft. Dabei muss diese Entscheidung nicht alleine getroffen werden, sondern kann auch von mehreren Stellen gemeinsam getroffen werden, die dann gemeinsam verantwortlich werden. Neben einer solchen, auf einer Subsumtion des Einzelfalles beruhenden Feststellung der Verantwortlichkeit gibt es die Möglichkeit, die Verantwortlichkeit gesetzlich festzulegen. Eine solche gesetzliche Festlegung der Verantwortlichkeit existiert beim vernetzten Fahrzeug weitestgehend nicht. Lediglich für eCall ist festgelegt, dass die Notrufabfragestellen und eCall-Notrufabfragestellen als für die Verarbeitung Verantwortliche gelten, Art. 6 Abs. 1 S. 1 eCall-Verordnung [11].

Für die Bestimmung, wer über die Mittel und Zwecke der Datenverarbeitung entscheidet, können tatsächliche Kriterien herangezogen werden.

Bezüglich der Entscheidung über die Zwecke können Anhaltspunkte für die Verantwortlichkeit sein, wessen Zwecken die Datenverarbeitung dient und wer sie initiiert hat. [12] Bezüglich der Entscheidung über die Mittel ist nach Ansicht der Artikel-29-Gruppe ebenfalls maßgeblich, wer tatsächlich die Entscheidung über die Mittel der Datenverarbeitung fällt. Fällt eine Stelle bezüglich einer Datenverarbeitung die Entscheidung über die Zwecke und überlässt einer anderen Stelle die Entscheidung über die Mittel, ist nach Ansicht der Artikel-29-Gruppe grundsätzlich die erste Stelle als Verantwortlicher zu betrachten, während die zweite Stelle jedenfalls unter Geltung der bisherigen Datenschutzrichtlinie [13] als Auftragsdatenverarbeiter in Betracht kommt [14].

Ein neues Instrument der DSGVO ist die Regelung zur gemeinsamen Verantwortlichkeit in Art. 26 DSGVO. Im Einzelfall ist prüfen, ob eine gemeinsame Verantwortlichkeit einschlägig ist und ggf. dann ein Vertrag nach Art. 26 DSGVO zu schließen ist. Ein möglicher Anwendungsfall könnte eine gewünschte enge Zusammenarbeit zwischen einer Kommune und einem Ladesäulenbetreiber sein.

Die Prüfung der Verantwortlichkeit muss letztlich immer unter Berücksichtigung aller relevanten Aspekte des Einzelfalles vorgenommen werden. Angesichts der Vielzahl von möglichen beteiligten Stellen, z.B. Hersteller, Diensteanbieter, Netzbetreiber, App-Anbieter und Halter[15] [16] , ist es auch angemessener Fallgruppen und Indizien für die Bestimmung des Verantwortlichen zu entwickeln, als bestimmten Beteiligten pauschal eine Verantwortlichkeit oder Nichtverantwortlichkeit zuzuweisen. Die Beurteilung ist von Relevanz, da ohne Verantwortlichen der Adressat der datenschutzrechtlichen Pflichten fehlt und somit das Datenschutzrecht nicht angewendet wird.

6.1.3. Verarbeitung zu ausschließlich persönlichen oder familiären Zwecken

Das Datenschutzrecht ist nicht anwendbar, wenn eine Verarbeitung zu ausschließlich persönlichen oder familiären Zwecken nach Art. 2 Abs. 2 c) DSGVO bzw. § 1 Abs. 2 Nr. 3 BDSG vorliegt.

Überlässt somit der Halter einem anderen Familienmitglied oder einem Freund das Fahrzeug im Rahmen einer Gefälligkeit, dann befindet er sich regelmäßig außerhalb des Anwendungsbereichs des Datenschutzrechts. Hier greift

[11] Delegierte Verordnung (EU) Nr. 305/2013 der Kommission vom 26. November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes

[12] Artikel-29-Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsdatenverarbeiter“, S. 10 ff., abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

[13] Richtlinie 95/64/EG

[14] Arikel-29-Datenschutzgruppe, a.a.O., S. 18

[15] Vgl. in: Weichert, Thilo Datenschutz im Auto – Teil 1. SVR, 2014, Nr. 6.

[16] s. Abschnitt 3.6

die Ausnahme nach Art. 2 Abs. 2 c) DSGVO, wonach die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten findet, wenn diese durch eine natürliche Person im Rahmen von ausschließlich persönlichen oder familiären Tätigkeiten erfolgt. Diese Vorschrift ist zwar eng auszulegen und nur dann anwendbar, wenn die Tätigkeit nicht nach außen gerichtet ist und so den familiären oder persönlichen Bereich verlässt [17], dies ist aber so lange nicht der Fall, wie die Daten im Fahrzeug verbleiben.

Ob der persönliche und familiäre Bereich verlassen wird, wenn sich der Halter, nachdem er das Fahrzeug von dem Freund oder Familienmitglied zurück erhalten hat, nun zu einer Werkstatt begibt und dort zu Diagnosezwecken Fahrzeugdaten auslesen werden, ist umstritten. [18]

6.1.4. Verarbeitung beim Mietwagen oder Carsharing bzw. im Rahmen eines Dienst- oder Arbeitsverhältnis

Der Verantwortliche ist der jeweilige Anbieter, also die Mietwagenfirma oder der Betreiber des Carsharing-Angebots bzw. das Unternehmen oder die Behörde, die Halterin des Dienst- oder Firmenwagens ist, die das Fahrzeug der betroffenen Person zu dienstlichen Zwecken bereitstellt und personenbezogene Daten ausliest und dadurch erhebt.

Über die Auswahl des Fahrzeugs bestimmt die Stelle über die darin befindlichen Datenverarbeitungssysteme (Mittel) und kann spätestens bei der Rückgabe der Fahrzeuge über die Zwecke der darin gespeicherten personenbezogenen Daten entscheiden. Insbesondere bei Dienst- und Firmenwagen kommt hinzu, dass die jeweilige Behörde oder Firma gegenüber der betroffenen Person meist weisungsbefugt ist [19].

Unternehmen, Arbeitgeber und Dienstherren haben die datenschutzrechtlichen Vorschriften in Bezug auf die bei ihnen Beschäftigten zu erfüllen. Bereits bei der Anschaffung von Fahrzeugen ist darauf zu achten, dass die Einhaltung der datenschutzrechtlichen Vorschriften möglich ist. Dies ergibt sich neben Art. 6 DSGVO auch aus Art. 25 DSGVO. Danach hat der Verantwortliche schon bei der Festlegung der Mittel geeignete Maßnahmen zur Wahrung der Datenschutzgrundsätze zu treffen. Sehenden Auges ein Fahrzeug anzuschaffen, das nicht in der Lage ist, die Datenschutzgrundsätze, wie z.B. Rechtsgrundlage der Datenverarbeitung und Vertraulichkeit, einzuhalten, stellt einen Verstoß gegen diese Norm dar. Daneben kann der Einsatz von unsicheren Verarbeitungssystemen einen Verstoß gegen Art. 32 DSGVO darstellen. Danach muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Schutzniveau zu gewährleisten. Dies sollte der Verantwortliche bei der Anschaffung von Datenverarbeitungssystemen prüfen.

Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, z.B. Anwälte oder Ärzte nach § 203 StGB, müssen prüfen, ob sie durch eine Speicherung von Daten, z.B. Speicherung von Patientendaten im Telefonbuch des Fahrzeugs, einen Verstoß gegen ihre Sorgfaltspflichten begehen, insbesondere wenn die Gefahr besteht, dass andere Fahrer auf diese Daten zugreifen können. Auch wenn datenschutzrechtlich eine Verantwortung erst mit einer Erhebung bestünde, sollten Hersteller aus ihrer Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme und im Sinne einer Kundenfreundlichkeit darauf hinarbeiten, dass auch in dieser spezifischen Konstellation ein angemessener Schutz gewährleistet ist.

Wird das Fahrzeug wiederum allgemein beruflich oder im speziellen von Berufsgeheimnisträgern (z.B. Arzt, Anwalt) genutzt, und synchronisiert das Fahrzeug z.B. Adressdaten mit einer Cloud, kann dies eine unbefugte Übermittlung personenbezogener Daten darstellen, für die der Nutzer verantwortlich ist und für die der Cloud-Anbieter Auftragsdatenverarbeiter oder gemeinsam Verantwortlicher mit dem Nutzer wäre. Bei den Berufsgeheimnisträgern kann auch eine unbefugte Offenbarung von Geheimnissen vorliegen.

Denkbar ist, dass Fahrzeuge mit Sensoren Daten über die Umwelt speichern und als personenbezogene Daten vom Fahrzeug erhoben werden (z.B. über die Luftschnittstelle). Hierbei ist zu beachten, dass sich nur Daten bestimmter Sensoren für eine Personenbeziehbarkeit von Dritten eignen, insbesondere Video-Rohdaten. Daten der meisten Sensoren ermöglichen keine Personenbeziehbarkeit von Dritten, insbesondere Sensordaten von Radar, LiDAR (Laser-Abtastung), Infrarot, Ultraschall und anonymisierte Videodaten. Wie bereits im vorherigen Kapitel 6.1.3 ausgeführt, ist der Anwendungsbereich des Datenschutzrechts nur dann eröffnet, wenn die Tätigkeit nicht ausschließlich innerhalb einer persönlichen oder familiären Sphäre stattfindet [20]. Dies bedeutet, dass erst mit dem Verlassen der persönlichen oder familiären Sphäre der Anwendungsbereich eröffnet sein könnte. Wie oben im Kapitel 6.1.3 dargestellt ist umstritten, ob

[17] Vgl. zu § 1 Abs. 2 Nr. 3 BDSG: Simitis, in: Simitis, BDSG, § 1 Rn. 150, zu Art. 3 Abs. 2 RL 95/46/EG: EuGH, Urt. v. 06.11.2003, Az.: C-101/01

[18] Einer Meinung nach wird der persönliche und familiäre Bereich verlassen. Einer anderen Meinung nach ist die Sphärentheorie nicht als so weitreichend anzusehen, dass die Reparatur von privaten Gegenständen nicht mehr der Sphäre des Halters zuzuordnen ist. Zudem handle es sich auch nicht um Veröffentlichungen im Internet oder Videoaufnahmen und deshalb soll nach dieser Auffassung in diesem Fall das Haushaltprivileg Anwendung finden. Ob die Speicherung der privaten Daten in einer Public Cloud nicht mehr unter das Haushaltsprivileg fällt, wird sehr kontrovers diskutiert. Auch ist zu berücksichtigen, ob Daten gespeichert oder für Dritte veröffentlicht werden.

[19] Vgl. LAG Schleswig-Holstein: Urteil vom 20.01.2000 – Az.: 4 Sa 389/99, BeckRS 2000, 30814476

[20] EuGH, Urteil vom 11.12.2014, Az.: C-212/13, Rn. 33

die Sphäre verlassen wird, wenn Daten in den Zugriff Dritter gelangen, z.B. durch Übertragung über die Luftschnittstelle in eine Public Cloud, der Anwendungsbereich des Datenschutzrechts eröffnet sein könnte.

6.1.5. Anwendung auf den Kontext Fahrzeug

Nach der gemeinsamen Erklärung der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie[21] wird derjenige, der personenbezogene Fahrzeugdaten ausliest, d.h. erhebt, verantwortliche Stelle und die personenbezogenen Daten unterliegen ab diesem Zeitpunkt dem Geltungsbereich der DS-GVO.

Nach der oben genannten gemeinsamen Erklärung wird auf die Voraussetzung des Erhebens abgestellt. Eine Überlegung ist, dass die datenschutzrechtliche Interventionsrechte auf Auskunft, Berichtigung und Löschung, sowie Erklärungen und Widersprüche nur geltend gemacht werden können, wenn die verantwortliche speichernde Stelle bestimmbar ist. Stellt man auf das Fahrzeug selbst ab, könnte man vertreten, es fehle dem Halter an dem tatsächlichen und dem rechtlichen Erhebungswillen der Daten im Fahrzeug und den Verfügungsmöglichkeiten über diese Daten. Der Hersteller habe ohne Zugriffsmöglichkeit auf das Fahrzeug keine tatsächlichen Verfügungsmöglichkeiten über die Daten im Fahrzeug.

In Hinblick auf die Legaldefinition des Verantwortlichen in Art. 4 Nr. 7 DSGVO und die dort fehlende Anknüpfung an eine Erhebung bleibt abzuwarten, wie sich die Diskussion um die datenschutzrechtliche Verantwortlichkeit entwickeln wird. Es ist dann zu bestimmen, ob dieser Verantwortlicher, Auftragsverarbeiter oder einer von mehreren gemeinsam für die Verarbeitung Verantwortlichen ist. Unabhängig davon, ob der Hersteller Verantwortlicher im datenschutzrechtlichen Sinne ist, trifft ihn unter anderem nach dem Gedanken „Privacy by Design“ dennoch eine gewisse Verantwortung im Hinblick auf den Datenschutz.

Für die Bestimmung des Zeitpunkts der Datenerhebung durch eine verantwortliche Stelle lassen sich nach der oben genannten gemeinsamen Erklärung zwei Fallgruppen bilden:

In der ersten Fallgruppe geht es um Datenverarbeitungen, die lokal im Fahrzeug stattfinden. Dabei kann es sich z.B. um Fehlerspeicher, Entertainmentsysteme oder Müdigkeitssensoren ohne Online-Anbindung handeln. In der zweiten Fallgruppe werden Datenverarbeitungen mit Online-Anbindung behandelt. Dabei kann es sich z.B. um automatische Notrufsysteme, Entertainmentsysteme mit Online-Anbindung oder Parkplatzreservierungssysteme handeln.

6.1.5.1. Datenverarbeitungen ohne Online-Anbindung

Unter die erste Fallgruppe fallen sowohl Datenverarbeitungen in Fahrzeugen, die überhaupt keine Online-Anbindung verfügen (Offline-Fahrzeuge), als auch Datenverarbeitungen in Fahrzeugen mit Online-Anbindung, die das Fahrzeug nicht (z.B. durch Auslesen in der Werkstatt oder Übertragung über die Luftschnittstelle) verlassen. Wenn betroffene Person und Halter nicht identisch sind, könnte der Halter Verantwortlicher sein, wenn dieser über Zwecke und Mittel der Datenverarbeitung personenbezogener Daten entscheidet.

Handelt es sich bei der durch die Datenverarbeitung betroffenen Person um den Halter des Kraftfahrzeugs, gibt es für die lokal im Fahrzeug stattfindende Datenverarbeitung keine verantwortliche Stelle.

Betroffene Person ist, wer durch personenbezogene Daten identifiziert wird oder identifizierbar ist, Art. 4 Nr. 1 DSGVO. Halter ist, wer den Nutzen aus der Verwendung des Fahrzeugs zieht, für die Kosten des Fahrzeugs aufkommt und die Verfügungsgewalt über das Fahrzeug besitzt. Eigentümer und Halter müssen deshalb nicht identisch sein und auch die Zulassung auf eine bestimmte Person ist lediglich Indiz für die Haltereigenschaft. [22]. Im Folgenden wird der Halterbegriff in diesem Sinne verwendet. Von demjenigen, der die Verfügungsgewalt über das Fahrzeug besitzt, kann häufig angenommen werden, dass von ihm regelmäßig auch die Entscheidung über die Zwecke der Datenverarbeitung getroffen werden (So wohl auch Weichert, SVR 2016, 361, 364) und somit grundsätzlich in dieser Fallgruppe dafür verantwortlich ist.

Die Eigentümerstellung ist demgegenüber kein geeigneter Anknüpfungspunkt für die Bestimmung der Verantwortlichkeit. Selbst, wenn die betroffene Person das Fahrzeug erwirbt und der Verkäufer sich das Eigentum bis zur vollständigen Kaufpreiszahlung vorbehält oder z.B. einer Leasingbank Sicherungseigentum einräumt, dürfte weder Verkäufer noch Bank Verantwortlicher sein, da die Zugriffsmöglichkeiten auf das Fahrzeug stark eingeschränkt sind[23].

Wenn die Daten durch jemanden über eine Schnittstelle ausgelesen werden, wird derjenige nach der o.g. gemeinsamen Erklärung zur verantwortlichen Stelle. Hierbei sind verschiedene Sachverhalts-Konstellationen und datenschutzrechtliche Instrumente denkbar:

[21] Unabhängige Datenschutzbehörden des Bundes und der Länder/Verband der Automobilindustrie (VDA) Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge. 2016.

[22] OLG Köln, Beschluss vom 08.10.1993, Az.: Ss 414/93

[23] Faust BGB § 449. In Beck'scher Online-Kommentar BGB. Bamberger/Roth, 2015, 37. Edition Rn. 17-22.

- Die personenbezogenen Daten werden z.B. von einer Werkstatt ausgelesen und für eigene Zwecke verarbeitet.
- Die personenbezogenen Daten werden von einer Werkstatt als Auftragsverarbeiter nach Art. 28 DSGVO erhoben und für einen Auftraggeber als Verantwortlichen nach Art. 4 Nr. 7 DSGVO verarbeitet. Hierzu ist ein Vertrag nach Art. 28 DSGVO zu schließen.
- Die personenbezogenen Daten werden für eigene Zwecke erhoben und für bestimmte Zwecke an einen Dritten übermittelt.
- Zwei oder mehr Verantwortliche legen nach Art. 26 DSGVO gemeinsam die Mittel und Zwecke der Datenverarbeitung fest.
- Es werden keine personenbezogenen Daten erhoben, sondern nur anonyme Daten. Das Datenschutzrecht ist dann nicht anwendbar. Die Daten sind jedenfalls dann personenbezogen im Sinne des BDSG, wenn eine Verknüpfung mit der Fahrzeug-Identnummer (FIN) bzw. vehicle identification number (VIN) oder dem Kfz-Kennzeichen vorliegt[24] .

6.1.5.1.1. Datenschutzrechtliche Verantwortung des Herstellers Sofern der Hersteller bei Datenverarbeitungen ohne Online-Anbindung personenbezogene Daten aus dem Fahrzeug erhebt (insbesondere über die OBD-Schnittstelle am Fahrzeug) wird er nach der Gemeinsamen Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), 26.01.2016, verantwortliche Stelle. Zwar bestimmt der Hersteller durch die Entwicklung und die Konstruktion des Fahrzeugs die grundlegenden Abläufe der Datenverarbeitung im Fahrzeug, soweit er jedoch weder rechtliche noch tatsächliche Zugriffsmöglichkeiten auf die konkrete Datenverarbeitung im Kraftfahrzeug hat, kann er auch grundsätzlich nicht über die Zwecke der Datenverarbeitung bestimmen

Der Hersteller ist zwar nicht schon aufgrund seiner Stellung als Hersteller Verantwortlicher, allerdings unterliegt er in Einzelfällen nach der derzeit geltenden Rechtslage der Transparenzpflicht nach § 6c BDSG (vgl. Weichert, SVR 2016, 361, 365). Es ist fraglich, ob diese Vorschrift unter der Datenschutzgrundverordnung noch anwendbar sein wird. Die Verordnung selbst enthält keine entsprechende Regelung und für eine nationale Regelung scheint kein Raum mehr zu bestehen[25] .

Nach § 6c BDSG muss die „Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält“ gewisse Unterrichtungspflichten gegenüber der betroffenen Person erfüllen. Dazu gehört, der betroffenen Person nach § 6c Abs. 1 Nr. 2 BDSG über die Funktionsweise des Mediums in allgemeinverständlicher Form aufzuklären. Für § 6c BDSG müssen die ausgebende Stelle und der Verantwortliche dabei nicht identisch sein[26] , so dass eine Erstreckung auf den Hersteller erfolgen kann.

Der Begriff der mobilen personenbezogenen Speicher- und Verarbeitungsmedien des § 6c BDSG ist in § 3 Abs. 10 BDSG für das derzeit geltende nationale Recht definiert. Danach müssen drei Voraussetzungen gegeben sein: (i) Es müssen Datenträger sein, die an den Betroffenen ausgegeben werden, (ii) auf den Datenträgern darf nicht lediglich eine Speicherung, sondern darüber hinaus auch eine automatisierte Verarbeitung durch die ausgebende oder eine andere Stelle stattfinden und (iii) der Betroffene muss die Verarbeitung nur durch den Gebrauch des Mediums beeinflussen können.

Die erste Voraussetzung kann bei Fahrzeugen mit integrierten Speichern durchaus gegeben sein. Eigentumsrechtliche Fragen sind hier nicht maßgeblich, es kommt lediglich auf die tatsächliche Übergabe an[27] . Hauptanwendungsbereich der Norm sind Chipkarten, die über einen Mikroprozessor verfügen. Es wird vertreten, dass der Wortlaut technikoffen sei und daneben auch Chips in Betracht kommen, die in andere Objekte integriert sind[28] . Nicht anwendbar ist die Norm auf reine Speichermedien, auf denen keine weitergehende Verarbeitung der Daten erfolgen kann. Damit kommen grundsätzlich solche Komponenten eines Fahrzeugs in Betracht, die über Mikroprozessoren verfügen (zweite Voraussetzung der Norm).

Die dritte Voraussetzung soll nach dem Willen des Gesetzgebers nicht erfüllt sein, wenn der Benutzer die Verarbeitungsvorgänge auf vielfältige Art und Weise steuern kann. Das soll z.B. bei Notebooks und Mobiltelefonen der Fall sein, nicht jedoch, wenn der Betroffene lediglich z.B. durch Tasten am Lesegerät die Auswahl zwischen wenigen vorgegebenen Alternativen trifft [29]. Bei komplexen Systemen kann und muss danach abgegrenzt werden, welche Bereiche der Hard- und Software der Betroffene steuert und welche er lediglich gebraucht[30][31]. Bei Datenverarbeitungsvorgängen im Fahrzeug hat

[24] Verband der Automobilindustrie (VDA) Datenschutz-Prinzipien für vernetzte Fahrzeuge. 2014 ⟨URL: https://www.vda.de/dam/vda/Medien/DE/Themen/Innovation-und-Technik/Vernetzung/Datenschutz-Prinzipien/VDA-Datenschutz-Prinzipien-2014/vda-datenschutzprinzipien-2014.pdf⟩.

[25] Kühling, Jürgen et al. DIE DATENSCHUTZ-GRUNDVERORDNUNG und DAS NATIONALE RECHT. 2016 S. 348.

[26] Scholz BDSG § 6c. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage Rn. 23.

[27] Scholz BDSG § 3. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage Rn. 269.

[28] Scholz BDSG § 3. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage Rn. 267.

[29] Deutscher Bundestag, Drucksache 14/5793, S. 60

[30] Hornung, Gerrit Der Personenbezug biometrischer Daten. Datenschutz und Datensicherheit (DuD) 28 2004, Nr. 7.

[31] Scholz BDSG § 3. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage Rn. 277 m.w.N..

der Fahrer aber an vielen Stellen keine Steuerungsmöglichkeit[32] .

§ 6c BDSG kann damit grundsätzlich auf diejenigen Datenspeicher mit Verarbeitungsfunktionen in Fahrzeugen anwendbar[33], bei denen keine Steuerungsmöglichkeit durch den Benutzer vorliegt. Es ist jeweils im Detail zu prüfen, ob alle Voraussetzungen des § 6c BDSG für den spezifischen Sachverhalt vorliegen.

6.1.5.1.2. Gewährleistungsrechtliche Verantwortung des Verkäufers Der Verkäufer ist ebenfalls nicht lediglich aufgrund seiner Verkäuferstellung Verantwortlicher nach Art. 4 Nr. 7 DSGVO.

Es wird die Ansicht vertreten, dass der Verkäufer aus gewährleistungsrechtlichen Gesichtspunkten darauf zu achten hat, den Käufer hinreichend über Datenverarbeitungsvorgänge im Fahrzeug zu informieren, wenn diese über die „übliche Beschaffenheit“ nach § 434 Abs. 1 Nr. 2 BGB (Bürgerliches Gesetzbuch) hinausgeht. So könnte eine Datenverarbeitung im Fahrzeug eine Abweichung von der üblichen Beschaffenheit nach § 434 Abs. 1 Nr. 2 BGB (Bürgerliches Gesetzbuch) darstellen. [34] Der Begriff der „üblichen Beschaffenheit“ steht im Wandel und könnte mit stärkerer Vernetzung von Fahrzeugen anders interpretiert werden. Werden die Beschaffenheit und damit die Datenverarbeitungssysteme im Fahrzeug allerdings vereinbart, ist das Fahrzeug in dieser Hinsicht nach § 434 Abs. 1 S. 1 BGB frei von Sachmängeln.

Auf die datenschutzrechtliche Zulässigkeit hat die Verbreitung oder Üblichkeit von Datenverarbeitungsvorgängen im Fahrzeug keine Auswirkungen.

6.1.5.2. Datenverarbeitungen mit Online-Anbindung

Der Verantwortliche ist einfacher zu bestimmen, wenn eine Datenverarbeitung mit Online-Anbindung vorliegt, somit Daten beim Online-Fahrzeug über die Luftschnittstelle von einer verantwortlichen Stelle erhoben werden. Sofern die Stelle über die Mittel und Zwecke entscheiden kann, ist sie für die erhobenen Daten verantwortliche Stelle, Art. 4 Nr. 7 DSGVO. Wie bei den Datenverarbeitungen ohne Online-Anbindung können verschiedene Konstellationen vorliegen (z.B. Datenverarbeitung mit Einbeziehung eines Auftragsverarbeiters oder eine Datenverarbeitung durch zwei oder mehrere gemeinsam für die Verarbeitung Verantwortliche).

In der Regel werden bei Online-Fahrzeugen die Hersteller oder ggf. dritte Dienste-Anbieter personenbezogene Daten erhalten und damit als verantwortliche Stelle anzusehen sein. Insbesondere, wenn Hersteller Zusatzdienstleistungen für das Fahrzeug anbieten und dabei in ihren Backend-Servern Daten speichern, sind sie verantwortliche Stelle für diese Datenverarbeitungen.[35]

Fraglich ist, ob der Hersteller auch für die Datenverarbeitungen im Fahrzeug verantwortliche Stelle ist, die gerade nicht erhoben werden, wenn er über eine Softwareupdatefunktion über die Luftschnittstelle („Over-the-air“) weitreichende Modifikationen an der Datenverarbeitung im Fahrzeug vornehmen könnte.[36] . Andererseits könnte es nach der gemeinsamen Erklärung darauf ankommen, welche Daten aus dem Fahrzeug erhoben werden und dass die verantwortliche Stelle eine rechtliche Legitimierung für deren Erhebung hat.

6.1.5.3. Zwischenfazit

Eine Frage für die Anwendbarkeit des Datenschutzrechts ist, ob die Ausnahme nach Art. 2 Abs. 2 c) DSGVO vorliegt, es sich also um eine ausschließlich persönliche oder familiäre Tätigkeit handelt. Ist dies nicht der Fall, kann das Datenschutzrecht anwendbar sein.

Die Verantwortlichkeit für datenverarbeitende Fahrzeuge kann nicht durch pauschale Zuweisungen bestimmt werden. Es hat sich gezeigt, dass bei der Datenverarbeitung ohne Online-Anbindung zwei Unterfallgruppen zu unterscheiden sind. Solange die betroffene Person und der Halter, also die Person, die regelmäßig wegen ihrer Verfügungsmacht über das Fahrzeug auch über die Zwecke der Datenverarbeitung bestimmt, identisch sind, gibt es für die im Fahrzeug stattfindende Datenverarbeitung grundsätzlich keinen Verantwortlichen.

[32] Vgl. in: ADAC Wo Ihr Auto überall Daten speichert . August 2016.

[33] Hornung, Gerrit Verfügungsrechte an fahrzeugbezogenen Daten. Datenschutz und Datensicherheit, 39 2015, Nr. 6 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0430-8⟩.

[34] Vgl. hierzu OLG Hamm, Beschluss v. 28.07.2015 und Beschluss v. 02.07.2015, Az.: 28 U 46/15. Das OLG Hamm sah einen Sachmangel im konkreten Fall nicht als gegeben an, ein Sachmangel könnte aber gegeben sein, wenn eine „nicht beeinflussbare Weiterleitung personenbezogener Daten von dem Fahrzeug an unbefugte Dritte zu befürchten stünde“.

[35] vgl. in: Hansen, Marit Das Netz im Auto & das Auto im Netz. Datenschutz und Datensicherheit, 39 2015, Nr. 6 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0431-7⟩.

[36] Vgl. in: Weichert BDSG § 3. In Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG. Däubler/Klebe/Wedde/Weichert, 2013, 3. Auflage.

Werden neben Daten des Halters auch Daten Dritter verarbeitet, etwa weil Sensoren auf die Außenwelt gerichtet sind oder eine andere Person als der Halter das Fahrzeug fährt, kann der Halter Verantwortlicher im Sinne des Datenschutzrechts sein.

Es ist dann zu prüfen, ob eine Verarbeitung [37], insbesondere eine Erhebung, vorliegt[38] . Bei Offline-Fahrzeugen erfolgt dies im Regelfall über die OBD-2 Buchse erfolgen, bei Online-Fahrzeugen ist zu prüfen, ob die Datenverarbeitung rein im Fahrzeug abläuft, oder ob und welche Daten z.B. über die Luftschnittstelle vom Fahrzeug erhoben werden.

Hierbei wird im Regelfall der Empfänger der personenbezogenen Daten auch Verantwortlicher sein.

Es ist aber auch möglich und anhand der allgemeinen datenschutzrechtlichen Maßstäbe zu prüfen, ob die Voraussetzungen einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO oder durch einer Verarbeitung im Auftrag nach Art. 28 DSGVO vorliegen.

6.1.6. Mögliche Rechtsgrundlagen

Die Datenverarbeitung ist nur dann rechtmäßig, wenn eine Rechtsgrundlage die Verarbeitung rechtfertigt oder eine wirksame Einwilligung vorliegt. Dieser bewährte Regelung, die als Verbot mit Erlaubnisvorbehalt bekannt ist[39], bleibt auch unter der Datenschutz-Grundverordnung erhalten. Nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung nur rechtmäßig, wenn eine der dort genannten Rechtsgrundlagen vorliegt.

Nachfolgend wird deshalb untersucht, welche Rechtsgrundlagen für die Datenverarbeitung im Zusammenhang mit Fahrzeugen in Betracht kommen oder ob die Verarbeitung auf eine Einwilligung gestützt werden kann.

6.1.6.1. Einwilligung

Die Einwilligung ist ein mögliches Instrument zur Rechtfertigung der Verarbeitung von personenbezogenen Daten und wird in Art. 6 (1) a) DSGVO als mögliche Rechtsgrundlage genannt. Die Bedingungen für eine wirksame Einwilligung sind in Art. 7 DSGVO näher geregelt.

Eine Schriftform, von der man nach dem § 4 I S. 3 BDSG nur in Ausnahmefällen oder bei einer elektronischen Einwilligung abweichen durfte, ist nach der Datenschutz-Grundverordnung nicht mehr gefordert. Allerdings muss nach Art. 7 Abs. 1 DSGVO der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung eingewilligt hat. Insbesondere, wenn die Einwilligung elektronisch eingeholt werden soll, ist dem Verantwortlichen hier zu raten, ein entsprechend beweissicheres technisches Verfahren zu betreiben.

Art. 7 Abs. 2 DSGVO sieht vor, dass die Einwilligungserklärung, wenn sie auch andere Sachverhalte betrifft, in einer klaren und einfachen Sprache erfolgen muss und von den anderen Sachverhalten klar zu unterscheiden ist.

Nach Art. 7 Abs. 3 DSGVO hat die betroffene Person die Möglichkeit, die Einwilligung mit Wirkung für die Zukunft jederzeit zu widerrufen. Das bedeutet für das technische Verfahren, dass es über Möglichkeiten verfügen muss, einen solchen Widerruf zu berücksichtigen, indem die personenbezogenen Daten, die aufgrund dieser Einwilligung verarbeitet wurden, gelöscht oder anonymisiert werden und eine weitere Erhebung ausgeschlossen wird. Dies hat solange nicht zu erfolgen, sofern der Verantwortliche eine andere Rechtsgrundlage für die Datenverarbeitung hat.

Insbesondere wegen der jederzeitigen Widerrufsmöglichkeit ist die Einwilligung als Legitimationsmodell nur in Einzelfällen für Geschäftsmodelle geeignet. Die verantwortliche Stelle könnte sich in der Situation widerfinden, Daten für die Erfüllung eines Vertrages verarbeiten zu müssen und dies als Recht für den Kunden vertraglich vereinbart zu haben, aber durch einen Widerruf einer Einwilligung die Legitimation der Datenverarbeitung zu verlieren und den Vertrag mit dem Kunden nicht mehr einhalten zu können.

Es wird diskutiert, ob es möglich ist, dass für dieselbe Datenverarbeitung neben der Einwilligung weitere Rechtsgrundlagen parallel angewendet werden können[40] oder ob dies die Informiertheit der Einwilligung beeinträchtigt, da der Betroffene dann nicht weiß, ob er überhaupt eine Wahl hat und was die Folgen eines Widerrufs sind.

Nach Art. 7 Abs. 3 S. 4 DSGVO muss der Widerruf der Einwilligung so einfach sein, wie die Erteilung der Einwilligung. Dies ist vergleichbar mit der Regelung in § 309 Nr. 13 BGB, welche hohen Formerfordernissen bei der Kündigung von Verbraucherverträgen Grenzen aufzeigt. Damit wird die verbreitete Praxis, Verbraucher durch hohe Kündigungshürden,

[37] Vgl. Legaldefinition in Art. 4 Nr. 2 DSGVO

[38] Unabhängige Datenschutzbehörden des Bundes und der Länder/Verband der Automobilindustrie (VDA) Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge. 2016.

[39] Scholz/Sokol BDSG § 4. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage Rn. 3.

[40] Däubler BDSG § 4a. In Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG. Däubler/Klebe/Wedde/Weichert, 2014, 4. Auflage Rn. 35.

insbesondere durch die Vorgabe von Formerfordernissen in Verträgen zu halten auch für den Bereich des Datenschutzrechts antizipiert. Bezogen auf den Kontext des Fahrzeugs kann dies bedeuten, dass eine Einwilligung, die z.B. über das Multimediasystem/Head-Unit des Fahrzeugs eingeholt wurde „genauso einfach“ auch widerrufen werden können muss.

Darüber hinaus kann Erwägungsgrund Nr. 32 zur Interpretation herangezogen werden. „Die Einwilligung sollte durch eine bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Nicht ausreichend sollen bereits vorab angekreuzte Kästchen, Untätigkeit oder Stillschweigen sein. Für das vernetzte Fahrzeug kann dies bedeuten, dass lediglich das Führen eines datenverarbeitenden Fahrzeugs durch eine betroffene Person keine Einwilligung darstellt.

Für die Beurteilung der Freiwilligkeit ist nach Art. 7 Abs. 4 DSGVO „in größtmöglichem Umfang“ zu berücksichtigen, ob die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung von einer Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht wird, obwohl diese Daten hierfür nicht erforderlich sind. Dies bedeutet, dass die Freiwilligkeit der Einwilligung dadurch entfallen kann, dass die Abgabe der Einwilligung mit einem Vertrag über eine Dienstleistung gekoppelt ist, aber durch sie eine Datenverarbeitung gerechtfertigt werden soll, die für die Erbringung einer Dienstleistung nicht erforderlich sind. Diese Vorschrift dürfte solche Geschäftsmodelle betreffen, bei denen die Anbieter sich umfangreiche Rechte an den personenbezogenen Daten einräumen lassen[41] .

Die Freiwilligkeit der Einwilligung ist auch problematisch, wenn sie innerhalb eines Arbeitsverhältnisses eingeholt wird. Es handelt sich bei Arbeitsverhältnissen um Abhängigkeitsverhältnisse, weil die betroffenen Personen existenziell auf dieses Verhältnis angewiesen sind[42] . Entsprechend kritisch sind solche Einwilligungen in Arbeitsverhältnissen zu sehen. Nach Erwägungsgrund Nr. 155 ist die Einwilligung im Arbeitsverhältnis unter Geltung der DSGVO indes nicht grundsätzlich ausgeschlossen, vielmehr obliegt es den Mitgliedsstaaten hierfür Bedingungen festzulegen[43] . Dabei ist die Problematik der Abhängigkeit des Arbeitnehmers von seinem Arbeitgeber angemessen in der gesetzgeberischen Abwägung zu berücksichtigen. Die weitere Rechtsgrundlage, auf die ein Arbeitgeber sich derzeit berufen kann, § 32 BDSG, wird nachfolgend im Zusammenhang mit den sonstigen Rechtsgrundlagen noch erörtert. Wie die Umsetzung der DSGVO in diesem Punkt aussehen wird, bleibt abzuwarten.

Bei der Beurteilung der Freiwilligkeit sind die Umstände des konkreten Sachverhalts zu berücksichtigen. So könnte die Freiwilligkeit fehlen, wenn ohne eine Wahl zu haben in einem hypothetischen Fall eine betroffene Person ein Fahrzeug nur dann starten könnte, wenn sie in bestimmte Datenverarbeitungsvorgänge einwilligt.

Erwägungsgrund 43 S. 2 DSGVO stellt weitere Anforderungen an die Freiwilligkeit der Einwilligung in der Hinsicht, dass verschiedene Verarbeitungsvorgänge auch einer gesonderten Einwilligung bedürfen, wenn dies im Einzelfall angebracht ist. Damit soll sichergestellt werden, dass der Nutzer nicht nur in ein Bündel von Datenverarbeitungsvorgängen einwilligen kann[44] . Für die Einwilligung in Datenverarbeitungen im Zusammenhang mit Fahrzeugen muss jeweils geprüft werden, ob es „im Einzelfall angebracht ist“, dass eine gesonderte Einwilligung für den jeweiligen Verarbeitungsvorgang existiert oder die „gebündelte“ Einwilligung mehrere verschiedene Verarbeitungsvorgänge umfassen darf. Es ist auch auf eine transparente und nachvollziehbare Form zu achten.

Fraglich ist hierbei aus welcher Sicht die Beurteilung des „angebracht“ sein erfolgen muss. Aus Sicht der betroffenen Person und deren Schutzbedarf bei der Abgabe von Einwilligungen könnte man darauf abstellen, ob die betroffene Person ein Interesse hat, in die eine Datenverarbeitung einzuwilligen, in die andere jedoch nicht. Eine andere Auslegungsmöglichkeit wäre, dass technische Zwänge bei der Abwägung zu berücksichtigen sind.

Ein weiteres Problem stellen Drittbetroffene[45] dar, zu denken ist z.B. an andere Fahrer eines Fahrzeugs, Mitfahrer, Fußgänger und Fahrer[46] . Wird eine Datenverarbeitung auf Einwilligungen der betroffenen Personen gestützt, kann nur jede betroffene Person für sich selbst einwilligen bzw. die Eltern für das Kind nach Art. 8 Abs. 1 S. 2 DSGVO. Um bei einem vernetzten Fahrzeug die Rechtmäßigkeit der Datenverarbeitung nachweisen zu können, ist zu berücksichtigen, dass diese Fahrzeuge häufig von mehreren Personen genutzt werden. Wenn es einen Verantwortlichen gibt und die Anwendbarkeit des Datenschutzrechts gegeben ist, muss bei einer Datenverarbeitung, die sich auf eine Einwilligung stützt, sichergestellt sein, dass die Einwilligung aller betroffener Personen vorliegt. Wenn diese Datenverarbeitung über die Einwilligung gerechtfertigt werden soll, stellt sich die Frage, wie dies noch praktikabel umgesetzt werden soll.

Im Kontext des autonomen Fahrens gilt es noch verschiedene datenschutzrechtliche Fragen zu klären. So müssen für die

[41] Schantz, Peter Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016, Nr. 26.
[42] Scholz BDSG § 4a. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage Rn. 62.
[43] Schantz, Peter Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016, Nr. 26.
[44] Schantz, Peter Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016, Nr. 26.
[45] allgemein zur Problematik der Drittbetroffenen: in: Cebulla Umgang mit Kollateraldaten - Datenschutzrechtliche Grauzone für verantwortliche Stellen. ZD Heft 11 2015.
[46] vgl. in: Weichert, Thilo Datenschutz im Auto – Teil 1. SVR, 2014, Nr. 6.

Bestimmung des Fahrzeugs im Raum und die Berechnung der weiteren Fahrroute Sensoren auf die Umwelt des Fahrzeugs gerichtet werden. Aber es ist unmöglich, von jedem Passanten vor der Vorbeifahrt eine Einwilligung einzuholen. Andererseits ist bei § 6c BDSG nur eine Abwägung durchzuführen und im Sinne einer datenschutzfreundlichen Umsetzung ist es denkbar, dass Video-Rohdaten auf die für die Beurteilung des Straßenverkehrs wesentlichen Objekte reduziert werden und man deshalb insoweit von einer Anonymisierung sprechen könnte.

6.1.6.2. Verarbeitung zur Erfüllung eines Vertrages

Die Verarbeitung kann nach Art. 6 Abs. 1 b) DSGVO darauf gestützt werden, dass sie für die Erfüllung eines Vertrages, dessen Partei die betroffene Person ist, erforderlich ist. Erforderlich bedeutet hier, dass der Vertrag ohne die Verarbeitung nicht sinnvoll erfüllt werden kann. Dabei ist für jedes Datum zu prüfen, ob eine Vertragserfüllung auch ohne dieses Datum sinnvoll möglich ist. Nur wenn dies nicht der Fall ist, kann die Erforderlichkeit bejaht werden. Die Datenschutz-Grundverordnung stellt in Art. 6 Abs. 1 lit. b DSGVO fest, dass die betroffene Person Vertragspartei sein muss. Ein Vertrag zwischen A und B kann also keine Grundlage für die Erhebung von personenbezogenen Daten des Dritten C sein.

Die Rechtsgrundlage löst für den Verantwortlichen das Problem, dass eine bestimmte zwischen den Parteien als Rechte und Pflichten vereinbarte Leistungserfüllung der Verarbeitung von Daten bedarf, aber bei einer freiwilligen Einwilligung die betroffene Person jederzeit durch ihren einseitigen Widerruf der Datenverarbeitung die Rechtsgrundlage entziehen könnte, aber weiterhin das Leistungsversprechen besteht. Durch Art. 6 Abs. 1 b) DSGVO können personenbezogene Daten ohne gesonderte Einwilligung verarbeitet werden, sofern dies im Rahmen der Rechte und Pflichten für den Vertrag erforderlich ist.

Beispielsweise ist es bei einer Vereinbarung, in der sich ein Diensteanbieter gegenüber dem Kunden verpflichtet hat, den Kilometerstand des Fahrzeugs in einer App darzustellen, notwendig, dass das über die Fahrzeug-Identifizierungsnummer (FIN) personenbeziehbare Datum „KM-Stand“ aus dem Fahrzeug über die Luftschnittstelle erhoben wird und im Backend so verarbeitet wird, dass der Kunde des Vertrags den KM-Stand in der App abrufen kann.

Der Vertrag unterliegt ggf. den inhaltlichen Einschränkungen für Allgemeine Geschäftsbedingungen nach § 305ff BGB.

6.1.6.3. Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung

Beim eCall- Dienst wird entweder durch einen Sensor registriert, ob es zu einem Unfall kam und automatisch ein Notruf zu einer Notrufzentrale abgegeben oder manuell durch einen Schalter im Fahrzeug ein Notruf abgesetzt. Die eCall-Verordnung [47] verweist jedoch lediglich in Art. 6 darauf, dass Verarbeitung personenbezogener Daten in Übereinstimmung mit dem Datenschutzrecht zu erfolgen hat. Ob in der Verordnung der eCall-Dienst eine eigene Rechtsgrundlage enthalten ist, ist umstritten.

Die Verordnung 2015/758 über die EG-Typengenehmigung für bordeigene eCall-Systeme enthält in Art. 6 weitere Regelungen zum Datenschutz. So ist dort eine strikte Zweckbindung der personenbezogenen Daten für Notfallsituationen, das Verbot einer dauernden Verfolgung und die kontinuierliche Löschung der Daten im internen Speicher und Transparenzpflichten geregelt.

6.1.6.4. Verarbeitung zur Erfüllung von lebenswichtigen Interessen

Nach Art. 6 Abs. 1 d) DSGVO dürfen personenbezogene Daten verarbeitet werden, wenn dies erforderlich ist, „um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“. Nach Erwägungsgrund 46 soll diese Rechtsgrundlage bezüglich Interessen einer anderen natürlichen Person grundsätzlich nur dann zur Anwendung kommen, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Als Beispiele werden die Überwachung von Epidemien und Naturkatastrophen genannt.

In der Literatur wird vertreten, dass die Norm dem Schutz bestimmter höchstpersönlicher Rechtsgüter dient. Es sei objektiv zu beurteilen, ob diese betroffen seien und stehe nicht zur Disposition der betroffenen Personen oder des Verantwortlichen[48] .

Vom Wortlaut der Norm ausgehend, kommen im Hinblick auf das vernetzte Fahrzeug solche Verarbeitungsvorgänge in Betracht, die unmittelbar für die Sicherheit im Straßenverkehr erforderlich sind. Fraglich ist, inwieweit die Norm einschränkend auszulegen ist. Eine Interessensabwägung oder Verhältnismäßigkeitsprüfung ist kein Tatbestandsmerkmal

[47] Delegierte Verordnung (EU) Nr. 305/2013 der Kommission vom 26.November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes

[48] Frenzel Art. 6. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 20.

dieser Erlaubnisnorm. Der Verordnungsgeber scheint offensichtlich davon ausgegangen zu sein, dass bei einer Situation, in der es um die lebenswichtigen Interessen der betroffenen Person geht, dieses Interesse stets überwiegt. Allerdings ist die Norm entsprechend eng auszulegen, um den Anwendungsbereich nicht unverhältnismäßig weit auszudehnen.

6.1.6.5. Erforderlich zur Erfüllung einer Aufgabe im öffentlichen Interesse

Fraglich ist, wie weit Art. 6 e) auszulegen ist. Danach kann eine Verarbeitung gerechtfertigt werden, wenn sie für eine Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung einer öffentlichen Aufgabe erfolgt, die dem Verantwortlichen übertragen wurde. Die erste Alternative könnte nach ihrem Wortlaut für die Datenverarbeitung im und um das vernetzte Auto einen weiten Anwendungsbereich finden. So liegt es z.B. im öffentlichen Interesse, das Problem der Parkplatzknappheit in deutschen Innenstädten zu entschärfen oder Verkehrsströme effizient zu lenken. Aus der unterschiedlichen Formulierung der beiden Alternativen ergibt sich auch, dass die erste Alternative nicht auf öffentliche Aufgaben, also solche, deren Erfüllung grundsätzlich dem Staat obliegt, begrenzt ist[49]. Für die erste Alternative ist lediglich erforderlich, dass es sich um eine Aufgabe im öffentlichen Interesse handelt, während die zweite Alternative das Vorliegen einer öffentlichen Aufgabe als Tatbestandsmerkmal fordert.

Im Sinne der Bestimmtheit kann der Anwendungsbereich der Norm nicht so weit gehen, dass alle Belange, die irgendwie die Öffentlichkeit und nicht nur Privatinteressen berühren, gerechtfertigt werden können. Nach Erwägungsgrund Nr. 10 sollen die Mitgliedstaaten „die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen“. Der nationale Gesetzgeber hat hier also die Möglichkeit, die Voraussetzungen „zu konkretisieren, d.h. anzupassen und auszufüllen“[50] .

6.1.6.6. Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten

Nach Art. 6 Abs. 1 f) DSGVO kann die Verarbeitung darauf gestützt werden, dass sie erforderlich zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Jedes rechtlich anerkanntes Interesse ist ein berechtigtes Interesse (Vgl. zu § 28 Abs. 1 Nr. 2 BDSG: Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 24). Dieses Tatbestandsmerkmal erfüllt daher kaum eine eingrenzende Funktion. Um eine Verarbeitung auf diese Rechtsgrundlage stützen zu können, liegt der Schwerpunkt der Prüfung daher bei der Erforderlichkeit und der Interessenabwägung.

Selbst wenn ein berechtigtes Interesse des Verantwortlichen vorliegt, können die Voraussetzungen dieser Rechtsgrundlage nicht gegeben sein, weil eine Abwägung ergibt, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person die berechtigten Interessen überwiegen. Aus dem Wortlaut der Norm kann sich eine Darlegungslast zu Ungunsten der betroffenen Person ergeben[51]. Um ein Überwiegen der Betroffeneninteressen zu vermeiden, kommen insbesondere technische Maßnahmen in Betracht, die geeignet sind, die Eingriffsintensität auf Seiten der betroffenen Personen herabzusenken. An diesem Maßstab wäre dann auch zu prüfen, ob diese Norm für Datenverarbeitungen im Zusammenhang mit vernetzten Fahrzeugen vorliegt.

6.1.6.7. Beschäftigtendatenschutz

Beschäftigtendatenschutz ist sowohl im BDSG als auch in der Datenschutz-Grundverordnung in einer eigenen Norm geregelt. Der Beschäftigtendatenschutz kann nach Art. 88 DSGVO weiterhin durch die Mitgliedsstaaten geregelt werden. § 32 BDSG, der den Beschäftigtendatenschutz aktuell regelt, kann daher erhalten bleiben[52] . Eine solche bereichsspezifische Regelung ist auch notwendig, da Arbeitsverhältnisse einerseits durch ein Ungleichgewicht zwischen Beschäftigten und Arbeitgebern gekennzeichnet sein können und andererseits viele Stellen, insbesondere Arbeitgeber, Dienstherren und staatliche Stellen, ein hohe Informationserwartung haben. Besonders für Arbeitgeber kann es von Interesse sein sein, Arbeitsleistungen zu kontrollieren und hierbei elektronische Datenverarbeitungen zu nutzen (vgl. Seifert, in: Simitis, BDSG, 8. Aufl. 2014, § 32 Rn. 4 ff.).

[49] Frenzel Art. 6. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 23.

[50] Kühling, J./Martini, Mario/Johanna, Heberlein Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf. http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf S. 28.

[51] Frenzel Art. 6. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 31.

[52] Kühling, J./Martini, Mario/Johanna, Heberlein Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf. http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf S. 450.

Nach § 32 BDSG dürfen personenbezogene Daten „für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist“. § 3 Abs. 11 BDSG definiert den Begriff der Beschäftigten näher. Der Datenschutz wird durch die Nennung der Bewerberinnen und Bewerber und die Personen, deren Beschäftigungsverhältnis beendet ist, auch auf die Zeit vor Beginn und nach Ende des Arbeits- oder Dienstverhältnisses erstreckt[53] . Für Dienstwagen bedeutet das, dass personenbezogene Daten auch nach dem Ende eines Arbeits- oder Dienstverhältnisses dieser Norm unterliegen und die nachfolgenden Voraussetzungen einzuhalten sind.

Auch hier ist der zentrale Begriff die Erforderlichkeit. Erforderliche Datenverarbeitungen sind solche, die nicht lediglich nützlich, sondern geboten sind. Die Erforderlichkeit ist daher zu verneinen, wenn zwischen mehreren gleich effektiven Maßnahmen nicht die am wenigsten belastende gewählt wurde. Im Rahmen einer Interessenabwägung ist darüber hinaus festzustellen, ob die Interessen des Arbeitgebers die Interessen des Arbeitnehmers überwiegen[54] . Es ist also vom Arbeitgeber zu prüfen, ob diese Voraussetzung für den Einsatz vernetzter Fahrzeuge in jedem Einzelfall gegeben ist.

Soweit Funktionen des vernetzten Fahrzeugs dazu bestimmt sind, den Arbeitnehmer zu überwachen, muss § 87 Betriebsverfassungsgesetz beachtet werden. Danach hat der Betriebsrat ein Mitbestimmungsrecht bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Bei Beschäftigten im öffentlichen Dienst sehen die Mitbestimmungsgesetze entsprechende Vorbehalte zu Gunsten der Personalräte vor.

6.1.7. Informationspflichten

Weiterhin ist zu untersuchen, welche Informationen den betroffenen Personen nach der Datenschutz-Grundverordnung zur Verfügung gestellt werden müssen. Diese Fragen sind in Art. 13 und 14 DSGVO geregelt. Art 13 regelt die Informationspflichten, für Datenerhebungen direkt bei der betroffenen Person. Art. 14 regelt die Informationspflichten, die erfüllt werden müssen, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben werden. Für beide Normen gelten gemäß Art. 12 Abs. 1 DSGVO, dass die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln sind.

Die Begriffe sind nicht gesetzlich definiert. In der Literatur wird vertreten, „Präzise“ bedeute inhaltliche Richtigkeit und Vollständigkeit[55] , „Transparenz“ soll durch die Informationen hergestellt werden und enthalte somit keine eigenen Anforderungen an die Information selbst[56] . Verständlichkeit sei durch eine adressatengerechte Kommunikation erreicht, wobei für Adressaten mit unterschiedlichem Wissensstand mehrschichtige Informationen erforderlich sein können[57] . „Leichte Zugänglichkeit“ sei gegeben, wenn betroffene Personen mit den ihnen zur Verfügung stehenden Mitteln auf die Informationen zugreifen kann. Ebenfalls wird vertreten, dass wenn Informationen in elektronischer Form übermittelt werden, diese durch gängige Software visualisierbar sein müsse[58].

6.1.7.1. Erhebung von personenbezogenen Daten bei der betroffenen Person

Nach Art. 13 Abs. 1 DSGVO muss der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung gewisse Informationen mitteilen.

Dabei handelt es sich um

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“.

Wenn die Verarbeitung darauf gestützt wird, dass berechtigte Interessen des Verantwortlichen oder eines Dritten die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen[59], muss die betroffene Person über die Interessen des Verantwortlichen oder eines Dritten informieren werden.

[53] Gola/Klug/Körffer § 32. In BDSG. Gola/Schomerus, 2015, 12. Aufl. Rn. 1.
[54] Gola/Klug/Körffer § 32. In BDSG. Gola/Schomerus, 2015, 12. Aufl. Rn. 10.
[55] Paal Art. 12. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 28.
[56] Paal Art. 12. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 29.
[57] Paal Art. 12. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 30, 31.
[58] Paal Art. 12. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1 Rn. 32.
[59] Art. 6 Abs. 1 f) DSGVO

Wenn Daten von dem Verantwortlichen an eine andere Stelle übermittelt werden, muss der Empfänger oder die Kategorie von Empfängern angegeben werden.

Sollen Daten an ein Drittland übermittelt werden, ist darüber zu informieren, ob die Kommission beschlossen hat, dass das Datenschutzniveau in diesem Land als angemessen einzustufen ist oder nicht. Liegt ein solcher Beschluss nicht vor, muss darüber informiert werden, welche geeigneten Garantien zum Schutz der personenbezogenen Daten vorliegen.

In Abs. 2 ist normiert, welche weiteren Informationen für eine faire und transparente Verarbeitung erforderlich sind.

Das sind:

- die Dauer der Speicherung
- falls die Dauer noch nicht festgelegt werden kann, die Kriterien, nach denen die Dauer bestimmt wird
- Informationen über die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit
- das Recht, die Einwilligung zu widerrufen
- die Möglichkeit, sich bei einer Aufsichtsbehörde zu beschweren
- „e) 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 mögliche Folgen die Nichtbereitstellung hätte“
- ob eine automatisierte Entscheidungsfindung, einschließlich Profiling, stattfindet. Ist dies der Fall, müssen „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Personen“ erteilt werden. Ob ein Profiling vorliegt, ist gemäß Art. 4 Nr. 4 DSGVO danach zu bestimmen, ob die Daten dazu verwendet werden, bestimmten persönliche Aspekte einer Person zu bewerten oder vorherzusagen. Dies ist im Rahmen des vernetzten Autos z.B. bei sogenannten Pay as you drive-Versicherungen der Fall, bei denen anhand des Fahrverhaltens entschieden wird, ob einem Versicherten gegebenenfalls ein Rabatt gewährt wird.

Im Falle einer Zweckänderung müssen die Informationen, die in Abs. 2 genannt werden, erteilt werden, Art. 13 Abs. 3 DSGVO.

Die Informationspflicht entfällt nach Art 13 Abs. 4 DSGVO soweit die betroffene Person bereits informiert ist. Um feststellen zu können, ob eine betroffene Person bereits informiert ist, müsste aber eine Verkettbarkeit zwischen der ersten Information und späteren Erhebungen bestehen.

Hierbei kann man der Ansicht sein, dass wenn eine Verkettung für die Verarbeitung nicht erforderlich ist und trotzdem eine Personenbeziehbarkeit, z.B. über eine dritte Stelle, besteht, in solchen Fällen auf den Gedanken von Art. 11 DSGVO zurückgegriffen kann, wonach eine Identifizierung der betroffenen Person nicht zur bloßen Einhaltung der Verordnung vorzunehmen ist. Dies würde bedeuten, dass ein Verantwortlicher, der aufgrund von datenschutzfreundlichen Maßnahmen die Daten nicht mehr einer betroffenen Person zuordnen kann, die Informationspflicht gegenüber der betroffenen nicht erfüllen muss. Andererseits kann man argumentieren, dass in Erwägungsgrund 64 DSGVO der Verantwortliche „alle vertretbaren Mittel“ nutzen muss.

Bei der Umsetzung der Transparenzpflicht ist bei einer Darstellung im Fahrzeug im Rahmen der technischen Begrenzungen auf eine adäquate Darstellung für den Betroffenen hinzuarbeiten. Weiterhin müssen Wege gefunden werden, die Vielzahl der rechtlich geforderten Informationen so aufzuarbeiten, dass sie für den technisch und rechtlich nicht besonders vorgebildeten Nutzer leicht verständlich sind und ebenso muss sichergestellt werden, dass Fahrer nicht von dem Steuern des Fahrzeugs abgelenkt werden (Vgl. auch die Ausführungen in Kapitel 7 Nutzerseitige Studien).

6.1.7.2. Informationspflichten bei der Erhebung von Daten nicht bei der betroffenen Person

Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, muss der Verantwortliche im Wesentlichen die gleichen Informationen an die betroffene Person erteilen.

Die Datenerhebung nicht bei der betroffenen Person spielt beim vernetzten Fahrzeug besonders dann eine Rolle, wenn es sich um Drittbetroffene handelt. Werden beispielsweise Fahrzeugdaten von einer Werkstatt ausgelesen, können sich darunter nicht nur die Daten der Person befinden, die das Fahrzeug zur Werkstatt gebracht hat, sondern auch Daten von sonstigen Nutzern des Fahrzeugs.

Für solche Fälle kommt die Ausnahme des Art. 14 Abs. 5 b) in Betracht, wonach keine Pflicht zur Informationserteilung besteht, wenn „die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde“.

6.1.8. Spezialgesetzliche Fragen

Spezialgesetzliche Regelungen können Vorrang vor den allgemeinen datenschutzrechtlichen Normen haben. Dabei kommen insbesondere das Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG), das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG) und das Energiewirtschaftsgesetz (EnWG) in Betracht. Spezifische Regelungen für KFZ-Daten existieren nicht.

6.1.8.1. Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG)

Das IVSG gilt nach seinem § 1 für intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern, wobei der Begriff der intelligenten Verkehrssysteme nach § 2 Nr. 1 IVSG als „Systeme, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an Schnittstellen zu anderen Verkehrsträgern eingesetzt werden“. Hinsichtlich des Datenschutzes wird in § 3 S. 2 IVSG lediglich darauf verwiesen, dass personenbezogene Daten nur aufgrund einer bundesgesetzlichen Regelung erhoben, verarbeitet oder genutzt werden dürfen. Es handelt sich also nicht um einen eigenen Erlaubnistatbestand sondern lediglich um einen deklaratorischen Verweis, der einen Rückgriff auf landesgesetzliche Normen ausschließt[60] .

6.1.8.2. Telemediengesetz (TMG)

Mit Geltung der Datenschutz-Grundverordnung ab 2018 wird die bisher schwierige Abgrenzung zwischen BDSG und TMG nicht mehr erforderlich sein, da die Datenschutzvorschriften des TMG (§ 11 ff.) nicht mehr anwendbar sein werden[61][62]. Eine Betrachtung dieser Regelungen soll hier deshalb außen vor bleiben.

6.1.8.3. Telekommunikationsgesetz (TKG)

Der Datenschutz im Bereich der Telekommunikation ist in den §§ 91 ff. TKG geregelt. Sie schützen die informationelle Selbstbestimmung der Beteiligten einer Telekommunikation vor den Diensteanbietern[63]. § 91 TKG formuliert daher, dass der Anwendungsbereich gegeben ist für den „Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken“. Normadressaten sind demnach, Unternehmen die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken (Telekommunikationsdiensteanbieter)[64]. Telekommunikationsdienste liegen vor, wenn die erbrachten Dienste „ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertagungsdienste in Rundfunknetzen“, § 3 Nr. 24 TKG.

Liegt der Anwendungsbereich des TKG vor, ist das BDSG nur noch subsidiär anwendbar. Nach Art. 95 DSGVO formuliert die Verordnung keine Anforderungen, die über die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), auf der die Regelungen des TKG beruhen, hinausgehen.

Soweit im Rahmen des vernetzten Fahrzeugs über Mobilfunk Übertragungsleistungen durch eine eingebaute SIM-Karte angeboten werden, kann insoweit die Anwendbarkeit des TKG für die Signalübertragung grundsätzlich gegeben sein[65] .

Von der Übertragungsebene ist die Inhaltsebene zu unterscheiden. So ist zu prüfen, ob der Dienst überwiegend in der Übertragung von Signalen bestehen, was häufig nicht der Fall sein dürfte[66] Damit sind die über die vernetzten Fahrzeuge angebotenen Dienste selbst als Inhaltsdaten zu qualifizieren und unterfallen dem BDSG.

[60] Kremer, Sascha Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz? RDV, 2014.

[61] Keppeler, Lutz Martin Was bleibt vom TMG-Datenschutz nach der DS-GVO? - Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz. MMR, 2015, Nr. 12.

[62] Schantz, Peter Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016, Nr. 26.

[63] Braun § 91. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4 Rn. 1.

[64] Eckhardt § 91. In Recht der elektronischen Medien. Spindler/Schuster, 2015, 3. Auflage Rn. 10.

[65] vgl. in: Kremer, Sascha Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz? RDV, 2014.

[66] Weichert, Thilo Datenschutz im Auto – Teil 1. SVR, 2014, Nr. 6.

6.1.8.3.1. Fernmeldegeheimnis Der Telekommunikationsdiensteanbieter unterliegt dem Fernmeldegeheimnis nach § 88 III TKG, welches das Grundrecht aus Art. 10 Grundgesetz (GG)[67] konkretisiert. Der Telekommunikationsdiensteanbieter ist zur Wahrung des Fernmeldegeheimnisses verpflichtet und darf sich und anderen daher gem. § 88 Abs. 3 TKG nicht über das erforderliche Maß hinaus Kenntnis von Inhalt oder Umständen der Telekommunikation verschaffen. Vom Fernmeldegeheimnis geschützt sind daher die Inhalte und Verkehrdaten nach § 3 Nr. 30 TKG, nicht aber die Bestandsdaten[68] .

Welche Kenntnisnahmen von Inhalten jeweils erforderlich ist, muss anhand des jeweiligen Einzelfalles beurteilt werden[69] . Es kommt auch in Betracht, dass die Kenntnisnahme im Rahmen von § 100 I TKG zur Erkennung von Viren oder Spam erforderlich sein kann. Dies wird damit begründet, dass der Telekommunikationsanbieter sich sonst an der Verbreitung solcher Inhalte beteilige[70] . Dies bedeutet, dass auch die Telekommunikationsdiensteanbieter zur IT-Sicherheit im vernetzten Fahrzeug beitragen könnten.

Tatsachen, die dem Fernmeldegeheimnis unterliegen, dürfen grundsätzlich nur für Zwecke der Erbringung der Telekommunikationsdienste und den Schutz der technischen Systeme verwendet werden.

6.1.8.3.2. Verkehrsdaten Verkehrsdaten nach § 3 Nr. 30 TKG sind im § 96 Abs. 1 TKG beispielhaft aufgezählt und umfassen neben den Nummern oder Kennungen der beteiligten Anschlüsse, Zugangsberechtigungsdaten, Beginn und Ende der Verbindung und übermittelte Datenmengen, wenn die Entgelte davon abhängen, alle „sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendigen“ Daten.

Die Verkehrsdaten sind nach § 96 Abs. 1 S. 3 TKG grundsätzlich vom Telekommunikationsdiensteanbieter unverzüglich nach Beendigung der Verbindung zu löschen, sofern die Verwendung der Verkehrsdaten nicht für die Aufrechterhaltung der Telekommunikation, Entgeltabrechnung nach § 97 TKG oder durch andere gesetzlich begründete Zwecke [71] oder zum Aufbau weiterer Verbindungen erforderlich ist. In der Rechtswissenschaft wird der Begriff der Unverzüglichkeit nach § 121 Bürgerliches Gesetzbuch (BGB) so definiert, dass kein schuldhaftes Zögern vorliegt. Hier ist der Begriff allerdings so zu verstehen, dass die Daten sofort zu löschen sind, weil es, anders als im BGB, keiner Überlegungszeit hinsichtlich bestimmter Folgen bedarf[72] .

6.1.8.3.3. Standortdaten § 98 TKG regelt die Verarbeitung von Standortdaten. Anwendungsfall von § 98 TKG ist die GSM-Ortung durch Telekommunikationsdiensteanbieter. Sie dürfen nur für die Bereitstellung von sog. „Diensten mit Zusatznutzen“ nach § 3 Nr. 5 TKG verarbeitet werden und sie müssen entweder anonymisiert werden oder es muss eine Einwilligung vorliegen.

Allerdings findet die Verarbeitung von Standortdaten regelmäßig nicht durch Telekommunikationsdiensteanbieter im Rahmen eines Telekommunikationsdienstes statt, weshalb die Norm keinen großen Anwendungsbereich aufweist. Ebenfalls unterliegen die über vernetzte Fahrzeuge angebotenen Dienste selbst und eine etwaige GPS-Ortung regelmäßig nur dem BDSG.

Der Grundgedanke des § 98 TKG, wonach Standortdaten eine besondere Sensibilität aufweisen, ist jedoch im Rahmen von Abwägungen und Angemessenheitsprüfungen zu beachten[73][74]

6.1.8.4. Energiewirtschaftsgesetz (EnWG) und Messstellenbetriebsgesetz (MsbG)

Im Zusammenhang mit der Elektromobilität stellen sich Fragen nach der Abrechnung der Energiekosten und welche Daten dafür erforderlich sind, bzw. erhoben werden dürfen. Bislang war der Datenschutz in § 21 g EnWG geregelt. Danach war die Verarbeitung personenbezogener Daten nur dann erlaubt, wenn dies durch zum Datenumgang berechtigte Stellen erfolgte und soweit es zur Begründung, inhaltlichen Ausgestaltung und Änderung eines Vertragsverhältnisses auf Veranlassung des Anschlussnutzers, zum Messen des Energieverbrauchs und der Einspeisemenge, zur Belieferung mit Energie und der Abrechnung, zum Einspeisen von Energie einschließlich der Abrechnung, zur Umsetzung variabler

[67] Bock § 88. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4 Rn. 1.

[68] Jenny, Valerian § 88. In Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Plath, Kai-Uwe, 2016, 1 Rn. 5.

[69] Bock § 88. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4 Rn. 26.

[70] Bock § 88. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4 Rn. 26.

[71] z.B. § 100 I TKG

[72] Braun § 96. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4 Rn. 19.

[73] Buchner, Benedikt Datenschutz im vernetzten Automobil. Datenschutz und Datensicherheit - DuD, 39 2015, Nr. 6 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0432-6⟩, ISSN 1862–2607.

[74] Weichert, Thilo Datenschutz im Auto – Teil 1. SVR, 2014, Nr. 6 206 f..

Tarife, zum Aufklären und Beenden von Leistungserschleichungen erforderlich war. Prüfungsmaßstab ist also wieder, ob die Datenverarbeitung für vorgegebene Zwecke erforderlich ist. Es wurde vertreten, dass die Erforderlichkeit im Sinne einer objektivierten Interessenabwägung zu verstehen sein soll[75] . Andererseits kann man auch vertreten, dass die die Erforderlichkeit im Sinne einer Datenminimierung zu verstehen ist.

Fraglich war, ob eine datensparsame Nutzung von Ladesäulen wegen der detaillierten Vorgaben für die Abrechnung in § 40 EnWG möglich ist. So legt § 40 Abs. 2 Nr. 5 EnWG z.B. fest, dass in einer Rechnung an einen Letztverbraucher der Verbrauch des vergleichbaren Vorjahreszeitraums auszuweisen ist und Nr. 3 verlangt die Angabe der Zählpunktbezeichnungen. Die Erhebung und Speicherung dieser u.a. zur Erstellung von Bewegungsprofilen geeigneten Daten wäre daher erforderlich zur Abrechnung im Sinne von § 21 g Abs. 1 Nr. 3 EnWG. Diese Überlegungen sind allerdings durch eine Gesetzesänderung überholt, weil 21g EnWG durch Artikel 3 des Gesetzes zur Digitalisierung der Energiewende vom 29.08.2016 [76] weggefallen ist.

Es finden sich nunmehr datenschutzrechtliche Vorgaben im Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG). Das MsbG regelt in den §§ 19 ff. technische Vorgaben für Datenschutz und Datensicherheit bei Smart-Meter-Gateways und in den §§ 49 ff. werden allgemeine Anforderungen an die Datenerhebung, -verarbeitung und -nutzung formuliert. Für Messsysteme, die ausschließlich der Erfassung der zur Beladung von Elektromobilen entnommenen oder durch diese zurückgespeisten Energie dienen, werden die Vorschriften über die technischen Vorgaben für Datenschutz und Datensicherheit grundsätzlich nach § 48 S.1 MsbG erst ab dem 01.01.2021 anwendbar sein. Wenn in einem bestimmten Verfahren unverhältnismäßige Gefahren festgestellt werden, kann diese Frist kürzer sein, §§ 48 S. 2, 26 Abs. 1 MsbG.

§ 49 Abs. 1 MsbG legt fest, dass personenbezogene Daten nur von berechtigten Stellen erhoben, verarbeitet und genutzt werden dürfen. Berechtigte Stellen sind nach § 49 Abs. 2 MsbG Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmer nach dem EEG (Erneuerbare-Energien-Gesetz), Energielieferanten und jede Stelle, die über eine wirksame Einwilligung des Anschlussnutzers verfügt, wobei für die Wirksamkeit auf die Anforderungen des § 4a BDSG Bezug genommen wird. Den berechtigten Stellen ist es nach § 49 Abs. 3 MsbG erlaubt, sich zur Erhebung, Verarbeitung und Nutzung eines Dienstleisters zu bedienen. § 49 Abs. 5 MsbG enthält ein Kopplungsverbot. Die Belieferung mit Energie darf nicht davon abhängig gemacht werden, ob eine betroffene Person personenbezogene Daten preisgibt, die für die Belieferung mit Energie nicht erforderlich sind.

§ 50 Abs. 1 regelt, dass die Erhebung, Verarbeitung und Nutzung von Daten nur mit Einwilligung erfolgen darf oder wenn die Erforderlichkeit für bestimmte Zwecke gegeben ist. Die Norm legt damit auch für den Anwendungsbereich des MsbG fest, dass für jede Datenerhebung –verarbeitung und –nutzung entweder eine Einwilligung oder Rechtsgrundlage vorliegen muss (sog. Verbot mit Erlaubnisvorbehalt). Zu den in Betracht kommenden Zwecken zählt auch die Erfüllung von Verträgen mit dem jeweiligen Anschlussnutzer. § 50 Abs. 2 MsbG zählt dann nicht abschließend auf, welche Zwecke zulässig sein können. Nach § 50 Abs. 2 Nr. 3 MsbG kann es sich dabei auch um die Belieferung mit Energie einschließlich der Abrechnung handeln. Die Vorgaben für die Abrechnung finden sich weiterhin in § 40 EnWG und sind sehr umfangreich, was einer datenschutzfreundlichen Abrechnung entgegensteht. Erste Voraussetzung von § 40 EnWG ist, dass es sich um Energielieferungen an Letztverbraucher handelt. Letztverbraucher sind nach § 3 Nr. 25 EnWG natürliche oder juristische Personen, die Energie für den eigenen Verbrauch kaufen, wobei der Strombezug der Ladepunkte für Elektromobile dem Letztverbrauch gleichgestellt ist. Der Letztverbraucher ist durch einen unmittelbaren Eigenbedarf gekennzeichnet. Die Abgrenzung erfolgt danach, ob der Bezug von Energie eigenen Zwecken dient und ob sich der Beziehende und der Nutzer „als selbstständige wirtschaftliche Subjekte gegenüberstehen“[77] . Diese Voraussetzung liegt beim Kauf von Energie an einer Ladesäule zum Laden eines Elektromobils unproblematisch vor. Ladesäulenbetreiber und Fahrzeugnutzer sind im Regelfall voneinander wirtschaftlich selbständig. Fraglich ist, was durch die Gleichstellung des Bezugs der Ladepunkte mit dem Letztverbrauch erreicht werden sollte. Wenn der Strombezug der Ladepunkte selbst der Letztverbrauch ist, kann der Fahrzeugnutzer schon begrifflich nicht mehr Letztverbraucher sein, weil es nicht mehrere Letztverbraucher geben kann. Zweck der Regelung ist es unter anderem, dass das EnWG im Verhältnis zwischen Fahrzeugnutzer und Ladesäulenbetreiber nicht anwendbar sein soll[78] und durch klare energierechtliche Einordnungen von Ladesäulen Investitionshindernisse abgebaut werden sollen[79] Damit ist § 40 EnWG im Verhältnis zwischen Ladesäulenbetreiber und Fahrzeugnutzer nicht anwendbar, weil bereits der Ladesäulenbetreiber als Letztverbraucher gilt, die umfangreichen Bestimmungen zur Abrechnung sind zwischen Ladesäulenbetreiber und Fahrzeugnutzer nicht anwendbar und das EnWG steht datenschutzfreundlichen Abrechnungsmodellen nicht entgegen.

[75] Thiel, Markus § 21g. In EnWG. Kment, 2015, 1 Rn. 5.

[76] Bundesgesetzblatt Jahrgang 2016, Teil I Nr 43, S. 2034 ff.

[77] Theobald EnWG § 3. In Energierecht. Danner/Theobald, 2016, 89. EGL Rn. 207.

[78] Harendt, Bertram/Wolf, Catharina Energierechtliche Einordnung der Ladeinfrastruktur für Elektrofahrzeuge Information über geplante Änderungen des Energierechts im Jahre 2016. Januar 2016.

[79] Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Weiterentwicklung des Strommarktes (Strommarktgesetz). Januar 2016.

Zu denken ist hier unter anderem an Modelle, die Barzahlung am Automaten gestatten oder bequemer und für den Betreiber sicherer eine Prepaid-Lösung auf Basis anonym nutzbarer Credentials. Denkbar wäre auch ein Flatrate-Angebot, bei dem lediglich nachzuweisen wäre, dass für das das jeweilige Fahrzeug im laufenden Abrechnungszeitrum eine Flatrate besteht. Auf Basis entsprechender kryptografischer Lösungen wären sämtliche oben genannten Varianten anonym bzw. pseudonym nutzbar[80] .

[80] ABC4Trust ABC4Trust – Attribute-based Credentials for Trust. 2014 ⟨URL: www.abc4trust.eu⟩.

7. Nutzerseitige Studien

Mit den Herausforderungen der Digitalisierung und Vernetzung von Alltagstechnik konnten Nutzer, je nach Alter, schon in vielen Lebensbereichen Erfahrungen sammeln, sei es noch aus der Bürotechnik (Einführung von PCs, E-Mail), sei es aus der Unterhaltungselektronik (CD-Player, Spielkonsolen, Streaming-Musikplayer), der Telekommunikation (Mobiltelefone mit SMS usw.) oder in letzter Zeit aus einer zunehmenden Anzahl von Alltagsgeräten wie vernetzten Fernsehern, Uhren und Armbändern oder Glühbirnen[1]. Viele Studien zeigen, dass Nutzer solchen Digitalisierungsschüben nicht wehrlos ausgeliefert sind und sich dadurch auch nicht fremdbestimmen lassen[2][3][4][5]. Vielmehr „domestizieren" die Nutzer die Technik zu einem gewissen Punkt, zum Beispiel indem sie PCs über lange Zeit auf bestimmte Räume im Haushalt verbannt halten[6]oder indem sie heute die integrierten Webcams von Laptops zum Datenschutz abkleben. Umgekehrt sind den Nutzern dabei aber durch das Design der neuesten Generationen mobiler Technik Grenzen gesetzt. Zum einen erlauben ihnen geschlossene Systeme weniger Möglichkeiten zur Anpassung der Technik[7], zum anderen wirkt gerade die Vernetzung von Alltagsgegenständen wie Uhren, Glühbirnen oder auch Autos auf sie unverfänglich: Die Vernetztheit mit den damit verbundenen Gefahren sehen sie den Geräten nicht unbedingt an, weil das Internet darin „versteckt" ist[8]. Weiter ist in den gewohnten Abläufen etwa zur Einrichtung eines neuen Fernsehers schlicht nicht vorgesehen, Einstellungen zum Datenschutz – wie etwa zum regelmäßigen Löschen von Cookies – vorzunehmen.

In der Alltagswelt der Nutzer stellt das vernetzte Auto zunächst einen weiteren Gegenstand und Lebensbereich dar, der vernetzt und digitalisiert wird. Gleichzeitig bringt es aber besondere Rahmenbedingungen mit, die sich aus der hohen Bedeutung des Autos für (gerade deutsche) Konsumenten ergibt. Diese werden zunächst (Abschnitt 7.1) auf Basis bestehender Befunde aufgearbeitet. Danach werden (Abschnitt 7.2) Vorgehen und Befunde der Teilstudien vorgestellt, die im Rahmen des SeDaFa-Forschungsprojekts durchgeführt wurden. Schließlich (Abschnitt 8.1) werden aus diesen Befunden nutzerseitige Vorgaben für die Entwicklung technischer Lösungen zur Ermöglichung von Selbstdatenschutz im vernetzten Fahrzeug abgeleitet.

7.1. Forschungsstand: Herausforderungen für den Selbstdatenschutz im Fahrzeug

Es haben sich erst relativ wenige Studien mit der Nutzersicht auf den Datenschutz im vernetzten Automobil befasst.

Eine Erkenntnis ist zunächst, dass das Auto von den Nutzern als Garant für hohe Privatheit und als Schutzraum des Privaten wahrgenommen wird[9][10].

Weiter ist sich im Sinne des „versteckten Internets"[11]der Großteil der Nutzer weder über die Existenz von vernetzten Fahrzeugen noch über die Zugehörigkeit ihres eigenen Fahrzeugs zu eben dieser Klasse bewusst[12][13]. Diese Unkenntnis bezüglich vernetzter Fahrzeuge stellt jedoch eine Gefahr für das persönliche Datenschutzverhalten dar. Während Personen

[1] Karaboga, M. et al. White Paper Das Versteckte Internet: Zu Hause - Im Auto - Am Körper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt 2 Juli 2015.

[2] Haddon, Leslie Domestication and mobile telephony. Machines that become us: The social context of personal communication technology, 2003.

[3] Berker, Thomas/Hartmann, Maren/Punie, Yves Domestication of media and technology. McGraw-Hill Education (UK), 2005.

[4] Wirth, Werner/Von Pape, Thilo/Karnowski, Veronika An integrative model of mobile phone appropriation. Journal of Computer-Mediated Communication, 13 2008, Nr. 3.

[5] Ribak, Rivka/Rosenthal, Michele Smartphone resistance as media ambivalence. First Monday, 20 2015, Nr. 11.

[6] ThorstenQuandt/Pape, Thilo von Living in the Mediatope: A Multimethod Study on the Evolution of Media Technologies in the Domestic Environment. The Information Society, 26 2010, Nr. 5.

[7] Best, Kirsty/Tozer, Nathan Scaling digital walls: Everyday practices of consent and adaptation to digital architectural control. International Journal of Cultural Studies, 16 2013, Nr. 4.

[8] Karaboga, M. et al. White Paper Das Versteckte Internet: Zu Hause - Im Auto - Am Körper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt 2 Juli 2015.

[9] Kent, Jennifer L. Still Feeling the Car - The Role of Comfort in Sustaining Private Car Use. Mobilities, 10 2015, Nr. 5.

[10] Sheller, Mimi/Urry, John Mobile Transformations of 'Public' and 'Private' Life. Theory, Culture & Society, 20 2003, Nr. 3 ⟨URL: http://tcs.sagepub.com/content/20/3/107.abstract⟩.

[11] Karaboga, M. et al. White Paper Das Versteckte Internet: Zu Hause - Im Auto - Am Körper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt 2 Juli 2015.

[12] Schiller, Thomas et al. Datenland Deutschland – Connected Car. 2015 ⟨URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/manufacturing/150909_DEL-15-5015_Brosch%C3%BCre_DasConnectedCar_rz_WEB-safe.pdf⟩.

[13] FIA What Europeans think about connected cars. 2016.

mit einem hohen Kenntnisstand bezüglich moderner Fahrzeugkonzepte ein ausgeprägtes Risikobewusstsein für den Datenschutz zeigen, korreliert Unwissenheit häufig mit Geringschätzung des Risikos[14]. Werden Autofahrer jedoch explizit zur Datenpreisgabe befragt haben sie konkrete Vorstellungen, an welche Empfänger sie bestimmte Datentypen zu einem bestimmten Zweck freigeben möchten[15][16]. So legen mehrere Befragungen nahe, dass Nutzer bei der Entscheidung der Datenpreisgabe eine Kosten-Nutzen-Abwägung vollziehen. Die Aussicht auf eine erhöhte Verkehrssicherheit durch die Datenweitergabe Nutzenvorteile bewegt dabei Nutzer eher zur Freigabe von Daten als dies bei Entertainmentangeboten der Fall ist[17][18]. Doch nicht nur der Nutzungszweck spielt für Anwender eine Rolle. Eine besondere Bedeutung kommt auch der Vertrauenswürdigkeit der Empfänger zu. Nutzer sind bei der Preisgabe von Daten an Empfänger, denen sie kommerzielle Interessen unterstellen (z.B. App-Anbieter), deutlich zurückhaltender als bei Institutionen der öffentlichen Hand (z.B. Polizei)[19]. Die Umfrage von Müller-Peters zeigt aber auch gleichermaßen, dass mit Transparenz und der Zusprache von Kontroll- und Eingriffsmöglichkeiten durch den Nutzer die Akzeptanz von datenverarbeitenden Diensten und Services unabhängig vom Anbieter gesteigert werden kann.

Der Ansatz des Selbstdatenschutzes wird somit durch die Nutzer selbst gefordert und kann nicht nur als nutzerrechtliches Werkzeug, sondern auch als Akzeptanz förderndes Mittel für Anbieter auf dem Markt von Online-Mehrwertdiensten betrachtet werden.

7.2. Empirische Studien

7.2.1. Quantitative Befragungsstudie der TU Darmstadt

7.2.1.1. Motivation

Der Umgang mit und die Rechte über nutzergenerierte Daten sind einige der kontrovers diskutierten Themen der Gegenwart. Aus Sicht der Nutzer stellt Selbstdatenschutz dabei ein erstrebenswertes Ziel dar, auch wenn die Bereitschaft zu Einschränkungen und zum Verzicht auf Komfort und Funktionsvielfalt sich im tatsächlichen Verhalten nur bedingt niederschlägt[20][21]. Entsprechend decken die oben dargelegten Studien erste relevante Ansatzpunkte für die Ausgestaltung eines selbstbestimmten Datenschutzes im Automobil auf. Dabei beruhen die Erkenntnisse jedoch auf relativ abstrakten Fragestellungen, die oftmals ohne ein konkretes Rahmenszenario auskommen. Je unkonkreter der Befragungsrahmen, desto breiter ist jedoch der Interpretationsspielraum, der den Befragten aufgespannt wird. Einzelne Antworten können mit unterschiedlicher gedanklicher Verankerung gegeben werden, sodass eine valide Interpretation der Ergebnisse erschwert wird. Daher wurde im Frühjahr 2016 eine eigene Online-Befragung durchgeführt, um quantitative Aussagen über die Einstellungen von Nutzern zum Thema Datenschutz im vernetzten Fahrzeug zu erfassen. In Anlehnung an die Szenarien-Technik aus der Usability-Forschung[22] wurden konkrete Anwendungsszenarien von Online-Mehrwertdiensten im vernetzten Fahrzeug entwickelt, um ein einheitliches Anwendungsverständnis bei den Probanden zu ermöglichen. Durch den Einsatz eindeutiger Szenarien sollte eine Grundlage und Verankerung für die gestellten Fragen geschaffen werden, sodass den Befragten der Zugang zu den Fragen erleichtert wird[23]. Unter Einsatz dieser Methodik wurden folgende Forschungsfragen verfolgt:

- Unter welchen Bedingungen sind Nutzer bereit Ihre Daten preis zu geben?
- Welche Daten sind für die Nutzer kritisch im Sinne des Datenschutzes?
- Welche Rolle spielt der Empfänger für die Bereitschaft zur Datenpreisgabe?

[14] Schoettle, B./Sivak, M. A survey of public opinion about connected vehicles in the U.S., the U.K., and Australia. In 2014 International Conference on Connected Vehicles and Expo (ICCVE). Nov 2014, ISSN 2378–1289.

[15] Müller-Peters, H Der vernetzte Autofahrer–Akzeptanz und Akzeptanzgrenzen von eCall Werkstattvernetzung und Mehrwertdiensten im Automobilbereich. Schriftenreihe Forschung am IVW Köln, Bd, 3 2013.

[16] FIA What Europeans think about connected cars. 2016.

[17] Schiller, Thomas et al. Datenland Deutschland – Connected Car. 2015 ⟨URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/manufacturing/150909_DEL-15-5015_Brosch%C3%BCre_DasConnectedCar_rz_WEB-safe.pdf⟩.

[18] FIA What Europeans think about connected cars. 2016.

[19] Müller-Peters, H Der vernetzte Autofahrer–Akzeptanz und Akzeptanzgrenzen von eCall Werkstattvernetzung und Mehrwertdiensten im Automobilbereich. Schriftenreihe Forschung am IVW Köln, Bd, 3 2013.

[20] Hui, Kai-Lung/Tan, Bernard C. Y./Goh, Chyan-Yee Online Information Disclosure: Motivators and Measurements. ACM Trans. Internet Technol. 6 November 2006, Nr. 4, ISSN 1533–5399.

[21] Acquisti, Alessandro/John, Leslie K/Loewenstein, George What is privacy worth? The Journal of Legal Studies, 42 2013, Nr. 2.

[22] Rosson, Mary Beth/Carroll, John M. The Human-computer Interaction Handbook. Hillsdale, NJ, USA: L. Erlbaum Associates Inc., 2003 ⟨URL: http://dl.acm.org/citation.cfm?id=772072.772137⟩, ISBN 0–8058–3838–4. – KapitelScenario-based Design.

[23] Richter, Michael/Flückiger, Markus D Usability Engineering kompakt: benutzbare Produkte gezielt entwickeln. Springer-Verlag, 2013.

- Welcher Zusammenhang besteht zwischen der Datenschutzeinstellung im Auto und dem Datenschutzverhalten im Alltag?
- Von welchen Faktoren hängt die Bereitschaft zur Datenpreisgabe ab?

7.2.1.2. Methode

7.2.1.2.1. Stichprobe 45 Personen nahmen erfolgreich an der Online-Umfrage teil. Die Teilnehmer wurden über Werbung in sozialen Medien sowie Kontaktaufnahmen im Umfeld des Instituts für Arbeitswissenschaft rekrutiert. 67 % der Befragten waren männlich. Die Altersspanne betrug 18 bis 75 Jahre, wobei 62 % der Teilnehmer aus der Altersgruppe 18–36 Jahre stammten. Unter den Befragten verfügten 73 % über ein eigenes Auto. Abbildung 7.1 stellt die Zusammensetzung des Probandenkollektivs nochmals graphisch dar.

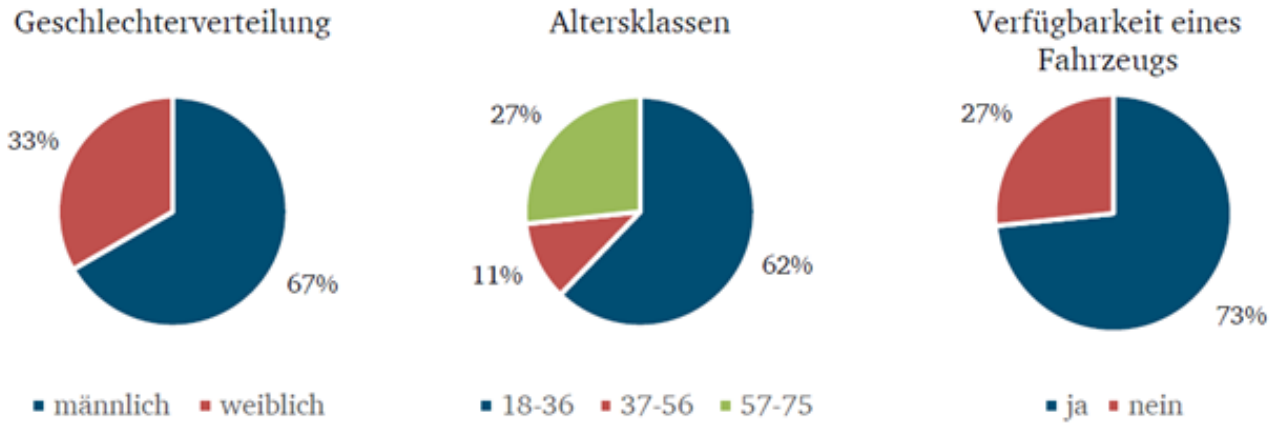


Abbildung 7.1: Zusammensetzung des Probandenkollektivs der Online-Befragung ($N = 45$).

7.2.1.2.2. Fragebogen Der Fragebogen orientierte sich an den oben aufgeführten Forschungsfragen und gliederte sich in insgesamt drei Blöcke. Im ersten Block wurden konkrete Anwendungsszenarien eingeführt und die Akzeptanz derselben erfasst. Dabei bewerteten die Befragten den jeweiligen konkreten Nutzen der in den Anwendungsszenarien beschriebenen Mehrwertdienste und gaben ihre Bereitschaft zur Preisgabe von anfallenden Daten an. Zur Bewertung des Einflusses der Zweckgebundenheit auf die Bereitschaft zur Datenpreisgabe wurde im Zuge der Szenarien-basierten Erfassung auch die Preisgabe von solchen Daten abgefragt, die für den beschriebenen Dienst nicht funktionsrelevant sind. Der zweite Block widmete sich allgemeinen Datenschutzeinstellungen im Fahrzeug sowie der bisherigen Datenschutzpraxis im (mobilen) Internet. Hierbei wurde die Nutzersicht auf die Datenschutzrelevanz einzelner Datentypen sowie die Vertrauenswürdigkeit von verschiedenen Empfängern mit Bezug auf den Umfang der Daten erfasst. Darüber hinaus wurde erhoben, unter welchen Umständen sich die Bereitschaft zur Datenpreisgabe erhöht und wie sich das bisherige Datenschutzverhalten außerhalb des Fahrzeugkontexts darstellt. Der letzte Block umfasste demographische Fragen sowie Fragen zur Verfügbarkeit eines eigenen Autos. Mit Ausnahme von Block drei bestand der Fragebogen aus einzelnen Aussagen, zu denen die Teilnehmer ihre Zustimmung auf einer fünfstufigen Likertskala von „stimme nicht zu“ bis „stimme zu“ angeben konnten. Abbildung 7.2 stellt eine Aussage samt Antwortskala beispielhaft dar. Der letzte Block bestand hingegen aus einfachen Fragen mit mehreren vorgegebenen Antwortoptionen. Im Folgenden werden den Antwortlabels Zahlenwerte zugewiesen. So bedeutet 1 „stimme nicht zu“, während 5 „stimme zu“ repräsentiert.

7.2.1.2.3. Die Szenarien Die Szenarien orientieren sich an den in Kapitel 3 eingeführten Anwendungsfällen. Hierbei wurde jeweils ein Szenario zu einem Online-Mehrwertdienst aus den Bereichen *Entertainment/Vernetzung, Navigation/Effizienz* und *Sicherheit* dargestellt. Jedes Szenario umfasst eine Mehrwertsbeschreibung sowie eine Auflistung der dafür preis zu gebenden Daten. Angelehnt an die Kategorie „Drittanbieter-Erweiterungen“ (vgl. Tabelle 3.1) beschreibt das Szenario „Das vernetzte Fahrerlebnis“ den Einsatz von Mehrwertdiensten, die neben präferenzbasierten Nachrichten auch das sprachgesteuerte Empfangen und Versenden von E-Mails im Fahrzeug ermöglichen. Zudem beinhaltet das Szenario auch einen Online-Musikstreamingdienst, der basierend auf der Nutzungshistorie eine individuelle präferenzbasierte Musikauswahl vorschlägt. Funktionsrelevante Daten sind das Nutzungsverhalten (zum Beispiel (z.B.)Musikauswahl) sowie persönliche Informationen (z.B. Kunden-ID, Name). Das Szenario „Prädikative Navigation“ bezieht sich auf die

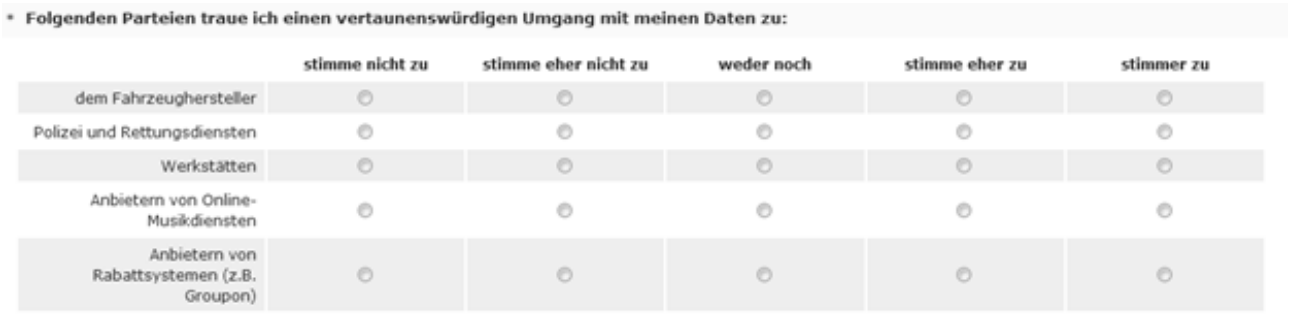


Abbildung 7.2: Beispielhafte Aussage samt fünfstufiger Likertskala aus dem Online-Fragebogen.

Kategorie „Location-Based Services“ und beschreibt ein intelligentes Navigationssystem, dass die Fahrtziele des Nutzers automatisch antizipiert, vorschlägt und auch bei Streckenbehinderungen eine zeiteffiziente Fahrt ermöglicht. Für diese Anwendung werden GPS-Daten sowie insassenbezogene Daten erfasst sowie auf Einträge eines synchronisierten Kalenders zurückgegriffen. Als Referenzszenario aus dem Bereich Sicherheit wird ein automatisches Notrufsystem vorgestellt, das im Falle eines Unfalls die GPS-Position sowie insassenbezogene Daten an die Rettungskräfte weiterleitet.

7.2.1.2.4. Durchführung Der Fragebogen wurde mit Hilfe des Online-Anbieters LimeSurvey erstellt und verwaltet. Die Teilnehmer bekamen einen Link zur Online-Umfrage zugesendet und hatten über einen Zeitraum von 14 Tagen Zeit an der Umfrage teilzunehmen. Der Fragebogen konnte zwischengespeichert werden, sodass nicht alle Fragen am Stück beantwortet werden mussten. Im Durchschnitt dauerte die Beantwortung des Fragebogens 13 Minuten.

7.2.1.3. Befunde

Im Folgenden werden die deskriptiven Ergebnisse der Online-Befragung berichtet. Hierzu werden zu jedem Einzelbefund die mittlere Antworttendenz in Form des Mittelwerts (M) sowie das Ausmaß der Antwortstreuung durch die Standardabweichung (sd) angegeben.

7.2.1.3.1. Enthusiasmus für Sicherheit und Effizienz, aber Zurückhaltung bei der Bereitschaft zur Datenpreisgabe Insgesamt zeigten sich die Teilnehmer an den dargebotenen Funktionen der Mehrwertdienste interessiert. Dabei erhielten eine verbesserte Navigation (M = 4,33; sd = 1,09) sowie eine erhöhte Sicherheit (M = 4,13; sd = 1,14) besonders hohe Zustimmungen, während die Vernetzung mit Bekannten und/oder anderen Verkehrsteilnehmern eher abgelehnt wurde (M = 2,36; sd = 1,28). Unterschiede zeigten sich auch zwischen den Altersklassen. Junge Teilnehmer ($<$ 37 Jahre) waren an Musikstreaming-Diensten stärker interessiert als an einer Synchronisation des E-Mail-Postfachs im Auto (M = 4,11; sd = 1,23 vs. M = 2,74; sd = 1,48), wohingegen ältere Teilnehmer ($>$ 56 Jahre) beide Dienste mit eher zurückhaltendem Interesse begegneten (M = 2,93; sd = 1,28 vs. M = 3,06; sd = 1,67). Im Kontrast zum Interesse an den Funktionen der Mehrwertdienste steht die Bereitschaft zur Preisgabe der Daten. Weder zur Nutzung der prädikativen Navigation, noch zur Nutzung von Informations- und Unterhaltungsdiensten (Szenario „Das vernetzte Fahrerlebnis“) zeigten sich die Teilnehmer bereit die Daten bereitzustellen (alle $M < 2{,}94$). Dabei zeigten sich jedoch auch hier Unterschiede zwischen den Altersklassen. Besonders Teilnehmer $>$ 56 Jahre gaben eine geringe Bereitschaft zur Datenweitergabe an, unabhängig von der Art der Daten (alle $M < 1.67$).

7.2.1.3.2. Vertrauenswürdigkeit und persönliche Relevanz beeinflussen die Bereitschaft zur Datenweitergabe Trotz der eingeschränkten Bereitschaft zur Datenpreisgabe differenzierten die Teilnehmer zwischen verschiedenen Anlässen zur Datenpreisgabe. So gaben die Teilnehmer an Ortungsdaten für ein automatisches Notrufsystem preisgeben zu wollen (M = 4,8; sd = 0,68), während sie die gleichen Daten für Kommunikations-, Unterhaltungs- (M = 1,27; sd = 0,69) und selbst für Navigationsdienste (M = 1,62; sd = 1,03) nicht teilen wollten. Dabei zeigte sich, dass die Bereitschaft zur Datenweitergabe in solchen Szenarien höher war, die eine Funktion bedienten, die eine höhere persönliche Relevanz und Akzeptanz bei den Teilnehmern hatte. Die permanente Verfolgung der gefahrenen Route wurde durch die Teilnehmer nicht befürwortet. Auch wenn die durchgehende Positionsaufzeichnung zum Beispiel durch die prädikative Navigation direkt zweckgebunden war, äußerten die Teilnehmer keine klare Zustimmung (M = 3,02; sd = 1,49). Als Gründe für die Zurückhaltung gaben die Teilnehmer an, besonders einen Datenklau zu befürchten (M = 4,11; sd = 1,17).

Des Weiteren spielte auch die Wahrnehmung des Autos als sicherer Rückzugsraum eine Rolle, die auch schon von Roßnagel[24] festgehalten wurde. Entsprechend gaben die Teilnehmer an das Auto als privaten Raum wahrzunehmen (M = 3,91; sd = 1,20), dessen Existenz sie durch die permanente Datenweitergabe gefährdet sehen.

Darüber hinaus beeinflusste auch der Ort der Datenverarbeitung die Bereitschaft zur Datenpreisgabe. Das lokale Speichern von Daten im Auto wurde von den Teilnehmern der Datenübertragung an einen externen Empfänger bevorzugt. So präferierten die Teilnehmer die lokale Speicherung von Positionsdaten zur prädikativen Navigation (M = 2,64; sd = 1,48) gegenüber der Datenübertragung an den Hersteller (M = 1,62; sd = 1,03). Wurde jedoch eine Datenübertragung angenommen, dann differenzierten die Teilnehmer auch zwischen der Vertrauenswürdigkeit unterschiedlicher Datenempfänger. Unabhängig von den Szenarien wurden verschiedene Parteien gemäß ihrer Vertrauenswürdigkeit in Bezug auf den Umgang mit erhobenen Daten bewertet. Dabei zeigte sich, dass solchen Parteien mit Skepsis begegnet wurde, denen primär ein wirtschaftliches Interesse unterstellt wurde. Nahezu im Einklang mit den Befunden von Müller-Peters[25] gaben die Teilnehmer an Einsatz- und Rettungsdiensten tendenziell zu vertrauen (M = 4,04; sd = 1,28), während Anbietern von Rabattsystemen und Musikstreaming-Diensten kein verantwortungsvoller Umgang mit den Daten zugesprochen wurde (M = 1,24; sd = 0,53 beziehungsweise M = 1,71; sd = 0,89). Auch das Vertrauen in Hersteller und Werkstätten bezüglich des Datenumgangs war begrenzt (M = 2,16; sd = 1,24 beziehungsweise M = 2,73; sd = 1,27).

7.2.1.3.3. Datum ist nicht Datum - Nutzer differenzieren zwischen Datentypen Die Anwendungsfälle in Kapitel 3 verdeutlichen, dass eine Vielzahl an Daten im Auto erfasst und verarbeitet werden kann. Dabei gesteht nicht nur das Bundesdatenschutzgesetz verschiedenen Daten unterschiedliche Sensibilitäten und damit verbundene Schutzwürdigkeiten zu. Auch die Nutzer stuften verschiedene Daten unterschiedlich kritisch mit Bezug auf den Datenschutz ein. Je höher der Personenbezug, desto sensibler wurde ein Datum bewertet. Die Teilnehmer dieser Umfrage gaben an, dass besonders Kalendereinträge einen hohen Personenbezug hätten (M = 4,89; sd = 0,38). Auch die Historie der eigenen Musik- und Nachrichtenauswahl (M = 4,29; sd = 1,01), das Fahrprofil (M = 4,33; sd = 0,93) und die Positionsdaten (M = 4,47; sd = 0,84) wurden als eher personenbeziehbare Daten bewertet. Bei Daten zum Betriebszustand des Fahrzeugs sahen die Teilnehmer zeigten die Teilnehmer keine explizite Tendenz bezüglich der Personenbeziehbarkeit (M = 3,42; sd = 1,22). Dabei missachteten sie das Potential zur Profilbildung, die auch Betriebsdaten bergen. Den Nutzern mangelte es an einer umfassenden Kenntnis über die Tracking-Möglichkeiten, die aus der permanenten Erhebung von vermeintlich rein technischen Daten hervorgehen. Dennoch steht die beobachtete Differenzierung zwischen Datentypen im Einklang zu bisherigen Umfrageergebnissen[26], spiegelt aber nur bedingt Klassifikationen wieder, die durch Expertenkreise[27] oder im Bundesdatenschutzgesetz vorgenommen werden.

7.2.1.3.4. Diskrepanz zwischen Datenschutzeinstellung und Datenschutzverhalten Entgegen den meist recht entschiedenen Angaben für einen strengen Datenschutz zeigen Studienteilnehmer regelmäßig einen eher freigiebigen Umgang mit ihren Daten. Diese als „intention-behavior gap“ (e.g. Sheeran, 2011[28]) bezeichnete Diskrepanz zwischen beteuerter Intention und tatsächlich gezeigtem Verhalten konnte auch in dieser Studie beobachtet werden. Obwohl die Teilnehmer durchweg der Datenpreisgabe kritisch gegenüberstanden und angaben auch funktionskritische Daten wie zum Beispiel Positionsdaten für Informations- und Unterhaltungsdienste nicht preisgeben zu wollen (alle $M < 2{,}67$), berichteten sie im Durchschnitt ein konträres Verhalten. Gefragt zu ihrem Datenschutzverhalten in sozialen Netzwerken oder bei der Installation von neuen Anwendungen auf mobilen Geräten gaben sie an nicht oder nur bedingt auf die Preisgabe von Daten zu achten (M = 1,729; sd = 1,18 beziehungsweise M = 2,312; sd = 1,22). Betrachtet man das berichtete Datenschutzverhalten etwas genauer, so zeigen sich dennoch Unterschiede zwischen den Teilnehmern, die auch unabhängig vom Anwendungskontext fortbestehen. Teilnehmer, die angaben im Alltag nicht oder nur begrenzt auf aktivierte Ortungsdienste des Smartphones zu achten (N = 14), zeigten eine höhere Bereitschaft ihre Daten im Fahrzeugkontext preiszugeben (M = 3,50 ; sd = 1,40) als solche, die auf die Aktivierung der Ortungsdienste des Smartphones achteten (N = 29; M = 2,10; sd = 1,26). Somit zeigten sich Teilnehmer, die angaben bereits jetzt ein hohes Datenschutzbewusstsein im Umgang mit dem (mobilen) Internet zu haben, auch bezüglich des Datenschutzes im vernetzten Automobil kritischer.

[24] Roßnagel, Alexander Grundrechtsausgleich beim vernetzten Automobil. Datenschutz und Datensicherheit - DuD, 39 2015, Nr. 6, ISSN 1862–2607.

[25] Müller-Peters, H Der vernetzte Autofahrer–Akzeptanz und Akzeptanzgrenzen von eCall Werkstattvernetzung und Mehrwertdiensten im Automobilbereich. Schriftenreihe Forschung am IVW Köln, Bd, 3 2013.

[26] FIA What Europeans think about connected cars. 2016.

[27] Unabhängige Datenschutzbehörden des Bundes und der Länder/Verband der Automobilindustrie (VDA) Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge. 2016.

[28] Sheeran, Paschal Intention—Behavior Relations: A Conceptual and Empirical Review. European Review of Social Psychology, 12 2002, Nr. 1.

7.2.1.3.5. Transparenz, aber nicht Vergütung erhöht die Bereitschaft zur Datenweitergabe Im Einklang mit bisherigen Befunden[29] ergab die hiesige Umfrage, dass Nutzer der Preisgabe von Daten kritisch gegenüber eingestellt sind. Unter welchen Bedingungen sind Nutzer aber dennoch bereit Daten zu teilen? Im Kontrast zu den Ergebnissen von Danezis, Lewis und Anderson[30], die durch monetäre Anreize die Befragten zur Datenpreisgabe bewegen konnten, zeigten sich die Teilnehmer dieser Studie nicht bereit Daten im Gegenzug für finanzielle Vorteile preiszugeben. So waren die Teilnehmer weder bereit Daten für eine Vergünstigung beim Erwerb oder der Nutzung eines Mehrwertdienstes (M = 1,84; sd = 1,07) preiszugeben, noch zeigten Vergünstigungen beim Fahrzeugkauf (M = 2,22; sd = 1,26) oder die Aussicht auf einen günstigeren Versicherungstarif Wirkung (M = 2,40; sd = 1,29). Im Gegensatz dazu waren die Teilnehmer eher bereit Daten im Tausch für einen wahrgenommenen Mehrwert des Dienstes zu teilen (M = 3,31; sd = 1,41). Den stärksten Anreiz zur Steigerung der Bereitschaft zur Datenweitergabe stellte jedoch Transparenz dar. Mit der Aussicht auf eine transparente sowie der expliziten Angabe des Datenempfängers gaben die Teilnehmer eine erhöhte Bereitschaft zur Datenpreisgabe an (M = 3,69; sd = 1,35). So zeigt sich im Einklang mit den obigen Befunden zu den Einflussfaktoren auf die Bereitschaft zur Datenpreisgabe, dass Transparenz, Vertrauenswürdigkeit und ein ersichtlicher persönlicher Nutzen eines Mehrwertdienstes grundlegend für die Gestaltung eines Datenaustauschs im Sinne der Nutzer sind. Die hiesigen Ergebnisse legen nahe, dass eine solche Ausgestaltung für Entertainmentdienste schwieriger wird als für Dienste, die die Bedürfnisse nach Effizienz und Sicherheit bedienen.

7.2.2. Qualitative Nutzerstudie Uni Hohenheim

Eine Erkenntnis bisheriger Projekte zur Nutzerperspektive auf Datenschutz im Internet liegt darin, dass man neben Befragungen zu Einstellungen und Handlungsbereitschaft auch den konkreten alltäglichen Umgang von Nutzern mit Möglichkeiten zum Schutz ihrer Privatheit untersuchen sollte. So schrieb das Konsortium des vom Bundesministerium für Bildung von Forschung (BMBF) geförderten acatech-Projekts in seinem Schlussbericht (2013, p. 24[31]) „Eine Untersuchung der alltäglichen Privatheitspraktiken der Nutzerinnen und Nutzer im Internet wäre [...] stärker zu fördern, um so noch konkretere Aussagen über etwaige, zukünftig entstehende Umgangsformen und Problemlagen treffen zu können.„ Das vernetzte Fahrzeug ist aus den bereits in der Einleitung dieses Kapitels erwähnten Gründen ein solches gerade im Entstehen begriffenes Phänomen mit einer Vielzahl an Problemlagen, die ohne Berücksichtigung des alltäglichen Nutzungskontextes schwer auf Basis von Nutzereinstellungen oder -intentionen zu verstehen sind. So können bestehende Datenschutzbedenken, die etwa bei telefonischen Repräsentativbefragungen geäußert wurden, in der Nutzungssituation im Auto an Bedeutung verlieren, weil das Auto selbst als geschützter Raum wahrgenommen wird. Weiter ist das Verhalten im Auto als gewohnter Alltagsraum so stark habitualisiert, dass auch Absichten zum aktiven Selbstdatenschutz daran scheitern können, dass in den gewohnten Abläufen kein Raum und keine Gelegenheit ist, um Datenschutzeinstellungen zu treffen. Drittens ist das Auto etwa im Gegensatz zum persönlichen Smartphone ein sozialer Raum, der häufig von einer Vielzahl an Personen geteilt wird. Jeder, dessen Privatheit potentiell gefährdet ist, ist aber nicht in gleichem Maß an Entscheidungen zum Selbstdatenschutz beteiligt. Um solchen Einflussfaktoren in der Komplexität alltäglicher Technikknutzung gerecht zu werden, wurde eine qualitative Befragungsstudie zur Exploration von Sicht- und Verhaltensweisen zum Selbstdatenschutz mit frühen Nutzern vernetzter Autos durchgeführt Kernfragen dabei waren:

- Wie nehmen sie die Problematik des Selbstdatenschutzes überhaupt war? Welche Vorstellungen vom Datenaufkommen, -speicherung, -übermittlung usw. bestehen, welche positiven oder bedrohlichen Assoziationen haben die Nutzer mit Vernetztheit, welches Problembewusstsein tritt ungefragt zutage?
- Welche Erwartungen und Einstellungen zum Datenschutz haben die Nutzer? Auf welche Weise unterscheiden sie unterschiedliche anfallende Datentypen in ihrer Sensibilität, auf welcher Basis beurteilen sie die Bedrohlichkeit, die von unterschiedlichen Akteuren wie Autoherstellern oder App-Anbietern ausgeht?
- Welche Strategien und Verhaltensweisen zum Schutz ihrer Daten wenden sie an? Welche Strategien sind ihnen bekannt, warum bedienen sie sich dieser oder lassen sie ungenutzt?

7.2.2.1. Methode

7.2.2.1.1. Stichprobe Die Teilnehmer wurden über verschiedene Online- und Offline-Kanäle, wie zum Beispiel Vereine oder Auto-Foren rekrutiert. Voraussetzung für die Teilnahme an der Studie war die zumindest gelegentliche Nutzung eines Fahrzeuges samt dazugehöriger Connected-Car-Plattform (mercedes me connect, audi connect, BMW ConnectedDrive, etc.). Außerdem sollten mindestens zwei unterschiedliche Typen von Anwendungen des Dienstes verwendet wer-

[29] FIA What Europeans think about connected cars. 2016.
[30] Danezis, George/Lewis, Stephen/Anderson, Ross J How much is location privacy worth? In WEIS. Band 5, Citeseer 2005.
[31] Acatech (Hrsg.) Privatheit im Internet.Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten. Springer Berlin Heidelberg, 2013.

den aus den Kategorien Navigation, Car remote, Unterhaltungsangebote, Kommunikation, Concierge-Service, Mitfahrer-Wlan oder sonstige Apps.

Alle Teilnehmer erhielten für ihre Teilnahme eine Aufwandsentschädigung von 30 Euro.

Insgesamt konnten 17 Personen befragt werden, davon zwölf Männer und fünf Frauen. Die Altersspanne betrug zwischen 20 und 58 Jahren. Die genaue Verteilung kann Tabelle 7.1 entnommen werden.

Tabelle 7.1: Alters- und Geschlechterverteilung der Teilnehmer

	18-24	*25-34*	*35-44*	*45-60*	Σ
männl.	4	6	0	2	12
weibl.	1	1	2	1	5
Σ	5	7	2	3	17

Vier der Teilnehmer lebten allein, alle anderen gaben an in einem Haushalt mit mehreren Personen zu leben. Des Weiteren befassten sich die Befragten teilweise beruflich mit der Thematik (sieben Befragte arbeiteten entweder in der Automobil- oder der IT-Branche), die meisten haben jedoch nur privat mit den vernetzten Fahrzeugen zu tun. Somit nutzte der größte Teil der Befragten das Fahrzeug auch rein privat.

Die Mehrzahl der Befragten waren Angestellte, drei gaben an, zu studieren oder noch in der Ausbildung zu sein, und ein Teilnehmer war selbstständig.

Sieben Personen in der Stichprobe fuhren einen Mercedes, vier einen BMW und drei einen Audi. Zusätzlich waren auch Fahrer der Marken VW, Opel und Ford mit jeweils einer Person in der Stichprobe vertreten.

7.2.2.1.2. Ablauf der Befragung An der Erhebung waren jeweils zwei Interviewer beteiligt. Ein Interviewer war für die Gesprächsführung hauptverantwortlich, der andere bediente die Videokamera. Gefilmt wurde vom Beifahrersitz aus, während der andere Interviewer vom Rücksitz aus die Fragen stellte. Es wurde nur in den Fällen das gesamte Interview gefilmt, bei denen der zweite Teil der Befragung auch im Auto stattfand. Andernfalls wurde zumindest vom ersten Teil der Befragung ein Video aufgenommen. Neben der Filmaufnahme wurde zudem eine Audioaufnahme angefertigt. Durchschnittlich dauerte das Interview circa 53 Minuten.

Die Befragung wurde in zwei Teile gegliedert. Im ersten Teil ging es um die Vorführung der Nutzung des Connected-Car-Dienstes. Hierzu wurde der Proband gebeten mit den Interviewern eine alltägliche, kurze Fahrt von ca. 10 Minuten Dauer zu machen. Während der Fahrt wurden die einzelnen genutzten Angebote angesprochen und jeweils nach der Funktion, der spezifischen Nutzungssituation, der Usability sowie der dahinter steckenden Datenlogistik gefragt. Im Anschluss wurde der Proband gebeten zudem zu erläutern, welche Dienste er nicht nutzt und weshalb er diese nicht verwendet.

Im zweiten Teil wurde die Befragung je nach Wunsch des Teilnehmers direkt im geparkten Auto oder an einem anderen Ort fortgeführt. Zunächst wurde der Teilnehmer nach seinem Verständnis von vernetzten Autos befragt. Anschließend wurde er gebeten, den Adoptionsprozess, also die Wahrnehmung, Kaufentscheidung, Einrichtung und Alltagsintegration des Dienstes zu beschreiben. Der letzte Teil der Befragung behandelte das Thema Datenschutz. Die Teilnehmer wurden etwa dazu befragt, wie transparent die Kommunikation der Hersteller in Bezug auf Datenschutz war und welche Kontrollmöglichkeiten sie wahrgenommen haben. Außerdem wurde gefragt, für wie sensibel die Befragten unterschiedliche Datentypen hielten und welche Gefahr sie in den einzelnen Anbietern sahen. Zum Schluss wurden die Befragten gebeten, den Vergleich zwischen Datenschutz im Social Web und Datenschutz im vernetzten Fahrzeug herzustellen.

Im Anschluss an die mündliche Befragung wurde von den Teilnehmern ein kurzer Fragebogen zu ihrer Person (Tätigkeit, Alter, usw.) ausgefüllt.

7.2.2.2. Befunde

7.2.2.2.1. Ohne explizite Ansprache eher geringes Problembewusstsein für Datenschutzfragen Wenn sie nicht aktiv darauf angesprochen wurden, artikulierten die Teilnehmer keine Datenschutzbedenken. In wenigen Fällen löste aber schon eine reine Verständnisfrage nach dem Verbleib der Daten kritische Anmerkungen aus. So etwa in der Antwort eines Nutzers von Spotify über ConnectedDrive auf die Frage „Wo, denkst du, werden die [Daten] gespeichert?“: „Also allein schon, dass eine App auf eine andere App zugreifen kann, ist ja schon eigentlich so eine Sicherheitslücke [...] Dass hier geheim irgendwelche Daten gespeichert werden, wo ich hinfahre oder sowas, das will ich den Autoherstellern mal nicht unterstellen, aber mir ist bewusst, dass das alles theoretisch machbar ist.“ *(Teilnehmer 9; ConnectedDrive)*.

Selbst wenn im Rahmen der Vorführung der im Auto verfügbaren Dienste durch die Befragten Optimierungswünsche ausgesprochen wurden, beschränkten sich diese weitgehend auf die Ausweitung bestimmter Funktionen und eine Verbesserung der Usability. Diese Wünsche stellten teilweise eher Herausforderungen für den Datenschutz dar. Ein solcher Wunsch, der prinzipiell mit Datenschutz konfligieren konnte, war der nach mehr Personalisierung. So sagte ein Teilnehmer: „Das gibt auch einen Newsletter für Mercedes me, ja, die kann ich anschauen [...]. Also das wird tatsächlich interessant, wenn sie immer mehr Nutzerdaten über mich haben, die Interessen, wo man dann wirklich eine one to one communication aufbauen kann." *(Teilnehmer 15; mercedes me connect)*. Ein weiterer Befragter äußerte den Wunsch nach mehr Integration mit anderen vernetzten Lebensbereichen: „Später finde es auch mal interessant, Vernetzungen vielleicht zum Haus [...] sowas halt: im Haus [ist es] 20 Grad, [...] ich steig ins Auto ein, hab da auch schon 20 Grad, so dass man irgendwie die Lebenswelt nachher überbrücken kann." *(Teilnehmer 15; mercedes me connect)*. Die mit einer solchen Vernetzung verbundene Öffnung von Schnittstellen stellt prinzipiell eine Herausforderung für den Datenschutz dar. In diesem Sinne als zumindest bedenklich könnte auch der Wunsch nach mehr Öffnung gegenüber Drittanbietern verstanden werden: „Jedes normale Handy kann diese Dinge eigentlich auch bieten, natürlich nicht mit so einem schönen Display [...]. Hier muss ich noch zusätzlich diese Grundgebühr bezahlen und habe eigentlich einen Dienst, der von VW bereitgestellt wird oder eingekauft wird, der eigentlich nicht ganz den Ansprüchen genügt, die ich hätte." *(Teilnehmer 6; Car-Net)*. Ergänzt sei an dieser Stelle, dass die Öffnung für Drittanbieter auch große Vorteile für den Selbstdatenschutz bringt, indem sie den Nutzern Wahlmöglichkeiten zwischen mehr oder weniger datenschutzfreundlichen Angeboten eröffnet (siehe dazu auch den Punkt „Mangel an Alternativen" unten).

Wenn Datenschutz aktiv angesprochen wurde, so geschah dies teilweise auch in einer dem Datenschutz kritischen Perspektive: „Ich würde es cool finden, wenn sich so alle Autos miteinander ein bisschen verständigen würden und dass man dann auch irgendwelche Staumeldungen, Vollsperrungen und so entsprechend, dass das dann vielleicht aufs Navi gebracht wird, [...] aber ich weiß nicht, ob das aus Datenschutzgründen oder so irgendwie so weit kommen kann. Aber das wäre eine schöne Sache." *(Teilnehmer 1; OnStar)*

Wurden die Befragten dann aktiv auf die Problematik des Datenschutzes angesprochen, dann kamen auch Bedenken und Sorgen zum Ausdruck.

> Interviewer: „Siehst du Vor- oder Nachteile wenn du weißt, Mercedes hat Zugriff auf diese Daten?"
>
> Befragter: „Sowohl als auch. Also ich denk, dass das klar auch irgendwo Nachteile sind, weil, wie gesagt, gläserner Mensch, es wird immer offensichtlicher, man kann auf viel mehr zugreifen, man weiß eigentlich durch Kameras und solche Ortungssysteme oder weiß Gott noch was, man weiß mit solchen Möglichkeiten einfach, wann, wie, wo was stattfindet, man kann dich wahrscheinlich auch abhören, was sprichst du, ist es für die irgendwie relevant oder so." *(Teilnehmerin 17, mercedes me connect)*

Auch an dieser Stelle ist jedoch bemerkenswert, dass die Bedenken häufig relativiert wurden.

7.2.2.2.2. Geringschätzung der Sensibilität der Daten Zum einen spielten die Befragten die Sensibilität der potentiell gefährdeten Daten herunter. Dabei wurden Argumente genannt, die auch aus der Internet-Privatheitsforschung gut bekannt sind, nämlich besonders, dass man selbst nicht zu verbergen habe (Solove, 2007[32]). Zum anderen wurden die im Fahrzeug anfallenden Daten als weniger sensibel dargestellt als Daten, die etwa in sozialen Netzwerken aufkommen. So erklärte eine Befragte: „Ich glaub, wir gehen da relativ locker mit um im Auto. Also bei Facebook zum Beispiel ist es wirklich so, dass nur Freunde irgendwas sehen können, weil man ja auch Fotos sieht, jetzt Fotos von uns, Fotos vom Hund. Ich würd nie Fotos von einem Kind reinsetzen, und aber da ist es halt ja einfach, [... jemand, der jetzt in irgendeiner Zentrale sitzt, kann mich als Person, hoffe ich, nicht zuordnen." *(Teilnehmerin 13; Audi connect)*. Die Hierarchie der involvierten Daten von wenig bis stark sensibel lässt sich etwa so beschreiben: Am wenigsten problematisch erschienen technische Fahrzeugdaten, danach kamen Daten zur Nutzung des Entertainment-Systems, dann Standortdaten, und als bereits stärker problematische Daten Kontaktdaten. Am problematischsten wurden Inhalte von persönlichen Gesprächen betrachtet, wie sie zwischen Passagieren im Auto oder über die Bluetooth Telefonverbindung anfallen.

7.2.2.2.3. Geringschätzung der Gefahr durch Anbieter Ein anderer Aspekt, gegenüber dem die Befragten wenig Beunruhigung zeigten, war die Gefahr, die von den hinter den Diensten stehenden Akteuren ausgehen könnte. Auch hier spielten sowohl Wahrnehmungen eine Rolle, die aus anderen Bereichen wie der Internetforschung bekannt sind, als auch Auto-spezifische Wahrnehmungen. Wie schon aus dem Umgang mit Internetkonzernen bekannt, scheinen die Nutzer auch beim Auto durch ein Gefühl der Unpersönlichkeit beruhigt gegenüber der Größe der Konzerne, die sie vielleicht überwachen könnten. „Also, ich find einfach, durch diese Großkonzerne (Pause) ich persönlich bin da schon so jemand,

[32] Daniel, J. Solove I've got nothing to hide'and other misunderstandings of privacy. San Diego Law Review, 44 2007.

der mal gerne, wenn er irgendwas wissen will, einfach das auf Google eingibt und so weiter. Und da ist es mir egal, wenn die irgendwelche Daten dann weltweit sammeln.“ *(Teilnehmer 12; Audi connect)*. Darüber hinaus war das Misstrauen gegenüber den Autokonzernen aber noch einmal deutlich geringer als gegenüber etwa Google und Facebook. Hier wurde etwa auf das geringere wirtschaftliche Interesse an der Verwendung privater Daten durch Autohersteller verwiesen: „Google und Apple, deren Kapital sind die Daten, und bei einem Automobil-Hersteller [. . .] deren Kapital ist das Produkt. Also der Automobil-Hersteller möchte sein Produkt optimieren, Google und Apple möchte nur maximale Daten sammeln und mit diesen Daten Kapital dann erzeugen, also sprich Geld verdienen.“ *(Teilnehmer 14; mercedes me connect)*. Mehrere Befragte sahen auch einen Grund zur Beruhigung darin, dass sie den Autoherstellern das Know-how zur Ausbeutung erhobener Daten absprachen: „Aber ich denke, dass VW, schon von der Qualität ihrer Software, die sind gar nicht in der Lage, diese [Lachen] Daten sinnvoll zu verwenden.“ *(Teilnehmer 6; Car-Net)*. Starkes Vertrauen brachten auch die renommierten Marken der Anbieter mit sich sowie die persönliche Beziehung zum Händler: „Dadurch, dass man halt eine persönliche Bindung irgendwie hat, auch durch den Autohändler, neigt man schon dazu, da ein bisschen mehr Vertrauen reinzustecken“ *(Teilnehmer 9; ConnectedDrive)*.

Ein vierter Aspekt, der auch das Vertrauen in den Umgang mit persönlichen Daten stärkte, war das große Vertrauen, dass Autofahrer in den physischen Schutz durch das Auto hatten. Dies kommt etwa bei dem folgenden Austausch zum Ausdruck, indem der Befragte eine Frage zur Datensicherheit auf die physische Sicherheit bezog:

> Interviewer: „Und ist das Auto für dich auch [...] ein persönlicher Raum, also siehst du dich hier [...] in deiner Privatsphäre geschützt?“
>
> Befragter: „Ich fühl mich, ehrlich gesagt, sehr sicher in diesem Auto, weil, wenn ich mir nicht sicher wäre, würde ich nicht auf Autobahn gehen und mit 240, 250 Sachen durchrasen. Also ich vertrau dem Auto komplett.“ *(Teilnehmer 2; mercedes me connect)*

Ging es bis zu diesem Punkt um die Wahrnehmung der Problematik und Gründe für die Geringschätzung der Gefahren durch die Nutzer, so konzentrieren wir uns in den folgenden Abschnitten auf tiefer liegende Probleme, die einem effizienten Selbstdatenschutz auch dann im Weg stehen würden, wenn die Nutzer dem Thema mehr Aufmerksamkeit und Sorge schenken würden.

7.2.2.2.4. Mangel an Alternativen Viele Befragte wiesen darauf hin, dass sie ohnehin wenig Optionen zum Schutz ihrer Daten hatten, sofern sie die Vorteile vernetzte Autos nutzen wollten. So sagte ein Teilnehmer: „Sie wollen den Service nutzen, also müssen Sie auch eine entsprechende Datenschutz-Erklärung mit unterschreiben„ (Teilnehmer 14; mercedes me connect). Die Datenschutzerklärung stellte hier also in der Wahrnehmung des Nutzers nicht eine Informationsgrundlage dar, die ihm bei Entscheidungen zum Schutz seiner Daten helfen könnte, sondern den Preis, den er zahlen musste, um den Dienst nutzen zu können.

Ein Mangel an Alternativen äußerte sich etwa in dem Moment, in dem man eine App zur Steuerung eines bestimmten Dienstes herunterlädt: „Ich kann am Anfang, glaube ich, sagen, wenn ich die App runterladen will, kann ich auf irgendwas zustimmen, wenn ich das nicht mache, kann ich die App auch nicht runterladen, also viel Möglichkeiten hab ich nicht. (lachend gesprochen)“ (Teilnehmer 9; ConnectedDrive). Diese Problematik ist natürlich schon von den App-Märkten in der Mobilkommunikation bekannt. Da im vernetzten Auto aber für viele Funktionen tatsächlich nur eine App verfügbar ist, erleben die Nutzer die Alternativlosigkeit teilweise noch stärker, weil sie nicht nur innerhalb einer App gegeben ist, sondern auch in Hinblick auf andere Apps.

Dass mögliche datensparsame Alternativen von Standard-Nutzungsweisen innerhalb von Angeboten durchaus von den Nutzern aufgegriffen wurden, ließ sich zumindest aus manchen Äußerungen ableiten. So aus dem folgenden Dialog, indem der Interviewer eine Möglichkeit zum punktuellen Löschen der Ortshistorie des Navigationsgerätes ansprach.

> Interviewer: „Also dir fehlt’s auch nicht, dass du jetzt zum Beispiel beim Navi vielleicht bei manchen Zielen sagen könntest, nee, da will ich jetzt nicht, dass die Daten gespeichert werden.“
>
> Befragter: „[...] Wenn sie die speichern und das eine Option wäre, dann wäre das schon interessant, ja.“ *(Teilnehmer 9; ConnectedDrive)*

7.2.2.2.5. Mangel an Gelegenheiten zum Selbstdatenschutz Eine weitere Herausforderung für den Selbstdatenschutz ergibt sich aus dem Mangel an Situationen, in denen die Nutzer ihn effektiv einsetzen könnten.

Ein erstes Problem ergibt sich dadurch, dass es manchmal nicht die Nutzer selbst waren, die die Nutzungsbedingungen gelesen und akzeptiert hatten. Stattdessen wurde dies von einem in der Technik versierten Freund gemacht:

> Interviewer: „Gab es da Nutzungsbedingungen am Anfang, die man unterschreiben musste?“

> Befragter: „Nur akzeptieren über die Website, aber das hat ein Bekannter für uns gemacht." *(Teilnehmerin 17; mercedes me connect)*

Auch vom Prozess in der Anschaffung eines Autos her gedacht, scheinen die Situationen, in denen Selbstdatenschutz-Entscheidungen getroffen werden, nicht besonders gut für das kritische Auswählen zwischen Alternativen geeignet. Ein solcher Moment ist die Kaufabwicklung, wenn man nach der Kaufentscheidung verschiedene Unterlagen unterschreiben muss. Erfahrungsgemäß handelt es sich bei diesem Prozess um eine Formalität, da alle Details vorher bereits mit dem Händler ausgehandelt wurden. In Hinblick auf die Auswahl und die Konfiguration des Autos hatten die Nutzer bereits alle Entscheidungen getroffen, sie überprüften nur noch die Richtigkeit der Dokumente. Dies kam im folgenden Austausch zum Ausdruck:

> Interviewer: „Gab es da irgendwelche Nutzungsbedingungen, die Sie bestätigen mussten? „
>
> Befragter: „Definitiv ja, dass ich da gewisse Dokumente unterschreiben musste vor Ort. Sie wissen selber, Sie kriegen dann einen Wust an Papieren, Sie wollen den Service auch nutzen." *(Teilnehmer 14; mercedes me connect)*

Die Händler spielten in diesem Prozess eine zwiespältige Rolle. Einerseits sind sie, wie oben dargestellt, als Experten auch Vertrauenspersonen der Kunden und häufig die einzigen Fachleute, mit denen diese es im Kaufprozess zu tun hatten. Andererseits waren sie am Verkauf möglichst umfangreicher digitaler Angebote interessiert. So ergab sich der nachfolgend wiedergegebene Eindruck, zu einer einem selbst nicht einsichtigen Konfiguration überredet worden zu sein: „Mein Vater hat damals das Auto konfiguriert, ich war da dabei dann, beim Händler, das wird natürlich alles angepriesen, das hab ich ja vorher auch schon gesagt, aber was das dann (Pause) am Ende hat man es bestellt, der Verkäufer ist zufrieden, der hat mehr verkauft wie er wollte, und dann war's das. Man weiß jetzt nicht, wie kann das (Pause) was beinhaltet das jetzt alles und bla, bla. Es ist einfach nicht transparent genug, um das jetzt genau sagen zu können, was das jetzt alle NOCH beinhaltet, NOCH für Funktionen, das ist (..) noch sehr schwammig irgendwie." *(Teilnehmer 9; ConnectedDrive)*.

Aus der Online-Privatheitsorschung heraus empfiehlt es sich auch, Nutzer Entscheidungen über Selbstdatenschutz jeweils in genau der Situation treffen zu lassen, in der sie bestimmte Informationen preisgeben müssen. Die Sensibilität bestimmter Daten ergibt sich nämlich häufig erst aus dem Kontext heraus und kann auch nur in diesem Kontext abgeschätzt werden (Nissenbaum, 2010[33]). Hier ergibt sich aber beim Auto die Herausforderung, die mit der Fahraufgabe beschäftigten Nutzer nicht zu überfordern. Tatsächlich erlebten die Befragten Nutzer aufpoppende Datenschutzmeldungen als Ablenkung, allerdings auch, weil sie tatsächlich häufig in der Situation keine wirkliche Wahl darstellen, sondern eher als eine Absicherung der Anbieter gegenüber den Fahrern wahrgenommen wurden. Zu dem bereits oben erwähnten Problem, dass Nutzer sich zu selten vor wirklichen Alternativen sehen und zu häufig zum Akzeptieren von Bedingungen gezwungen sehen, kommt hier das Problem, dass ein Popup-Fenster gerade im Auto eine unpassende Art der Durchführung eines Nutzerdialogs ist. So sagte ein Befragter: „Ich sage mal so, wenn mehr Transparenz vorliegen würde, dann könnte man schon mal davon ausgehen, wie die aussieht. Nämlich da [...] poppt dann irgendwas auf, liest sich eh kein Mensch durch, drückt auf okay, und das wars. Das sollte man sich vielleicht auch als Hersteller ein bisschen mehr überlegen, wie wie man diese Information den Leuten bereitstellen kann." *(Teilnehmer 9; ConnectedDrive)*.

7.2.2.2.6. Privatheitszynismus Ein letzter Faktor, der einem erfolgreichen Selbstdatenschutz im Weg steht, liegt auf einer viel tieferen Ebene als die hier bisher genannten und wird sich auch nicht im Rahmen der Automobilbranche allein beheben lassen: ein lähmendes Gefühl der Ohnmacht gegenüber der Überwachung von digitaler Kommunikationstechnik insgesamt. Beinahe in jedem Gespräch wurde auf eine allumfassende Überwachung verwiesen, vor der man sich ohnehin nicht schützen könne. Diese Grundstimmung, die beinahe in sämtlichen Interviews zum Ausdruck kam, geht aus dem folgenden Dialog gut hervor:

> Befragter: „Ich mache mir jetzt keine Illusionen, dass das irgendwie, auch beim iPhone, auch wenn ich den PC benutze und es heißt, es sind sichere Verbindungen und abhörsichere Verbindungen, da kann immer jemand mithören. Also deshalb, da mache ich mir jetzt keine Illusionen. Wenn ich mich am Telefon unterhalte oder auch mit dem Audi, jetzt im Audi, wenn ich da telefoniere, dass das was völlig Privates ist oder (Pause)
>
> Interviewer: Aber du würdest deine Nutzung jetzt deswegen nicht verändern?
>
> Befragter: Nein, ich denke, in dem Moment, wo ich jetzt an dieser modernen Welt teilnehmen will, muss mir bewusst sein, dass die/ also dass da wenig privat ist. *(Teilnehmer 11, Audi connect)*

Diese Sichtweise, in der Internet-Forschung als „Privacy Cynicism" (Hoffmann, Lutz & Ranzini, 2015[34]) oder „Online

[33] Nissenbaum, Helen A contextual approach to privacy online. Stanford University Press, 2011.

[34] Hoffmann, Christian Pieter/Lutz, Christoph/Ranzini, Giulia Privacy Cynicism : An Approach to Understanding the Institutional Privacy Paradox. In Amsterdam Privacy Conference. APC, Oktober 2015.

Apathy“ (Hargittai &Marwick, 2016[35]) bezeichnet, wird u.a. auf Erfahrungen mit der Machtlosigkeit gegenüber dem Diktat von Nutzungsbedingungen durch Internetkonzerne zurückgeführt sowie auf die massive Berichterstattung über Überwachung durch Regierungen und Unternehmen (von Pape, Trepte & Mothes im Druck[36]). Diese Erfahrungen wiederholen sich aber häufig auch im Umgang mit den autobezogenen Angeboten. Dies kam auch in dem folgenden Zitat eines Nutzers zum Ausdruck: „Wenn ich mich bei diesem MyAudiPortal anmelde - [man] muss zwei drei, vier Häkchen setzen, Datenschutzerklärung und hast du nicht gesehen, also letztendlich werden mit Sicherheit meine kompletten (Pause) meine Anschrift, Telefonnummer, Kontaktdaten usw. gespeichert und mit Sicherheit auch im Hintergrund entsprechend halt auch die Ziele, die ich anwähle und auch die Fahrten in irgendeiner Form gespeichert, ja. Letztendlich ist mir bewusst, dass ich dadurch komplett gläsern bin und man das komplett zurück verfolgen könnte, wo ich mich, was weiß ich, im letzten halben überall rumgetrieben habe.“ *(Teilnehmer 12; Audi Connect).*

Es zeigt sich: Möchte man die Nutzer als Konsumenten tatsächlich für einen Teil des Schutzes ihrer Daten in die Pflicht nehmen, dann muss man sie auch in eine Rolle versetzen, in der sie souverän im eigenen Interesse Entscheidungen treffen können. Das bedarf des Vorhandenseins wirklicher Alternativen, zwischen denen sie unter Abwägung der Datenschutzaspekte in dafür geeigneten Situationen wählen können. Es bedarf aber auch einer Grundstimmung der Selbstwirksamkeit und der Verbindlichkeit in Sachen Datenschutz. Selten klang aus den Äußerungen der Befragten ein Vertrauen in die rechtlichen und technischen Rahmenbedingungen hervor, das eigentlich Voraussetzung ist, damit sie selbst für den Schutz ihrer Daten eintreten können. Ein solches Beispiel ist das folgende Zitat auf die Frage hin, ob man sich vor dem Zugriff von Versicherungen auf die persönlichen Fahrdaten Sorge: „Ich denke es ist ausgeschlossen, dass sie das an die Versicherungen weiterleiten, aufgrund der Datenschutzbestimmungen.“ *(Teilnehmer 9; ConnectedDrive).*

7.2.3. Repräsentativbefragung Uni Hohenheim

Während die bereits vorgestellte qualitative Befragung der Universität Hohenheim ein ganzheitliches Bild davon gab, wie 18 Nutzer die Datenschutzproblematik in ihrem Alltag erleben und damit umgehen, wurden in der Repräsentativbefragung einzelne Aspekte in zwei Richtungen vertieft.

Es sollte untersucht werden,

- wie datenschutzbezogenes Wissen, sowie datenschutzbezogene Bedenken und andere Einstellungen zu vernetzten Fahrzeugen unter allen in Deutschland lebenden Autofahrern verteilt sind;
- wie sehr unterschiedliche Bevölkerungsgruppen in ihrer Beurteilung von Angeboten auf Lösungen zum Selbstdatenschutz achten, und inwiefern Selbstdatenschutz sich hier von anderen Anhaltspunkten unterscheidet, wie etwa unabhängige Gütesiegel zum Datenschutz, Anonymisierung und Verschlüsselung oder die datenschutzbezogene Reputation eines Unternehmens;
- wie Wissen, Bedenken und andere Einstellungen und Wahrnehmungen einander gegenseitig beeinflussen und welchen Einfluss sie auf Entscheidungen über die Nutzung der Technik haben können.

Dafür wird zunächst das methodische Vorgehen erläutert.

7.2.3.1. Stichprobe

Die Befragung wurde von Ende November bis Anfang Dezember 2017 vom Institut Kantar Public (vormals TNS Infratest) als computergestützte Telefonbefragung durchgeführt. Die Stichprobe war eine Zufallsauswahl aus der Basisstichprobe der Arbeitsgemeinschaft Deutscher Marktforschungsunternehmen (ADM Master-Sample). Diese gilt allgemein als der Standard zur Erreichung einer Repräsentativität für die deutsche Bevölkerung[37]. Von den insgesamt 1.010 Interviews wurden 708 Interviews per Festnetz geführt und 302 (30%) via Mobilfunk. Durch die per Mobilfunk geführten Interviews konnte sichergestellt werden, dass auch die Sichtweisen von Personen berücksichtigt werden, die keinen Festnetzanschluss hatten.

Unter den Befragten waren 445 Frauen und 565 Männer. Das Alter variierte zwischen 18 und 89, mit einem Durchschnittsalter von 53. Siebzehn Prozent der Befragten hatten einen Hauptschulabschluss, 28,5% die mittlere Reife oder

[35] Hargittai, Eszter/Marwick, Alice “What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, 10 2016, Nr. 21, ISSN 1932–8036.

[36] Pape, T. von/Trepte, S./Mothes, C. Privacy by Disaster? Press Coverage of Privacy and Digital Technology. European Journal of Communication.

[37] Heyde, C. von der Die ADM Stichproben für Telefonbefragungen. https://www.adm-ev.de/telefonbefragungen/?L=1%2525252527%252529, 07 2013.

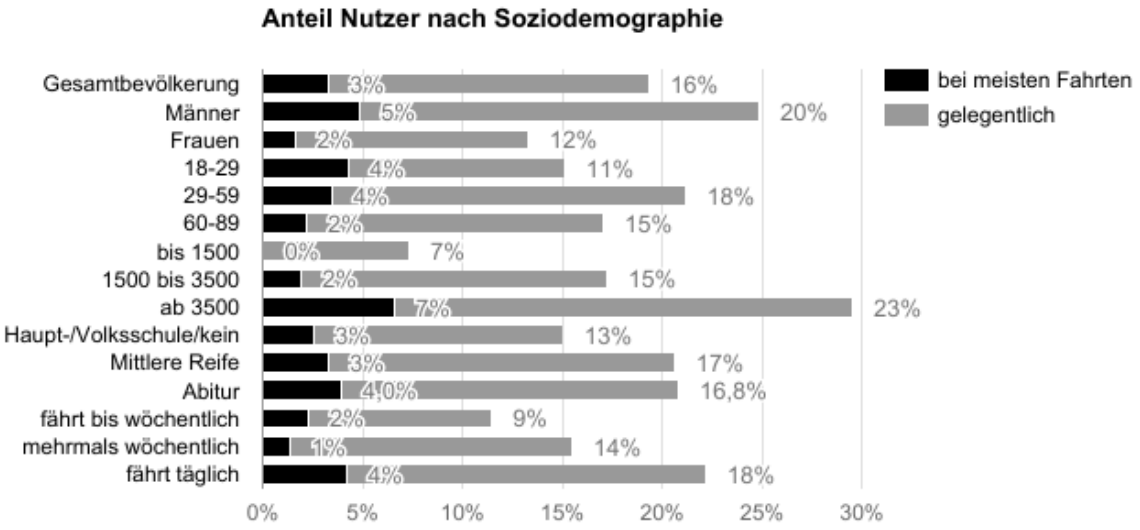
einen äquivalenten Abschluss, 53,8% das Abitur, und 0,4% gaben an, keinen Abschluss zu haben. Die berufliche Situation der Befragten war mehrheitlich eine Erwerbstätigkeit (61%), gefolgt von Dasein als Rentner (29%), Schüler oder Student (3%) und Hausfrau oder Hausmann (2,1%).

7.2.3.1.1. Verteilung von Nutzung und nutzungsbezogenen Einstellungen Die Einstellungen zu Datenschutz und Privatheit im vernetzten Fahrzeug können nicht losgelöst von den allgemeineren Einstellungen bezüglich der Technik und konkreten Angeboten betrachtet werden. Daher wird zunächst kurz darauf eingegangen, in welchem Umfang die Befragten bereits Dienste zum vernetzten Fahren nutzen und welche Einstellungen sie dazu haben.

Nutzung Um einen Anhaltspunkt dafür zu haben, welcher Anteil der Befragten als Nutzer eines vernetzten Fahrzeugs zu verstehen ist, wurden sie zunächst gefragt, ob sie Dienste nutzen, für die ihr Auto auf das Internet zugreift. Dies bestätigten 19% der Befragten. Dazu zählten 3%, die solche Dienste bei den meisten Fahrten nutzen (Abbildung 7.3). Angesichts der grundlegenden Schwierigkeiten, das Angebot „Vernetztes Fahrzeug“ zu definieren, ist eine solche Frage in einem Telefoninterview notwendig verkürzend. Dass nur 2,2 Prozent der Befragten in ihrer Antwort „weiß nicht“ angaben oder nicht antworteten, legt aber nahe, dass sie die Frage durchaus als verständlich empfanden.

Die Nutzung war deutlich höher bei Männern, bei Befragten in einem mittleren Alter (29 bis 59 Jahre), sowie bei Befragten mit höherem Einkommen und höherem Bildungsabschluss. Nutzer vernetzter Fahrzeug-Angebote sind auch stärker vertreten unter Fahrern, die häufiger selbst Auto fahren.

Abbildung 7.3: Anteil der Nutzer vernetzter Fahrzeug-Angebote nach Soziodemographie.



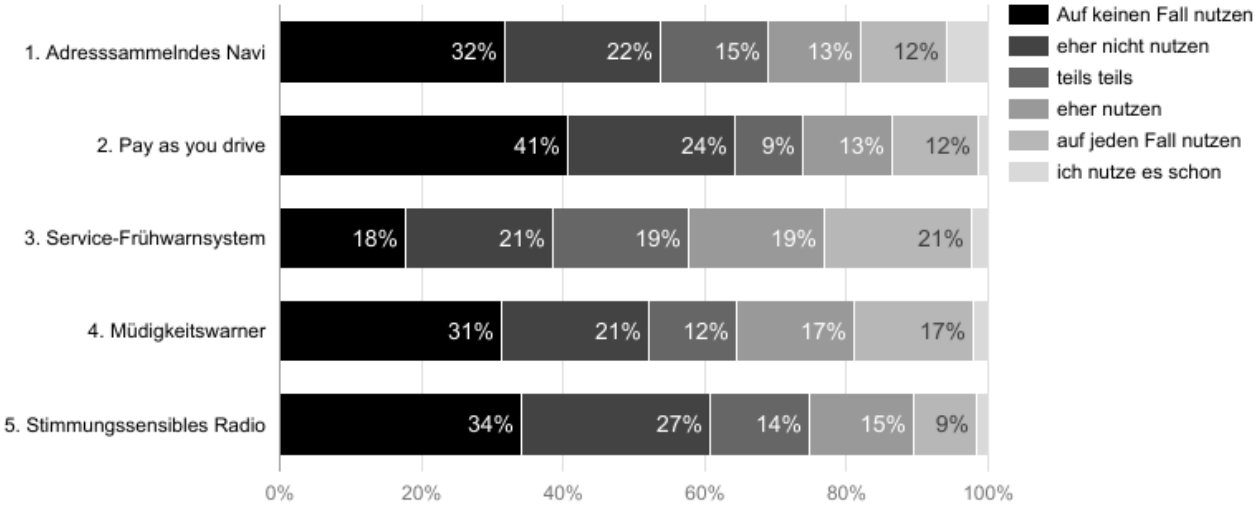
Nutzungsintention zu spezifischen Diensten Um die Einstellungen der Befragten für Angebote vernetzter Fahrzeuge zu erheben, wurden ihnen fünf beispielhafte Dienste genannt (Tabelle 7.2). Diese Dienste sind in grober Anlehnung an die im Projekt entwickelten Use-Cases (s. Kapitel 3) formuliert. Dabei wurden aber auch andere Gesichtspunkte berücksichtigt, wie die einfache Darstellbarkeit und die Abdeckung eines breiten Spektrums an Datenerfordernissen und Funktionalitäten, bis hin zu einem Angebot (Nr. 5) das derzeit nach Kenntnis des Autoren dieser Studie auf dem Markt in der Form noch nicht verfügbar ist.

Zu diesen Diensten wurde zunächst abgefragt, inwieweit man bereit sei, sie zu nutzen - wenn sie zu einem günstigen Preis verfügbar wären. Insgesamt war die Nutzungsintention der Befragten breit gestreut. Für jedes Angebot sagten mindestens 10%, dass sie es auf keinen Fall nutzen würden und mindestens 10%, dass sie es in jedem Fall nutzen würden oder derzeit schon nutzen. Im Schnitt über die fünf Angebote gab ein knappes Drittel (32 %) der Befragten an, die Angebote mindestens „eher nutzen“ zu wollen (Abbildung 7.4).

Tabelle 7.2: Dienste, zu denen die Nutzungsbereitschaft der Befragten erhoben wurde.

Nr.	Beschreibung des Angebots
1	Ein Navigationsdienst, der mögliche Fahrtziele aus den Kontakten in Ihrem Handy ausliest, damit Sie sie nicht selbst eingeben müssen.
2	Ein Versicherungsdienst, der Ihre Fahrweise beobachtet und Ihnen für sichereres Fahren günstigere Tarife gewährt.
3	Ein Frühwarnsystem, das den Hersteller per Funk über alle Auffälligkeiten im Fahrbetrieb informiert, so dass er Pannen noch abwenden oder die Werkstatt informieren kann.
4	Eine Kamera, die Sie als Fahrer überwacht und warnt, wenn Ihnen die Augen zufallen oder Sie sich sonst bedenklich verhalten.
5	Ein Autoradio, das sein Programm an Ihre Fahrsituation und Stimmung anpasst und Ihnen etwa bei Müdigkeit anregende Inhalte vorschlägt.

Abbildung 7.4: Nutzungsintention zu verschiedenen Diensten.



Die Nutzungsabsicht ist bei Männern mit 36,1% Zustimmung zu „eher nutzen“, „auf jeden Fall nutzen“ und „nutze es schon“ höher als bei Frauen (30,5%). Sie ist auch höher bei den Befragten mit Hauptschulabschluss oder keinem Abschluss (35,3%) als bei Befragten mit Mittlerer Reife (26,0%) oder Abitur (27,7%).

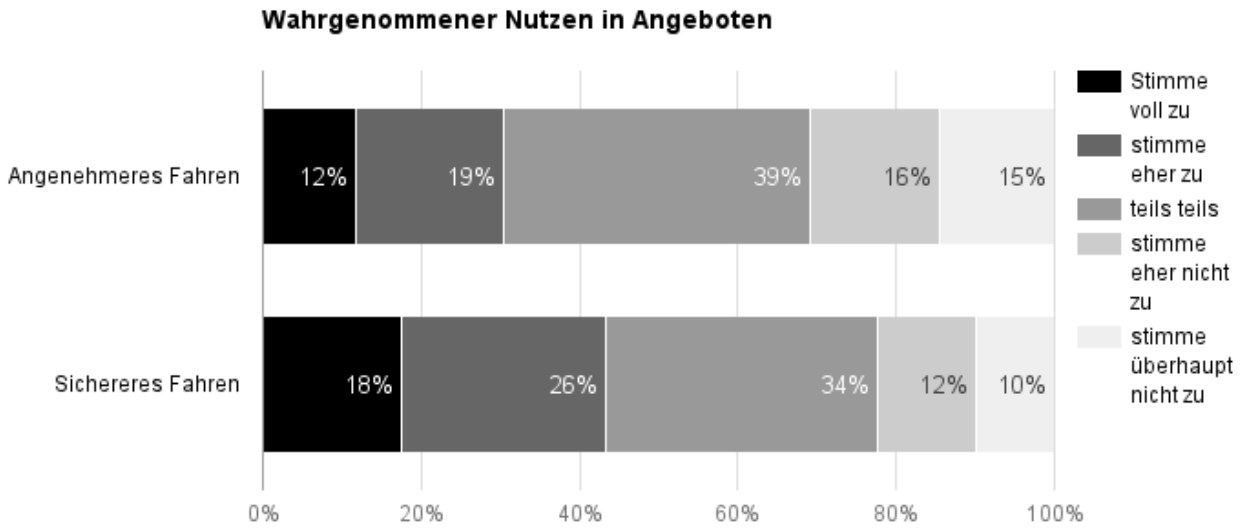
Wahrgenommener Nutzen Als zentraler Einfluss auf die Nutzungsintention – in der Regel vor Privatheitsbedenken – hat sich sowohl in der Literatur als auch in der von der Universität Hohenheim durchgeführten qualitativen Befragung von Nutzern die Einschätzung erwiesen, für wie nützlich man einen Dienst für konkrete Zwecke hält[38]. Konkret wurden die beiden zentralen Nutzungsdimensionen des angenehmen Fahrens und des sicheren Fahrens identifiziert und in der Befragung verwendet. Die Befragten sollten entsprechend angeben, inwieweit sie den Aussagen zustimmen, dass solche Dienste das Autofahren für sie angenehmer bzw. sicherer machen können. Auch hier streuen die Antworten breit (Abbildung 7.5). Die Befragten sahen den Nutzen der genannten Anwendungen tendenziell eher in der Gewährleistung eines sicheren Fahrens (44% eher oder volle Zustimmung) als eines angenehmen Fahrens (31% eher oder volle Zustimmung).

Die deutlichsten Unterschiede zeigten sich zwischen den Geschlechtern: Unter den Männern stimmte ein höherer Anteil mindestens eher zu, dass die Dienste das Fahren angenehmer (34,9%) und sicherer machen (48,3%) als dies unter Frauen der Fall war (25,7% bzw. 37,9%).

7.2.3.1.2. Verteilung von Datenschutzbezogenem Wissen und Einstellungen

[38] vgl. in: Dinev, Tamara/Hart, Paul An Extended Privacy Calculus Model for E-Commerce Transactions. Info. Sys. Research, 17 März 2006, Nr. 1 ⟨URL: http://dx.doi.org/10.1287/isre.1060.0080⟩, ISSN 1526–5536.

Abbildung 7.5: Wahrgenommener Nutzen in Form von angenehmerem bzw. sichererem Fahren



Wissen zu Datenschutz im Fahrzeug Das Wissen der Befragten zum Thema „Privatheit im Vernetzten Fahrzeug“ wurde durch einen Test gemessen. Dieser Test war in Anlehnung an einen etablierten Test zur Messung von Online-Privatheitskompetenz entwickelt (Trepte et al., 2015[39]) und in einer Vorstudie getestet worden. Dabei wurden den Befragten fünf Aussagen zu den Rahmenbedingungen von Datenschutz im vernetzten Fahrzeug vorgelesen, von denen drei wahr und zwei falsch waren (Tabelle 7.3). Die fünf Aussagen bildeten unterschiedliche Formen von Wissen zu Datenschutz und Privatheit im digitalen Zeitalter ab, nämlich Wissen über Datensammlungs- und -auswertungspraktiken, über technische Aspekte des Aufkommens von Daten im Fahrzeug, über mögliche Datenschutzstrategien und über gesetzliche Rahmenbedingungen.

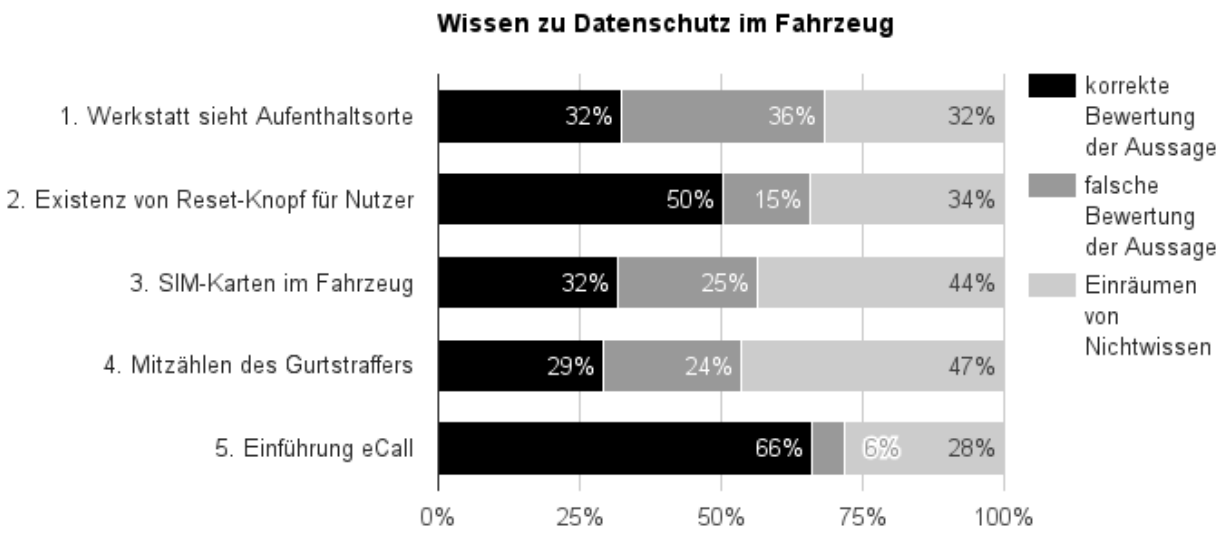
Tabelle 7.3: Aussagen aus Wissenstest.

Nr.	Aussage	wahr/falsch
1	Jede Autowerkstatt kann aus einem Neuwagen auslesen, wo er sich zu welchem Zeitpunkt befunden hat.	falsch
2	Die meisten Autos auf deutschen Straßen haben einen Knopf, über den man als Fahrer alle Fahrzeugdaten außer dem Kilometerstand löschen kann.	falsch
3	Damit sie mit dem Internet kommunizieren können, sind in vielen Neuwagen genau wie in Handies SIM-Karten verbaut.	wahr
4	Heutige Neuwagen speichern ab, wie häufig der Anschnallgurt etwa wegen starken Bremsens straff gezogen wurde.	wahr
5	In den nächsten Jahren soll in sämtliche Europäische Neuwagen ein Sender verbaut werden, der nach Unfällen automatisch einen Notruf absetzt	wahr

Insgesamt zeigt sich eine relativ große Unsicherheit darin, ob diese Aussagen stimmen oder nicht. Allein bezüglich der Einführung des eCall (Aussage 5) lag eine deutliche Mehrheit der Befragten in ihrer Antwort richtig. In ihren Einschätzungen über- und unterschätzen die Befragten teilweise deutlich den Grad, zu dem Daten zum Fahrverhalten aufkommen oder auslesbar sind. So gehen 36% fälschlich davon aus, dass jede Autowerkstatt bei einem modernen Fahrzeug auslesen könne, wo es sich zu welchem Zeitpunkt befunden hat (Abbildung 7.6). Umgekehrt glaubt ein Viertel der Befragten nicht, dass heutige Neuwagen abspeichern, wie häufig der Gurtstraffer aktiviert wurde.

[39]Trepte, S./Masur, P. K. Privatheitskompetenz in Deutschland. Ergebnisse von zwei repräsentativen Studien. https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Team_MP/Berichte/Privatheitskompetenz_2015-11-04.pdf, 11 2015.

Abbildung 7.6: Korrektheit der Bewertungen unterschiedlicher Aussagen zu Datenschutz im Fahrzeug



Die größte systematischen Unterschiede im Wissen lag zwischen den Geschlechtern: Männer lagen im Schnitt bei 2,3 Fragen richtig, Frauen bei 1,9 Fragen. Dieser Unterschied erklärt sich jedoch teilweise daraus, dass Frauen häufiger „weiß nicht“ angaben. Männer haben vermutlich häufiger geraten und lagen damit in der Hälfte der Fälle richtig. Befragte mit Abitur hatten ebenfalls signifikant mehr richtige Antworten (2,23) als Befragte mit Mittlerer Reife (2,04) oder einem niedrigeren Bildungsabschluss (2,02). In Bezug auf das Alter ist die einzige klare Tendenz, dass Befragte im Alter von über 70 Jahren ein deutlich geringeres Wissen hatten (1,76) als die jüngeren Befragten, deren Punkte nach keinem klaren Muster zwischen 1,99 (40-49-jährige) und 2,31 (30-39-jährige) schwankten.

Privatheitsbedenken Bei der Abfrage von Privatheitsbedenken gegenüber den genannten Beispielangeboten wurde hier ein Schwerpunkt auf die Gefahr einer institutionellen Überwachung durch Unternehmen oder Regierungsakteure gelegt. Zusätzlich wurde allgemein abgefragt, für wie besorgt man über eine Gefährdung der Privatsphäre von Nutzern sei. Diese Bedenken sind insgesamt eher stark ausgeprägt. Dabei waren die Bedenken gegenüber einer möglichen Überwachung durch Unternehmen höher als die gegenüber einer Überwachung durch Geheimdienste und staatliche Akteure (Abbildung 7.7).

Unterschiede in den Bedenken ergeben sich wiederum nach Geschlecht und Bildungsniveau: Unter den Frauen äußerten 62,7%, dass sie eher besorgt sind im Vergleich zu 59,7% unter den Männern. Sorgen sind auch stärker verbreitet unter Befragten mit mittlerer Reife (49,3%) und Abitur (46,5%) als unter Befragten mit Hauptschulabschluss oder ohne Abschluss (44,8%). Bezüglich dem Alter zeigt sich eine umgekehrt u-förmige Verteilung: In der untersten Altersgruppe (18 bis 29 Jahre) sind Bedenken bei einer knappen Mehrheit vorhanden (56,4%) im Vergleich zu knapp zwei Drittel unter den 30- bis 69jährigen (64,6%). Am wenigsten verbreitet sind Bedenken zu Privatheit und Datenschutz durch vernetzte Fahrzeuge unter den 70-bis 89jährigen (49,7%).

Achtsamkeit auf datenschutzrelevante Merkmale Privatheitsbedenken können sich einerseits in einer pauschalen Ablehnung von Angeboten äußern, in denen persönliche Daten auf irgendeine Art verarbeitet werden. Sie können aber auch eine höhere Achtsamkeit darauf hervorrufen, was mit den Daten genau geschieht – etwa wer Zugriff darauf bekommt, wie sie gespeichert werden, und wie man ihre Verwendung selbst kontrollieren kann. Dies setzt aber – neben dem Vorhandensein entsprechender Wahlmöglichkeiten – voraus, dass Nutzer auf datenschutzrelevante Merkmale von Angeboten achten. Um festzustellen, inwieweit dies unter den deutschen Autofahrern der Fall ist, wurden ihnen unterschiedliche Formen von Anhaltspunkten angeboten. Insgesamt wurden vier Arten von Anhaltspunkten angesprochen. Die Nutzer sollten jeweils angeben, wie sehr sie bei der Auswahl eines Angebots darauf achten würden (Tabelle 7.4)

Abbildung 7.7: Privatheitsbedenken bezüglich einer Gefährdung der Privatsphäre allgemein und Überwachung.

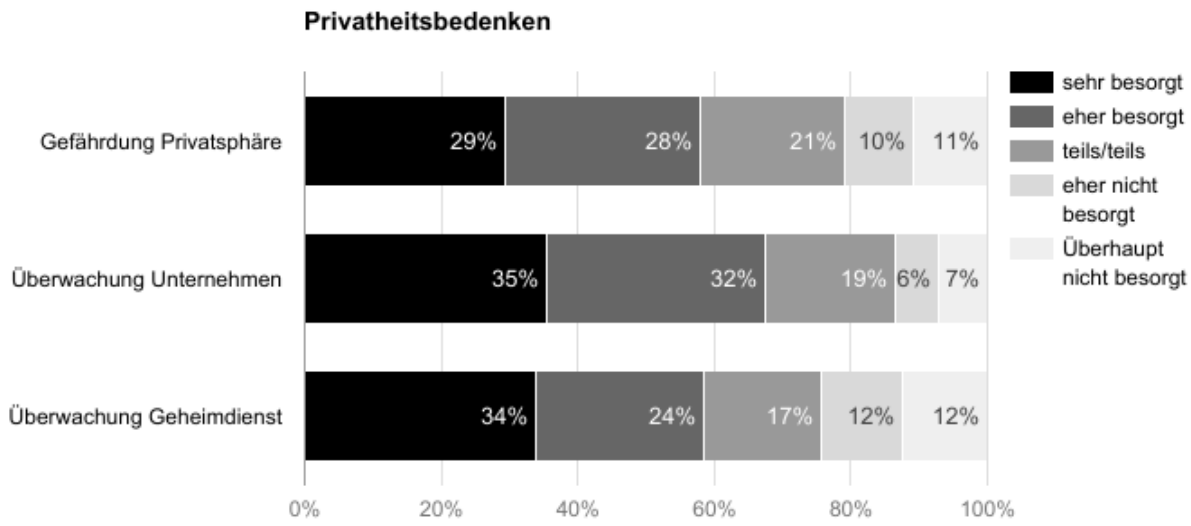


Tabelle 7.4: Anhaltspunkte für die Bewertung von Angeboten

Nr.	Anhaltspunkt
1	Welche technischen Maßnahmen die Dienste zu Anonymisierung, Verschlüsselung und sonstigem Schutz Ihrer Daten vornehmen.
2	Wie renommiert die dahinter stehenden Unternehmen in Sachen Datenschutz sind.
3	Welche unabhängigen Gütesiegel und Auszeichnungen die Dienste in Sachen Datenschutz erhalten haben.
4	In welchem Umfang Sie selbst Einstellungen zu Verarbeitung, Löschung und sonstiger Kontrolle über Ihre Daten vornehmen können.

Insgesamt gaben die Befragten an, relativ stark auf diese Kriterien zu achten (65% stark oder sehr stark). Als absolutes Maß für den Stellenwert von Datenschutzangeboten und -kriterien sollte dieser Wert allerdings nur bedingt verstanden werden, da das Achten auf Datenschutz auch mit einer hohen sozialen Erwünschtheit verbunden ist. Befragte neigen also dazu, ihre Aufmerksamkeit auf Datenschutz zu übertreiben, weil sie annehmen, dass Interviewer eine hohe Aufmerksamkeit als positive Eigenschaft werten. Auch unsere eigene qualitative Vorstudie zeigte, dass Nutzer eher wenig an Datenschutz denken, wenn sie nicht darauf angesprochen werden.

Belastbare Erkenntnisse liefert aber die Unterscheidung nach Typen von Anhaltspunkten und Nutzertypen. Die Unterscheidung nach Anhaltspunkten zeigt, dass insgesamt auf das Vorhandensein von Kontrolloptionen und Anonymisierungsmaßnahmen etwas mehr geachtet wird (73% bzw. 72% mindestens „eher stark“) als auf das Renommee des anbietenden Unternehmens (61%) und das Vorhandensein eines unabhängigen Gütesiegels (56%) (Abbildung 7.8).

Die verschiedenen Bevölkerungsgruppen unterschieden sich darin, wie sehr sie insgesamt auf Anhaltspunkte zum Datenschutz zu achten vorgaben. Bezüglich auf das Alter finden sich deutliche Unterschiede nur bei den höchsten Altersgruppen: Unter den 70-bis 89jährigen gab ein deutlich geringer Anteil (30,6%) an, sehr stark auf die Anhaltspunkte zum Datenschutz zu achten im Vergleich zu 41% bei den jüngeren Befragten. Deutliche Unterschiede zeigen sich auch in Hinblick auf den Schulabschluss. Diese Unterschiede variieren aber in Abhängigkeit vom jeweiligen Kriterium und werden daher nun getrennt betrachtet.

Am deutlichsten gestaffelt sind die Bildungsgruppen in der Bedeutung, die sie Möglichkeiten zur Selbstkontrolle zumessen: Während unter den Befragten mit einem Abitur 57% „sehr stark“ auf solche Möglichkeiten achten, beträgt dieser Anteil unter den Befragten mit Realschulabschluss 49% und unter jenen mit einem Hauptschulabschluss oder ohne Abschluss nur ein Drittel. Bei den drei anderen Anhaltspunkten ist der Unterschied schwächer ausgeprägt (Abbildung 7.9).

Abbildung 7.8: Aufmerksamkeit der Befragten auf unterschiedliche Anhaltspunkte zum Datenschutz von Angeboten.

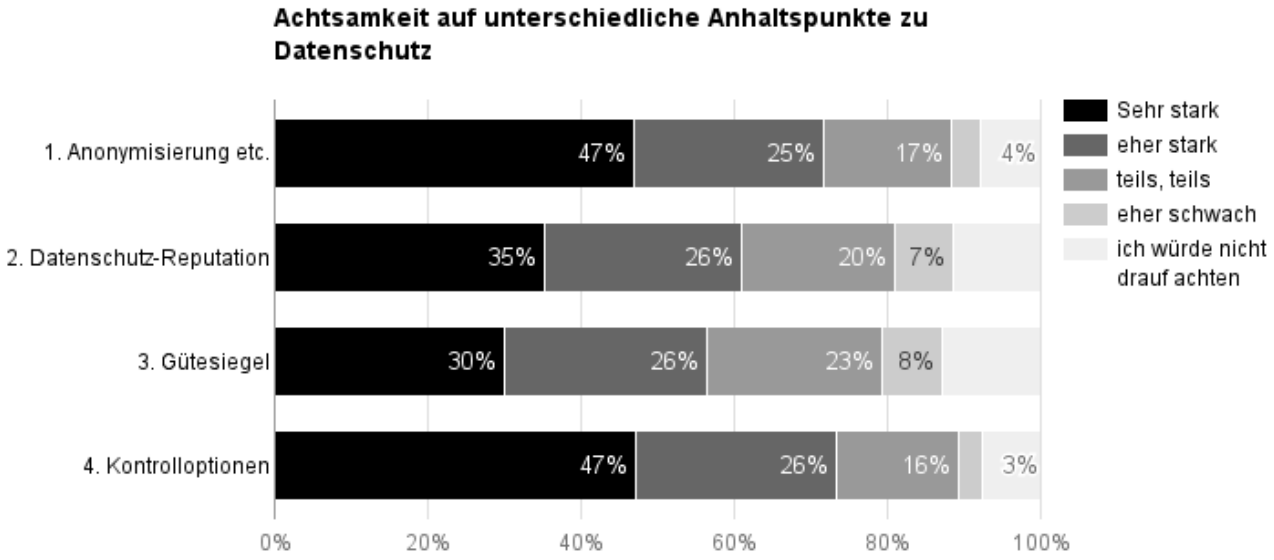
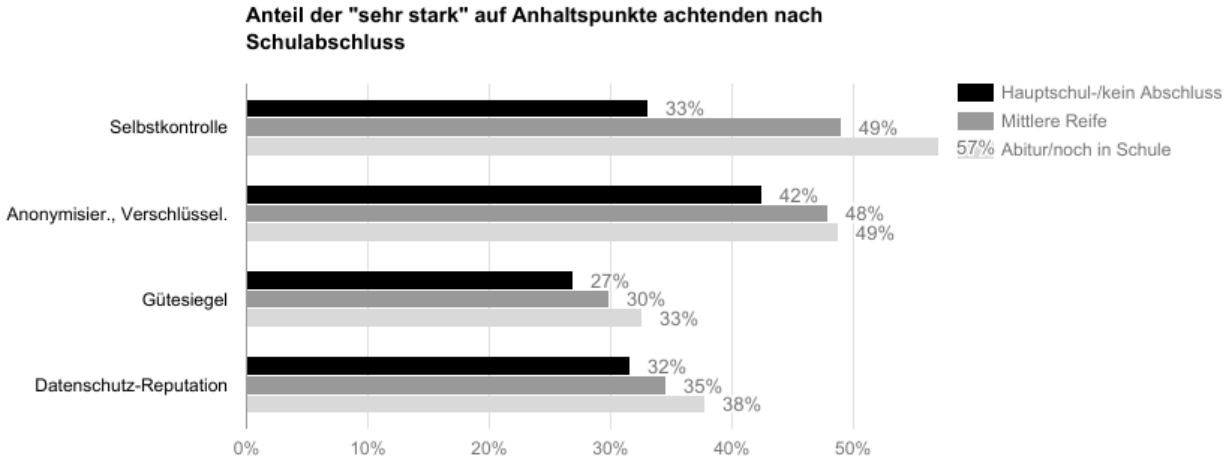


Abbildung 7.9: Anteil der „sehr stark“ auf unterschiedliche Anhaltspunkte achtenden nach Schulabschluss.



7.2.3.2. Verteilung von Datenschutzbezogenem Wissen und Einstellungen

Abschließend sollen noch zwei Schlaglichter auf das komplexere Zusammenspiel von Einflussfaktoren geworfen werden. Dafür wird zunächst untersucht, welchen Einfluss Wissen, Bedenken und die grundlegende Haltung zu Privatheit im Internet auf die Nutzungsintention für Vernetztes-Fahrzeug-Dienste haben. Zweitens wird betrachtet, welche Faktoren mit der Aufmerksamkeit auf unterschiedliche Anhaltspunkte zum Datenschutz von Angeboten des vernetzten Fahrens einhergehen.

7.2.3.2.1. Einflüsse auf Übernahmeintention Die reine Verteilung von Einstellungen und Intentionen in der Bevölkerung, wie sie oben dargestellt wurde, gibt noch keine Auskunft über deren jeweilige Bedeutung für einen Konsumenten, der über die Nutzung eines Dienstes nachdenkt: Wie wichtig sind Privatheitsbedenken in der Erwägung, ob man

einen Dienst nutzen möchte, wie wichtig ist die Einschätzung des erwarteten Nutzens, und wie wichtig ist, ob man eine Frau oder ein Mann ist? Zur Beantwortung dieser Fragen werden statistische Modelle herangezogen, die die Nutzungsintention schrittweise mit immer mehr Faktoren zu erklären versuchen.

In einem ersten Schritt werden Soziodemographie (Alter, Geschlecht, Schulabschluss, Nettoeinkommen), Fahrfrequenz, Datenschutzwissen und Zynismus gemeinsam betrachtet (Modell 1). Das Konstrukt des Privatheitszynismus ist in die Studie aufgenommen worden, da es in der qualitativen Befragung von Nutzern vernetzter Fahrzeuge als bedeutsam erschien. Viele Befragte schienen eine Haltung zu Privatheit im Internetzeitalter zu haben, die sich als Apathie und Zynismus beschreiben lässt und im folgenden Satz eines Teilnehmers zum Ausdruck kommt: „Wo ich jetzt an dieser modernen Welt teilnehmen will, muss mir bewusst sein, dass [...] da wenig privat ist." Um diese Grundeinstellung zu erheben, wurden drei Aussagen in die Befragung einbezogen, die teilweise aus der eigenen Vorstudie und teilweise aus der Literatur abgeleitet sind (Hoffmann et al., 2015[40]).

Die Faktoren Alter, Geschlecht, Schulabschluss, Einkommen, Fahrfrequenz Datenschutzwissen und -zynismus haben zusammengenommen einen signifikanten, aber relativ schwachen, Einfluss auf die Nutzungsintention. Statistisch gesprochen erklären sie 6% der Unterschiede in der Nutzungsintention (R^2=0,06, Tabelle 7.5, Modell 1). Dabei haben Alter, Geschlecht, Schulabschluss und Fahrfrequenz ein ungefähr gleiches Gewicht. Dass das Haushaltsnettoeinkommen hier keine Rolle spielt, lässt sich daraus erklären, dass die Angebote als „zu einem günstigen Preis" verfügbar beschrieben wurden. Aber auch Datenschutzwissen und Zynismus haben keinen Einfluss auf die Übernahmeintention. Ein entscheidender Zugewinn ergibt sich dagegen bei Einbezug der Bewertung der Nützlichkeit der Angebote (Modell 2): Nun kann die Nutzungsintention zu etwa 26% erklärt werden. Die direkten Einflüsse von Schulabschluss und Geschlecht sind in diesem Modell schwächer, weil sie vom wahrgenommenen Nutzen teilweise vermittelt werden: Die geringere Nutzungsintention bei Frauen und höher Gebildeten erklärt sich zum Teil daraus, dass sie einen geringeren Nutzen in der Technik sehen. Auf dieser Basis kann schließlich geprüft werden, ob die Privatheitsbedenken über sämtliche anderen Faktoren hinaus noch einen Einfluss auf die Nutzungsintention haben. Tatsächlich zeigt sich ein solcher Einfluss. Durch ihren Einbezug (Modell 3) kann die Nutzungsintention noch einmal signifikant besser erklärt werden: sie steigt 26% auf 28%. Im abschließenden Modell (3) anschaut, liegen Privatheitsbedenken an zweiter Stelle hinter dem wahrgenommenen Nutzen und vor Alter, Geschlecht oder Fahrfrequenz.

Tabelle 7.5: Einflüsse auf die Übernahmeentscheidung

	Modell 1	**Modell 2**	**Modell 3**
	B	*SE B*	*ß*
Alter	-0,01	0,00	-0,12**
Geschlecht	-0,37	0,10	-0,12**
Schulabschluss	-0,20	0,07	-0,11**
HH-Nettoeinkommen	0,00	0,02	0,00
Fahrfrequenz	0,22	0,06	0,12**
Datenschutzwissen	0,06	0,04	0,05
Zynismus	0,03	0,05	0,02
Wahrgenomm. Nutzen			
Privatheitsbedenken			
R^2	0,06	0,26	0,28
F für Änderung in R^2	7,11**	222,16**	18,94**

Einflüsse auf Übernahmeintention Schließlich soll der Blick auf die Möglichkeiten zu einem konstruktiven Umgang mit Privatheitsbedenken gelenkt werden. Privatheitsbedenken müssen nicht in einer Minderung der Übernahmeintention münden, sie können auch bei Vorhandensein entsprechender Angebote dazu führen, dass Konsumenten eher privatheitsverträgliche Angebote auswählen und diesen dann einen Vorteil auf dem Markt bescheren. Dafür müssen die Konsumenten aber zunächst auf entsprechende Aspekte der Angebote achten. Die vier in Betracht gezogenen Aspekte sind, wie bereits in Tabelle 7.4 dargestellt, Möglichkeiten zur Regulierung von Datenschutz, der Einsatz von Datenschutzfördernden Techniken etwa der Anonymisierung oder Verschlüsselung, die Reputation des Unternehmens in Sachen Datenschutz und unabhängige Siegel.

[40]Hoffmann, Christian Pieter/Lutz, Christoph/Ranzini, Giulia Privacy Cynicism : An Approach to Understanding the Institutional Privacy Paradox. In Amsterdam Privacy Conference. APC, Oktober 2015.

Zunächst werden die Einflüsse auf die durchschnittliche Aufmerksamkeit über die vier Aspekte hinweg im Durchschnitt betrachtet, eine Unterscheidung nach Aspekt erfolgt dann im zweiten Schritt. Soziodemographie, Fahrfrequenz, Datenschutzwissen und Zynismus (Tabelle 7.6, Modell 1) können Unterschiede in der Achtsamkeit im gleichen Umfang von etwa 6% erklären, in dem sie auch die Nutzungsintention erklären konnten (R^2=0,06). Weiter zeigt sich eine leichte Tendenz dahin, dass Befragte, die den Nutzen höher einschätzen, weniger stark auf Datenschutzaspekte achten (Modell 2). Der entscheidende Einfluss auf die Achtsamkeit ergibt sich aber aus den Privatheitsbedenken (Modell 3). Werden sie mit berücksichtigt, lassen sich Unterschiede in der Achtsamkeit auf Privatheitsaspekte mehr als dreimal so gut erklären, insgesamt zu ca. 20%. Unabhängig davon erweisen sich das Einkommen und die Fahrfrequenz als bedeutende Faktoren: Besserverdienende achten stärker auf den Datenschutz. Vielfahrer dagegen achten weniger stark auf den Datenschutz. Unterschiede nach Geschlecht und Bildungsniveau sind zwar ebenfalls vorhanden, aber sie erklären sich aus den höheren Privatheitsbedenken von Frauen und höher Gebildeten.

Tabelle 7.6: Einflüsse auf das Achten auf Kriterien insgesamt

	Modell 1	**Modell 2**	**Modell 3**
	B	*SE B*	*ß*
Alter	0,00	0,00	-0,05
Geschlecht	0,15	0,07	0,07*
Abschluss in 3 Stufen	0,11	0,05	0,09*
HH-Nettoeinkommen	0,06	0,02	0,14**
Fahrfrequenz	-0,13	0,04	-0,11**
Datenschutzwissen	0,01	0,03	0,02
Zynismus	0,07	0,04	0,06
Wahrgenomm. Nutzen			
Privatheitsbedenken			
R^2	0,06	0,06	0,20
F für Änderung in R^2	6,97**	4,61*	131,69**

Wie unterscheiden sich nun die verschiedenen Anhaltspunkte für Datenschutz in der Aufmerksamkeit, die ihnen von unterschiedlichen Befragten beigemessen wird? Eine Ausnahmerolle spielen hier Anhaltspunkte zum Selbstdatenschutz, also zum Umfang, in dem Nutzer selbst Einstellungen zur Verarbeitung, Löschung und sonstiger Kontrolle über Ihre Daten vornehmen können. Dies ergibt sich aus einem dem Modell 3 entsprechenden Modell zur Erklärung der Achtsamkeit auf Möglichkeiten, selbst Einstellungen zu Verwendung und Verbleib seiner Daten treffen zu können (R^2=0,21; F=23,1**). Diese steigt deutlich mit dem Bildungsabschluss (ß=0,13**). Die formale Bildung erweist sich als der nach den Privatheitsbedenken (ß=0,35**) wichtigste Faktor zur Erklärung, warum jemand auf Möglichkeiten zum Selbstdatenschutz achtet. Erst danach kommen das Haushalts-Nettoeinkommen (ß=0,11*) und die Fahrfrequenz (ß=-0,11**). Bemerkenswert ist dabei auch, dass das spezifische Datenschutzwissen hier keinen Einfluss hat (ß=0,00, n.s.), der über die formale Bildung hinausginge. Es ist also das Schulwissen und nicht irgendein davon unabhängiges fachbezogenes Wissen zum Thema Auto, das über die Aufmerksamkeit auf Möglichkeiten zum Selbstdatenschutz entscheidet. Diese Bedeutung der formalen Bildung findet sich nicht bei den anderen Anhaltspunkten für Datenschutz.

7.3. Zusammenfassung

Aus den oben dargestellten Studien ergeben sich die Rahmenbedingungen und Desiderate zum Selbstdatenschutz aus Nutzersicht, aus denen dann die nutzerseitigen Anforderungen abgeleitet werden.

Diese Rahmenbedingungen sind:

- **Primäre Wahrnehmung von Funktionalitäten und Usability.**

  Bei der spontanen Wahrnehmung und Einschätzung eines vernetzten Autos oder entsprechenden Dienstes dominiert nach unseren Befunden die Frage, welche Funktionen der Dienst bietet und wie einfach und praktisch er in der alltäglichen Handhabe ist. Dies zeigten die drei Studien zum Nutzerverhalten jeweils auf ihre Weise.

  Dies bedeutet aber nicht, dass Datenschutzbedenken keine Rolle spielen. In der Repräsentativebefragung ergab sich ein zwar im Effekt vergleichsweise geringer, aber doch eindeutiger Zusammenhang zwischen den Datenschutzbedenken und der Übernahmeintention in dem Sinne, dass Befragte mit stärkeren Bedenken weniger zur

Übernahme geneigt sind. Bei ähnlicher Funktionalität und Usability kann also die Datenschutzverträglichkeit eines Dienstes einen entscheidenden Vorteil in der Nutzungsintention bringen.

Die hohe Wahrnehmung von Funktionalitäten und Usability schließt auch nicht aus, dass Datenschutzbedenken in einer Abwägung die wahrgenommenen Vorteile eines Angebots überwiegen und zu einer Nichtnutzung oder nur eingeschränkten Nutzung führen können. So zeigte die quantitative Nutzerbefragung der TU Darmstadt, dass Nutzer eine präventive Navigation ablehnten, da sie eine permanente Verfolgung der gefahrenen Route verlangte. Umgekehrt konnte besonders die Schaffung von Transparenz bezüglich des Datenempfängers die Bereitschaft zur Datenpreisgabe für eine effizientere Navigation erhöhen. Dennoch sind Datenschutzvorkehrungen, die Einschränkungen in Funktionalitäten oder Usability mit sich bringen, den Nutzern schwer zu vermitteln. Gelingt diese Vermittlung nicht, so werden Nutzer sich bei bestehender Wahlfreiheit gegen die datenschutzfreundlichen Angebote entscheiden.

- **Relevanz von Vertrauenswürdigkeit und Datenklasse**

  Nicht nur die Funktionalität beeinflusst die nutzerseitige Entscheidung ob ein Dienst angenommen wird, sondern auch die Vertrauenswürdigkeit des Empfängers sowie der konkrete Datentyp. Nutzer unterstellen Unternehmen ein ökonomisches Interesse an den Daten und zeigen sich daher nur bedingt bereit Daten zu teilen. Ebenso spielt auch der Ort der Verarbeitung eine wichtige Rolle. Werden die Daten lokal im Auto verarbeitet und gespeichert, ist die Bereitschaft zur Datenpreisgabe höher als bei einer Datenverarbeitung außerhalb des Autos. Dies gilt jedoch nicht für alle Daten gleichermaßen. Nutzer differenzieren zwischen verschiedenen Datenklassen. Während Betriebsdaten des Fahrzeugs als vermeintlich rein technisch wahrgenommen und bereitwilliger geteilt werden, weisen Nutzer Standortdaten einen höheren Schutzbedarf zu.

- **Mangel an Wahlmöglichkeiten**

  Wenn die Nutzer im Rahmen der Einrichtung oder Nutzung eines Dienstes um einen eigenen Beitrag in Form einer Entscheidung oder Einverständnis gebeten werden, so geschieht dies aus ihrer Wahrnehmung heraus nur selten im Interesse einer Regulierung von Datenschutz und Nutzungswünschen nach ihren Präferenzen. Dafür fehlen ihnen häufig schon die Wahlmöglichkeiten. Häufig steht für eine Funktion wie etwa „Navigation“ nur ein Dienst zur Auswahl, und innerhalb von Diensten hat man nur die Optionen, ihn zu nutzen oder nicht zu nutzen, ohne feiner differenzieren zu können in Hinblick auf Nutzungsweisen, die mehr oder weniger Preisgabe von Daten verlangen. Vielmehr erleben die Nutzer jene Situationen, in denen sie etwa Datenschutzerklärungen akzeptieren und Einverständniserklärungen für Berechtigungen erteilen sollen als Momente der Preisgabe von Daten und der Aufgabe von Kontrolle.

- **Einschränkende situative Rahmenbedingungen**

  Die Einstellungen und Verhaltensweisen der Nutzer sind stark situativ geprägt. Dies bezieht sich sowohl auf die Situation im Gesamtprozess der Implementierung der Technik in den eigenen Alltag als auch auf die spezifische Nutzungssituation im Verkehr.

  In Hinblick auf den Gesamtprozess zeigte sich, dass die Situationen, in denen Nutzer folgenreiche Weichenstellungen für ihren Datenschutz treffen (Kaufabwicklung und technische Installation), die für eine entsprechende Reflexion und Meinungsbildung notwendigen Rahmenbedingungen oft nicht bieten. In Hinblick auf alltägliche Nutzungssituationen erscheinen gerade Popup-Meldungen auf dem Benutzerinterface, die Nutzer in der Anwendung bestimmter Dienste unterbrechen, um ihr Einverständnis zur Bereitstellung von Daten einzuholen, in mehrerer Hinsicht problematisch: Die Nutzer sind in der Situation besonders motiviert, den Dienst zu nutzen (sie haben die Nutzung schon begonnen), sie sind in der Regel kognitiv mit dem Fahren beschäftigt und können den Meldungen daher nur am Rande ihre Aufmerksamkeit widmen, und sie müssen u.U. Entscheidungen treffen, die auch die Daten ihrer Mitfahrer betreffen.

- **Wissenkluft im Achten auf Selbstdatenschutz**

  Die im Rahmen von Selbstdatenschutz eröffnete Möglichkeit für Nutzer, Datenflüsse, -speicherung usw. selbst zu kontrollieren, scheint Nutzer mit geringerem Bildungshintergrund weniger stark anzusprechen. Auf andere Anhaltspunkte zum Datenschutz eines Angebots, wie etwa das Vorhandensein von Gütesiegeln, achten geringer gebildete Autofahrer dagegen ungefähr gleich stark wie höher Gebildete. Ein allein auf Selbstdatenschutz setzender Ansatz läuft also Gefahr, bei geringer Gebildeten auf weniger Resonanz zu stoßen. So könnten diese in ihrem Datenschutz schon benachteiligt werden bevor sie überhaupt mit der komplexen Technik in Kontakt kommen.

- **Empfinden der Machtlosigkeit**

  Schließlich ist festzuhalten, dass selbst bei Bereitstellung von Wahlmöglichkeiten und situativen Rahmen-

bedingungen für reflektierte Entscheidungen zum eigenen Datenschutz und von Wahlmöglichkeiten die nutzerseitigen Voraussetzungen für Selbstdatenschutz eingeschränkt sind, da viele Nutzer durch ein Gefühl der Machtlosigkeit gelähmt sind. Dies führen die Befragten auf eine Vielzahl an Erfahrungen und Beobachtungen zurück, die ihnen die Vergeblichkeit von Selbstschutzmaßnahmen vor Augen geführt haben, sowohl als Kunden etwa von Google und Facebook als auch als Beobachter der Berichterstattung zu staatlicher Überwachung. Zwar liegen die Ursachen dafür zu einem großen Teil außerhalb des Bereichs „vernetzte Autos“ liegen, aber die derzeitigen Erfahrungen mit vernetzten Autos können sich von diesem Gesamtbild nicht entscheidend abheben.

8. Anforderungen

8.1. Anforderungen Nutzerperspektive

Die nutzerseitigen Anforderungen für Lösungen zum Selbstdatenschutz ergeben sich aus der Literaturarbeit und den eigenen Studien, die im Kapitel 8 (Nutzerseitige Analysen) ausgeführt werden. Sie werden im Folgenden mit jeweils kurzer Einleitung tabellarisch zusammengefasst.

Aus Nutzerperspektive bedeutet eine MUSS-Bedingung, dass ein Angebot, welches die Bedingung nicht erfüllt, in nicht hinnehmbarem Maße gegen die Interessen der Nutzer verstößt und/oder auf massive Ablehnung bei den Nutzern stoßen würde, die eine Akzeptanz des Angebots in größerem Umfang verhindern würde. Das Nichterfüllen einer SOLL-Bedingung bedeutet, dass die Interessen der Nutzer und/oder die Akzeptanz des Angebots in beschränktem Umfang beeinträchtigt werden.

8.1.1. Konfliktfreiheit

Ein Kernbefund der qualitativen sowie quantitativen Studien ist, dass Nutzer von Angeboten zum vernetzten Fahren zunächst die Funktionalitäten und die Einfachheit der alltäglichen Handhabung wahrnehmen, während die Datenschutzproblematik in der spontanen Wahrnehmung nachgeordnet ist. Daher müssen Ansätze zum Selbstdatenschutz zumindest mit der Nutzung der Kernfunktion der Angebote kompatibel sein. So würde ein Navigationsgerät, das aus Datenschutzgründen erst verspätet über Störungen im Verkehrsfluss informiert und Alternativrouten anbietet, bei einem bedeutenden Teil der Nutzer durchfallen, weil sie zu dieser Einschränkung nicht bereit wären. Einschränkungen bei der Nutzerführung sollen ebenfalls nach Möglichkeit vermieden werden. Sie könnten aber in beschränktem Maße noch hingenommen werden, wenn es nicht anders geht (vgl. Sasse, Smith, Herley, Lipford & Vaniea, 2016[1]). Auf keinen Fall dürfen die Lösungen zum Selbstdatenschutz die Nutzer so beanspruchen, dass sie den Anforderungen in der Fahrsituation nicht mehr gerecht werden können.

N01	Konfliktfreiheit von Nutzung und Datenschutz Die Wahrung des Datenschutzes MUSS mit der Nutzung der Kernfunktion des betroffenen Services/Apps/Produkts sowie der Fahrsituation kompatibel sein.
N01.01	Wahrung der Kernfunktion Die datenschutzrechtlichen Einstellungen MÜSSEN die Kernfunktion des Service/der App/des Produkts wahren.
N01.02	Nutzerführung Durch die Datenschutz-HMI SOLL die Nutzerführung des Systems nicht beeinträchtigt werden.
N01.03	Situative Angemessenheit Die Nutzerführung des Datenschutz-HMI MUSS den situativen, kognitiven und sicherheitsrelevanten Bedingungen im Fahrzeug genügen.

[1] Sasse, M. A. et al. Debunking Security-Usability Tradeoff Myths. IEEE Security Privacy, 14 Sept 2016, Nr. 5, ISSN 1540–7993.

8.1.2. Kontrolle

All jene Personen, über deren Daten entschieden wird, müssen an der Kontrolle über die Daten beteiligt sein. Insbesondere muss verhindert werden, dass einzelne Personen (technikaffine Freunde, Autohändler oder Fahrzeughalter) Entscheidungen im Namen anderer machen. Sofern personenbezogene Daten von mitfahrenden Passagieren oder Mitnutzern eines Autos erhoben werden, müssen diese auch ihr Einverständnis dazu geben.

In dem Maß, in dem die Bereitstellung bestimmter Funktionen oder eine erhöhte Usability die Preisgabe von Daten erfordern, müssen Nutzer diese Preisgabe insbesondere in Hinblick auf die fraglichen Datentypen und ihre parteienbezogene Weitergabe kontrollieren können. Dabei treffen die Nutzer die Entscheidung über die Datenpreisgabe in Abhängigkeit von der Funktion, die ein fraglicher Dienst ihnen erfüllt. Nur wenn sie die Legitimation des Datenempfängers im Nutzungskontext nachvollziehen und für sich selbst einen Nutzen identifizieren können, sind sie bereit ein Datum mit bestimmten Empfängern zu teilen. Diese drei Faktoren (Datentyp, Parteien, Funktionen) wurden in den Nutzerstudien als Kriterien identifiziert, nach denen Nutzer ihre Bereitschaft zur Preisgabe von Daten richten.

Voraussetzung für eine Kontrolle ist dabei, dass den Nutzern auch Alternativen zu Standard-Vorgehensweisen bereitgestellt werden. Die Alternative, auf eine Funktionalität ganz zu verzichten (“take it or leave it”) stellt nur eine beschränkte Wahlmöglichkeit dar, da Nutzer u.U. auf die Funktion angewiesen sind (vgl. Nissenbaum, 2011[2]). Sie läuft auch auf einen Konflikt zwischen Datenschutz und Kernfunktionalität hinaus (vgl. Punkt 1 dieses Kapitels). Daher sollen für eine Funktionalität unterschiedliche Dienste zu Verfügung gestellt werden, zwischen denen der Nutzer dann - bei gegebener Transparenz, vgl. Punkt 3. - auch nach Datenschutzkriterien den Besten auswählen kann. Weiter sollen Wahlmöglichkeiten auch unterhalb der Ebene eines ganzen Dienstes gegeben sein, so dass Nutzer über periphere Funktionen oder Usability-Features wählen können. Ein Beispiel wäre die Speicherung von Fahrtzielen, die Nutzern bei nachfolgenden Fahrten eine erneute Eingabe der Zieladresse abnehmen könnte. Dies bringt relativen Komfortgewinn und Zeitersparnis, die aber für bestimmte Fahrer unter bestimmten Bedingungen (etwa in beruflich geteilten Autos) geringer wiegen als das empfundene Risiko, das mit der Speicherung der Ortsdaten einhergeht.

Schließlich ist wichtig, dass die Kontrolle innerhalb der gegebenen Rahmenbedingungen möglich ist. Das bedeutet zum einen, dass die ganze Bandbreite an Nutzern in Hinblick auf Bildung, technische Fähigkeiten, usw. mit der Kontrolle zurechtkommen muss. Zum anderen soll die Kontrolle mit den Situationen kompatibel sein, in denen sie erfolgt. Die Nutzer sollen also (etwa durch das Fahren) kognitiv nicht so sehr beansprucht sein, dass sie die komplexen Entscheidungen nicht verarbeiten können. Folglich müssen entweder die Entscheidungen sehr einfach dargestellt werden oder sie müssen in anderen Situationen als der Fahrsituation getroffen werden. Zudem zeigen Shu (2009[3]) und Masur (in preparation[4]) deutlich, dass Nutzer Privatheitsentscheidungen stark auf der Basis situativer Faktoren treffen. Es muss also vermieden werden, dass Entscheidungen systematisch in solchen Situationen getroffen werden, in denen die Problematik der preisgegebenen Daten besonders gering und/oder der Nutzen der damit verbundenen Funktionalität besonders hoch erscheint.

Aufgrund der situativen Unterschiede in der Bewertung des Nutzwerts einer Funktion und der Bedenklichkeit von Daten muss den Nutzern auch eine Kontrolle über ihre Daten im Nachhinein ermöglicht werden, die auch die Löschung von Daten umfasst. Dies ergibt sich daraus, dass Nutzer zu unterschiedlichen Zeitpunkten die Bedeutung von bestimmten Funktionalitäten und die Bedeutung der Freigabe ihrer Daten unterschiedlich einschätzen.

[2] Nissenbaum, Helen A contextual approach to privacy online. Stanford University Press, 2011.

[3] Shu, C. W. Privacy or Performance Matters on the Internet: Revisiting Privacy Toward a Situational Paradigm. In Online Consumer Protection: Theories of Human Relativism. IGI Global, 2009.

[4] Masur, P. Situational Privacy and Self-Disclosure. Disseration in Preparation. Universität Hohenheim,.

N02	Kontrolle Der Nutzer MUSS die Möglichkeit haben die Freigabe, Aufzeichnung und Speicherung einzelner Datentypen zu unterbinden, zu revidieren, zu ändern oder zu löschen.
N02.01	Kontrolle durch alle Betroffenen Alle Personen, deren Daten betroffen sind, MÜSSEN in die Kontrolle eingebunden sein.
N02.02	Datentypabhängige Freigabe Der Nutzer MUSS die Möglichkeiten haben, die Freigabe einzelner Daten zu verweigern, solange es sich nicht um sicherheitsrelevante oder gesetzlich vorgeschriebene Funktionen handelt.
N02.03	Parteiabhängige Freigabe Der Nutzer MUSS die Möglichkeit haben, die Freigabe der personenbezogenen und personenbeziehbahren Daten auf einzelne Parteien zu beschränken.
N02.04	Funktionsabhängige Freigabe Der Nutzer MUSS die Möglichkeit haben, die Freigabe der personenbezogenen und personenbeziebahren Daten auf einzelne Funktionen zu beschränken, in denen er einen Nutzen für sich erkennt.
N02.05	Bereitstellung von Alternativen Die Kontrolle durch den Nutzer SOLL weiter differenzieren als nur im Sinne einer vollständigen Übernahme oder Ablehnung einer bestimmten Funktionalität. In Abhängigkeit der datenschutzbezogenen Präferenzen des Nutzers SOLL er die Möglichkeit haben, zwischen unterschiedlichen Angeboten zu wählen und innerhalb eines Angebots selektiv auf bestimmte Funktionalitäten und Aspekte der Usability zu verzichten.
N02.06	Angemessenheit der Kontrolle an Rahmenbedingungen Die Kontrollmöglichkeiten des Nutzers SOLLEN so gestaltet sein, dass die Kontrolle nicht aufgrund der Rahmenbedingungen eingeschränkt ist. Zu diesen Rahmenbedingungen gehören nutzerseitige Faktoren (Vorwissen), aber auch situative Faktoren (kognitive Beanspruchung, motivationale Beeinflussung u.ä.).
N02.07	Ermöglichung der Revidierung von Einstellungen Der Nutzer SOLL die Möglichkeit haben die Datenschutzeinstellungen zu revidieren oder anzupassen, ohne dabei auf die Leistung komplett verzichten zu müssen.
N02.08	Ermöglichung der Datenlöschung Der Nutzer MUSS die Möglichkeit haben, Nutzerprofile, Datenschutzeinstellungen zu löschen sowie die Datenfreigabe mit sofortiger Wirkung zu unterbinden.

8.1.3. Transparenz

Transparenz nimmt sowohl in den Ergebnissen der eigenen Nutzerstudien als auch in der Literatur eine herausragende Rolle ein. Zum einen hat sich Transparenz als der Faktor erwiesen, der Nutzer am ehesten zur Preisgabe von Daten bewegt. Zum anderen bietet erst ein transparenter Umgang mit Informationen zum Erhebungszweck oder zum Datenempfänger die Entscheidungsgrundlage über die Wahrnehmung eines bestimmten Dienstes. Unsere Studien zeigen, dass Nutzer sich bei der Kontrolle über den Datenschutz sehr stark an den Nutzungsintentionen und der Identität des Datenempfängers orientieren . Transparenz soll, wie Kontrolle, insbesondere umfassen, welche Datentypen verwendet werden, welche Parteien die Ziele der Übermittlung darstellen und welche Funktionen der Zweck der Übermittlung sind. Weiter muss dargestellt werden, an welchen Stellen und über welche Zeit die jeweiligen Daten gespeichert werden und wie Nutzer Kontrolle über ihre Daten ausüben können.

Schließlich gilt auch für die Transparenz, dass die Informationen in solchen Situationen bereitgestellt werden sollte, in denen sie relevant ist und verarbeitet werden kann, also vor Kontrollentscheidungen und in Situationen, in denen Nutzer nicht kognitiv eingeschränkt sind.

N03	Transparenz Der Nutzer MUSS nachvollziehen können in welchem Umfang Daten über ihn und sein Umfeld im Zuge der Nutzung an andere gelangen.
N03.01	Transparenz der übermittelten oder gespeicherten Datentypen: Der Nutzer MUSS nachvollziehen können, welche Daten über ihn und sein Umfeld übermittelt oder gespeichert werden.
N03.02	Transparenz der Übermittlungsziele Der Nutzer MUSS nachvollziehen können an welche Parteien welche Daten übermittelt werden.
N03.03	Transparenz des Übermittlungszweck Der Nutzer MUSS nachvollziehen können zu welchem Zweck die Daten verwendet werden sollen.
N03.04	Transparenz der Speicherung Der Nutzer MUSS nachvollziehen können an welchen Stellen und über welche Dauer welche Daten gespeichert werden.
N03.05	Transparenz der Kontrollmöglichkeiten Der Nutzer MUSS nachvollziehen können über welche Möglichkeiten zur Kontrolle er verfügt.
N03.06	Kontextbezug der Nutzerinformation Der Nutzer SOLL in der Situation informiert werden, in der er auch privatheitsrelevante Kontrollentscheidungen zu treffen hat.
N03.07	Angemessenheit an Rahmenbedingungen Die Information des Nutzers SOLL so weit aufbereitet werden, dass Nachvollziehbarkeit auch bei ungünstigen situativen (kognitive Beanspruchung des Fahrers durch Verkehrslage, Kommunikation mit Mitfahrern u.ä.), und nutzerseitigen (Vorwissen, Intelligenz) Rahmenbedingungen gewährleistet sind.

8.1.4. Gewährleistung vorausgesetzter Grundstandards

Solange die Nutzer in Hinblick auf Transparenz und Kontrolle in ihrem Selbstdatenschutz eingeschränkt sind, werden sie immer wieder Entscheidungen treffen und Einwilligungen vornehmen, deren Konsequenzen sie nicht durchschauen. Zusammen mit dem aus der Erfahrung mit dem Internet verbreiteten Grundgefühl der Machtlosigkeit bedeutet dies, dass viele sich mit dem Selbstdatenschutz überfordert fühlen. Dies zeigen neben unseren Befunden aus der qualitativen Nutzerstudie, auch andere Studien.

In dieser Situation ist wichtig, dass unabhängig von dem im Rahmen von Selbstdatenschutz geregelten Maß an Datenschutz auch Grundstandards gewährleistet werden und den Nutzern die Existenz dieser Grundstandards vermittelt wird. Dies ist ein wichtiges Mittel zur Überwindung des lähmenden Gefühls, man sei ein “Gläserner Mensch” oder habe sich selbst durch eine Vielzahl von Einverständniserklärungen in diese Situation manövriert.

N04	Gewährleistung von Grundstandards Über die Gebote der Transparenz und Kontrolle hinaus MUSS der Datenschutz Grundstandards entsprechen, deren Einhaltung Nutzer voraussetzen und auf die sie vertrauen.
N04.01	Gewährleistung der Datensicherheit Die Sicherheit der Daten vor Angriffen auf das System MUSS so weit gewährleistet sein, dass Nutzer ein hohes Maß an Vertrauen in eine rechtskonforme Verwendung der Daten setzen können. Die Maßstäbe SOLLEN hier auf dem gleichen Niveau liegen wie in anderen Bereichen des Verbraucherschutz wie Lebensmittelsicherheit oder Unfallschutz.
N04.02	Gewährleistung der Datensparsamkeit Das Ausmaß der Verwendung von Daten MUSS auf das Maß beschränkt werden, das für die Ermöglichung der entsprechenden Nutzung notwendig ist.
N04.03	Gewährleistung der Datenintegrität Die Korrektheit der erhobenen Daten MUSS gewährleistet sein, damit keine falschen Informationen über den Nutzer gespeichert werden.

8.2. Datenschutz und Datensicherheit

8.2.1. Methodik

Der nachfolgende Anforderungskatalog beruht auf einem Vorgehen nach dem Standard-Datenschutzmodell. Dieses Modell ist ein Konzept zur Beratung und Prüfung, das von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Anwendung empfohlen wird[5]. Es ist derzeit in der Version 1.0 veröffentlicht. Das Modell ermöglicht die systematische Entwicklung und Prüfung von Maßnahmen zum Schutz der Betroffenenrechte im Kontext von Datenverarbeitungsverfahren.

Eine datenschutzrechtliche Prüfung kann nicht damit enden, dass festgestellt wird, ob eine wirksame Einwilligung oder eine Rechtsgrundlage für eine Datenverarbeitung vorliegen. Im nächsten Schritt ist immer zu prüfen, ob durch technische und organisatorische Maßnahmen gewährleistet wird, dass die Grundsätze des Datenschutzes und der Datensicherheit eingehalten werden[6].

Datenschutzrecht ist aber hochgradig abstrakt. Der Gesetzgeber versucht möglichst technikoffene Normen zu formulieren und schreibt deshalb nicht ausdrücklich vor, welche Maßnahmen zu ergreifen sind. Würde er dies machen, bestünde die Gefahr, dass durch jede technische Neuerung ein neuer Gesetzgebungsprozess nötig würde. Er beschränkt sich deshalb darauf, festzulegen, dass unter „Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ geeignete Maßnahmen zur Umsetzung der Datenschutzgrundsätze zu treffen sind, Art. 25 Abs. 1 DSGVO.

Dies stellt den Rechtsanwender vor die große Herausforderung, aus diesen abstrakten Normen für seinen konkreten Fall Maßnahmen abzuleiten. Die Problematik spitzt sich zu, wenn man bedenkt, dass die Vorschriften der Datenschutzgrundverordnung für Verstöße gegen die Art 25 und 32 DSGVO Geldbußen von bis zu 10.000.000 oder im Falle von Unternehmen bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres vorsehen, Art. 83 Abs. 4 a) DSGVO. Solche Geldbußen lassen sich nur rechtfertigen, wenn die Adressaten des Datenschutzrechts wissen können, welche Maßnahmen von ihnen gefordert werden. Dieses Spannungsverhältnis zwischen dem Bedürfnis nach Rechtssicherheit und der möglichst umfassenden und technikoffenen Regelung des Datenschutzes soll durch das Standard-Datenschutzmodell aufgelöst werden. Dazu hat man sich zur Verwendung eines schutzzielbasierten Ansatzes entschieden. Schutzziele dienen dazu, Maßstäbe bei der Entwicklung und Prüfung von Verfahren zu setzen[7].

Einer der Vorteile dieses Ansatzes ist es, dass er die interdisziplinäre Zusammenarbeit zwischen Technikern und Juristen fördert, die für einen effektiven Datenschutz essentiell ist. Während Technikern ein schutzzielbasierter Ansatz und die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit aus der IT-Sicherheit bekannt sind, ist den Juristen der damit verbundene Widerstreit zwischen entgegengesetzten Anforderungen und die Auflösung solcher Spannungsverhältnisse durch Abwägung aus der Grundrechtsdogmatik bekannt. Weiterhin berücksichtigt er, dass die Bearbeitung von personenbezogenen Daten in einer Vielzahl von unterschiedlichen Kontexten stattfindet. Insoweit gewährt ein schutzzielbasierter

[5] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Das Standard-Datenschutzmodell (SDM). https://www.datenschutzzentrum.de/sdm/.

[6] Art. 25 und 32 DSGVO

[7] Grundlegend zu Schutzzielen: in: Rost, Martin/Pfitzmann, Andreas Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit, 2009, Nr. 6.

Ansatz genügend Abwägungsspielräume, um Einzelfälle angemessen zu berücksichtigen, gibt aber durch einen noch in der Entwicklung befindlichen Standardmaßnahmenkatalog hinreichend konkrete Vorgaben, welche Maßnahmen zur Umsetzung der datenschutzrechtlichen Anforderungen in Betracht kommen.

8.2.1.1. Datenminimierung

„Allen Gewährleistungszielen ist gemein, dass sie bestimmen, welche Eigenschaften und Parameter von im Vorhinein als zulässig bestimmten Verarbeitungsvorgängen und Begleitprozessen zu wahren sind. Daher fordert der Gesetzgeber, den Datenstrom auf Wesentliches und auf ein notwendiges Maß beschränkend[8] zu reduzieren, an der Quelle und jeder Verzweigung, im Vorhinein und – immer wichtiger im Zeitalter der mit dem Stichwort Big Data verknüpften explorativen Datenverarbeitung – im Zuge der Verarbeitung selbst. Diese grundlegende Anforderung erfasst in konzentrierter Form das Gewährleistungsziel der Datenminimierung, dessen Umsetzung daher einen durchgreifenden Einfluss auf Umfang und Intensität des durch die anderen Gewährleistungsziele bestimmten Schutzprogramms hat.

Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Erforderlichkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist.“[9]

8.2.1.2. Verfügbarkeit

Verfügbarkeit, Integrität und Vertraulichkeit sind aus der IT-Sicherheit bekannte Schutzziele, die in Art. 32 Abs. 1 b) DSGVO nunmehr als ausdrückliche gesetzliche Anforderungen an die Verarbeitung personenbezogener Daten genannt werden. Verfügbarkeit bedeutet, dass personenbezogene Verfahren zur Verfügung stehen sollen. Das bedeutet, dass die verarbeiteten Daten für die berechtigten Personen zugreifbar sein müssen, Daten auffindbar sind und mit den eingesetzten Verfahren bearbeitet werden können. Wer seine personenbezogenen Daten einem Verantwortlichen anvertraut, muss sich darauf verlassen können, dass er die damit verbundenen Funktionen und Vorteile auch nutzen kann. In der aktuellen Gesetzgebung wird ein Aspekt der Verfügbarkeit in der Nr. 7 der Anlage zu § 9 S. 1 BDSG genannt. Danach ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8.2.1.3. Integrität

Auch in der Rechtsprechung des Bundesverfassungsgerichts ist ein Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme anerkannt[10]. Es ist, wie das Grundrecht auf informationelle Selbstbestimmung, eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[11]. Das Gericht stützt die Notwendigkeit einer solchen Interpretation des allgemeinen Persönlichkeitsrechts auf eine „früher nicht absehbare[n] Bedeutung“ der Informationstechnik für die Entfaltung des Einzelnen aufgrund der zentralen Bedeutung dieser Systeme für die Lebensführung vieler Menschen[12]. Schon zu diesem Zeitpunkt betonte das Gericht, dass mit informationstechnischen Systemen nicht nur Personalcomputer gemeint sind, sondern auch in Kraftfahrzeugen solche Systeme zunehmend vorhanden sind[13]. Zwar sind die Schutzziele der Integrität und Vertraulichkeit nicht identisch mit dem Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme, was wohl im Wesentlichen in der komplizierten Abgrenzung dieses Grundrechts zu anderen Grundrechten begründet ist[14], dennoch ist es bemerkenswert, dass hier Begriffe aus der Informartionssicherheit verwendet wurden.

Das Schutzziel der Integrität umfasst die kontinuierliche Einhaltung von definierten Spezifikationen eines Systems, die zur Erfüllung des Zwecks der Datenverarbeitung festgelegt wurden. Es ist sicherzustellen, dass das System genau so funktioniert, wie es funktionieren soll und personenbezogene Daten vollständig, aktuell und inhaltlich richtig sind[15].

[8] Art. 5c DS-GVO

[9] SDM-Handbuch v.1.0, S. 11 f. in: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf.

[10] BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07

[11] BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07, Rn. 166

[12] BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07, Rn. 170 f.

[13] BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07, Rn. 173

[14] BVerfG, Urteil vom 27.02.2008, Az.: 1 BvR 370/07, Rn. 181 ff.

[15] SDM-Handbuch v.1.0, S. 13 in: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf.

8.2.1.4. Vertraulichkeit

Das Schutzziel der Vertraulichkeit soll die unbefugte Kenntnisnahme von personenbezogenen Daten verhindern. Dabei ist zu beachten, dass nicht nur Personen außerhalb der verantwortlichen Stelle unbefugt sein können, also „Hacker“ oder Dienstleister. Auch innerhalb der verantwortlichen Stelle ist zu prüfen, inwieweit es erforderlich ist, einzelnen Personen oder Personengruppen die Befugnis zur Kenntnisnahme einzuräumen[16].

8.2.1.5. Nicht-Verkettbarkeit

Das Schutzziel der Nicht-Verkettbarkeit soll die Verkettung von personenbezogenen Daten, die zu unterschiedlichen Zwecken erhoben wurden, verhindern. Dies kann insbesondere dadurch erreicht werden, dass nur die erforderlichen Daten erhoben werden und die Zweckbindung für diese Daten gewahrt bleibt. Wird die Anforderung der Datensparsamkeit nicht beachtet, besteht die Gefahr, dass die rechtliche Anforderung der Erforderlichkeit nicht eingehalten wird. Die Nichtbeachtung der Zweckbindung ist problematisch, wenn für einen neuen Zweck keine Rechtsgrundlage oder Einwilligung vorliegt. Es handelt sich dann regelmäßig um eine rechtswidrige Datenverarbeitung, soweit nicht die Voraussetzungen von Art. 6 Abs. 4 DSGVO vorliegen.

8.2.1.6. Transparenz

Das Schutzziel der Transparenz betrifft die Kenntnis von Datenverarbeitungsvorgängen aus Sicht der Betroffenen, der Betreiber und der Aufsichtsbehörden. Einschränkungen dieses Schutzziels können dazu führen, dass die Prüffähigkeit von Datenverarbeitungsvorgängen nicht oder nur eingeschränkt gegeben ist. Transparenz ist insoweit auch Voraussetzung für das Erkennen und Beheben von Mängeln. Zudem kann sich mangelnde Transparenz auf die Wirksamkeit von Einwilligungen auswirken, da diese eine Informiertheit des Betroffenen erfordern. Aus Sicht der Betroffenen handelt es sich um einen zentralen Aspekt des Schutzes ihrer informationellen Selbstbestimmung. „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“[17]

8.2.1.7. Intervenierbarkeit

Das Schutzziel der Intervenierbarkeit soll es den betroffenen Personen ermöglichen, ihre Betroffenenrechte effektiv geltend zu machen. Die Betroffenenrechte finden sich in den Art. 16 ff. An den Betreiber ist die Forderung zu stellen, dass für ihn die Möglichkeit besteht, jederzeit in Datenverarbeitungsvorgänge einzugreifen und sie aufgrund von erkannten Mängeln zu ändern[18].

[16] SDM-Handbuch v.1.0, S. 13f in: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf.

[17] BVerfG, Urteil vom 15.12.1983, Az. 1 BvR 209/83, Rn. 172

[18] vgl. SDM-Handbuch v.1.0, S. 15 in: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf.

8.2.2. Grundsätzliche Zulässigkeit der Datenverarbeitung

D01	Verbot mit Erlaubnisvorbehalt Wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, MUSS hierfür eine Rechtsgrundlage oder eine Einwilligung vorliegen, Art. 6 Abs. 1 DS-GVO
D01.01	Einwilligung Wenn die Datenerhebung, -nutzung und -verarbeitung auf Grundlage einer Einwilligung erfolgen, MUSS diese auf der freien und informierten Entscheidung des Betroffenen beruhen, Art. 7 DS_GVO
D01.01.01	Freiwiligkeit Soweit die Datenverarbeitung auf eine Einwilligung als Rechtsgrundlage gestützt wird, MUSS diese freiwillig erteilt werden. Zu klären: Freiwillig bei Notwendigkeit zum Nutzen des PKW? Sehr kritisch, wenn Nutzung des Fahrzeugs im Rahmen eines abhängig beschäftigten Arbeitsverhältnisses erfolgt.
D01.01.02	Informiertheit Den Betroffenen MÜSSEN die zum Verständnis der Verarbeitungsvorgänge erforderlichen Informationen zur Verfügung stehen, bevor die Einwilligung erteilt wird[19]
D01.01.03	Nachweisbarkeit Die Erteilung der Einwilligung MUSS durch den Verantwortlichen nachgewiesen werden können.
D01.01.04	Widerruflichkeit Der Betroffene MUSS das die Möglichkeit haben, seine Einwilligung für die Zukunft zu widerrufen, Art. 7 Abs. 3 DSGVO.
D01.01.04.01	Datenverarbeitung nach Widerruf Es muss technisch und organisatorisch sichergestellt werden, dass nach einem Widerruf keine Datenerhebung oder -verarbeitung mehr stattfindet, die auf der Einwilligung beruhte, Art 7 Abs. 3 S. 4 DSGVO.
D01.01.04.02	Einfachheit des Widerrufs Der Widerruf MUSS so einfach sein, wie die Einwilligungserklärung.
D01.02	Erforderlichkeit bei Rechtsgeschäften Wenn die Datenverarbeitung auf die Begründung, Durchführung, oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Verhältnisses gestützt wird, MUSS das Erheben, Verarbeiten und Nutzen der Daten auf das Erforderliche beschränkt sein, Art 6 Abs. 1 b) DSGVO.
D01.03	Wahrung der berechtigten Interessen des Verantwortlichen Wenn die Datenverarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, dürfen (MUSS) die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überweigen, Art 6 Abs. 1 f) DSGVO.
D01.04	Datenübermittlung in Drittländer Datenübermittlungen in Drittländer dürfen (MUSS) nur stattfinden, wenn die Kommission ein ausreichendes Datenschutzniveau festgestellt hat, oder anderweitige Garantien für den Schutz der personenbezogenen Daten vorliegen, Art. 45 ff..

[19] siehe Art. 13 ff DS-GVO

8.2.2.1. Transparenz

D02	Transparenz Betroffene, Aufsichtsbehörden und Betreiber von Systemen MÜSSEN personenbezogene Verfahren prüfen können. Dafür ist Voraussetzung, dass die Datenverarbeitung für sie nachvollziehbar wird.
D02.01	Dokumentation Die Datenverarbeitung MUSS umfassend dokumentiert sein. (Art. 5 Abs.2 DS-GVO)
D02.02	Auskunftsansprüche Es MUSS sichergestellt werden, dass einem Betroffenen auf sein Verlangen hin Auskunft über die ihn betreffenden personenbezogenen Daten gegeben wird, Art. 15 DSGVO. Dies betrifft unter anderem die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die Speicherdauer und die Betroffenenrechte.
D02.02.01	Auskünfte nur an Berechtigte Die verantwortliche Stelle MUSS sicherstellen, dass Auskünfte nur an die Berechtigten erteilt werden. Es ist zu berücksichtigen, dass neben den Betroffenen auch andere Stellen ggf. ein Auskunftsrecht geltend machen können. Auch dann ist sicherzustellen, dass Auskünfte nur an Berechtigte gegeben werden.
D02.02.02	Auskunftsverlangen unter Pseudonym Wenn ein Betroffener einen Dienst unter einem Pseudonym nutzt, SOLL sichergestellt sein, dass er unter diesem Pseudonym auch seinen Auskunftsanspruch geltend machen kann.
D02.03	Informationspflichten Der Nutzer MUSS über die Informationen zur Datenverarbeitung erhalten.
D02.03.01	Nutzergerechte Form Die Informationen für den Nutzer MÜSSEN in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erteilt werden, Art. 12 Abs. 1 DSGVO
D02.03.02	Information bei Datenerhebung bei der betroffenen Person Werden personenbezogene Daten bei der betroffenen Person erhoben, muss der Verantwortliche bei der Erhebung die betroffene Person über • den Namen und die Kontaktdaten des Verantwortlichen • die Kontaktdaten des Datenschutzbeauftragten • die Zwecke und die Rechtsgrundlage der Datenverarbeitung • die berechtigten Interessen, falls die Datenverarbeitung auf Art. 6 Abs. 1 f) DSGVO gestützt wird • die Empfänger oder Kategorien von Empfängern der Daten • die Absicht der Übermittlung in ein Drittland oder an eine internationale Organisation, sowie weiteren Informationen zur Rechtmäßigkeit dieser Übermittlung, vgl. Art. 13 Abs. 1 f). • die Dauer der Speicherung oder die Kriterien für die Festlegung der Dauer • die Betroffenenrechte • das Recht, die Einwilligung jederzeit zu widerrufen • das Beschwerderecht bei einer Aufsichtsbehörde • die Folgen der Nichtbereitstellung der personenbezogenen Daten • das Bestehen einer automatisierten Entscheidungsfindung oder eines Profilings informieren, Art. 13 DSGVO.
D02.03.03	Information bei Datenerhebung, die nicht bei der betroffenen Person erfolgt Erfolgt die Datenerhebung nicht bei der betroffenen Person, MUSS der Verantwortliche die gleichen Informationen dem Betroffenen zur Verfügung stellen und zusätzlich über die Quelle der Daten informieren, Art. 14 DSGVO. Die Information muss innerhalb einer angemessenen Frist erfolgen, die nicht länger als einen Monat dauern darf. Werden die Daten zur Kommunikation mit der betroffenen Person genutzt, müssen die Informationen bei der ersten Kontaktaufnahme erteilt werden. Werden die Daten einem anderen Empfänger offengelegt, muss die Information vor dieser Offenlegung erteilt werden.

D02.04	Datenschutz-Folgenabschätzung Bei einem hohen Risiko für die Rechte und Freiheiten der Betroffenen MUSS der Verantwortliche eine Datenschutz-Folgenabschätzung vorab erstellen, Art. 35 EU-DSGVO. Die Folgenabschätzung SOLL, wenn auch ggf. in einer gekürzten Version, veröffentlich werden.
D02.05	Transparenz für die betroffene Person im Fahrzeug herstellen Die Transparenz der Verarbeitung von personenbezogenen Daten MUSS für die betroffenen Personen auch unmittelbar im Fahrzeug hergestellt werden.
D02.05.01	Transparenz durch HMI herstellen Die Transparenz der Datenverarbeitung SOLL unmittelbar durch das HMI des Fahrzeugs gewährleistet werden.
D02.05.02	Transparenz durch Borddokumente Die Transparenz der Datenverarbeitung SOLL auch durch eine umfassende schriftliche Borddokumentation gewährleistet werden.

8.2.2.2. Nicht-Verkettbarkeit

D03	Nicht-Verkettbarkeit Es MUSS organisatorisch und technisch sichergestellt werden, dass personenbezogene Daten nur für einen bestimmten, vorher festgelegten Zweck erhoben, verarbeitet und genutzt werden.
D03.01	Zweckbindung Die Verarbeitung personenbezogener Daten darf (MUSS) nur für festgelegte, eindeutige und legitime Zwecke stattfinden, Art 5 Abs. 1 b) EU-DSGVO.
D03.01.01	Bestimmung des Verfahrenszwecks Der Zweck der Verarbeitung MUSS vor dem Beginn der Verarbeitung festgelegt werden.
D03.01.02	Legitime Zwecke Es MÜSSEN legitime Zwecke vorliegen.
D03.01.03	Bindung an den Zweck Personenbezogene Daten MÜSSEN in einer mit den festgelegten Zwecken zu vereinbarenden Weise verarbeitet werden, Art. 6 Abs. 4 DSGVO.
D03.01.04	Zweckänderung Die Zwecke dürfen (MUSS) nicht geändert werden, wenn hierfür nicht eine Einwilligung oder Rechtsgrundlage vorliegt.
D03.02	Datensparsamkeit Die Datenverarbeitung MUSS dem Zweck angemessen und erheblich sein, sowie auf das für die Zweckerreichung notwendige Maß beschränkt sein, Art. 5 Abs. 1 c) EU-DSGVO.
D03.03	Anonymität und Pseudonymität Personenbezogene Daten MÜSSEN so früh wie möglich anonymisiert oder pseudonymisiert werden, soweit diese nicht mehr im Form von unmittelbar personenbezogenen Daten für eine Datenverarbeitung mit Rechtsgrundlage benötigt werden.
D03.03.01	Anonymität vor Pseudonymität Die Anonymisierung von Daten SOLL der Pseudonymisierung vorgezogen werden.
D03.03.02	Anonymität Daten SOLLEN anonymisiert werden. Dies ist der Fall, wenn der Personenbezug entfernt wird und keine Möglichkeit mehr besteht, ihn wiederherzustellen.
D03.03.03	Pseudonymität Personenbezogene Daten SOLLEN pseudonymisiert werden. Dies ist der Fall, wenn personenbezogene Daten in einer Weise verändert werden, dass der Personenbezug nur noch über eine Zuordnungsregel wiederhergestellt werden kann, Art. 4 Nr. 5 DSGVO.
D03.05	Getrennte Verarbeitung für unterschiedliche Zwecke Personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, MÜSSEN getrennt verarbeitet werden.

8.2.2.3. Intervenierbarkeit

D04	Intervenierbarkeit Es MUSS sichergestellt werden, dass in ein personenbezogenes Verfahren eingegriffen werden kann. Dabei sind insbesondere die Betroffenenrechte zu berücksichtigen.
D04.01	Recht auf Löschung Es MUSS sichergestellt werden, dass personenbezogene Daten unverzüglich gelöscht werden, wenn die betroffene Person dies berechtigterweise verlangt, Art. 17 DSGVO.
D04.01.01	Löschung bei weiteren Verantwortlichen Wenn personenbezogene Daten durch den Verantwortlichen veröffentlich wurden, SOLL er auch weitere Verantwortliche über die Geltendmachung des Löschanspruchs informieren, Art. 17 Abs. 2 DSGVO.
D04.02	Recht auf Einschränkung der Verarbeitung Es MUSS sichergestellt werden, dass die Datenverarbeitung auf ein begründetes Verlangen der betroffenen Person hin eingeschränkt werden kann, Art. 18 DSGVO.
D04.03	Recht auf Berichtigung Es MUSS sichergestellt werden, dass unrichtige personenbezogene Daten berichtigt werden, wenn die betroffene Person dies begehrt, Art. 16 DSGVO.
D04.04	Recht auf Datenübertragbarkeit Es MUSS sichergestellt werden, dass der Betroffene sein Recht auf Datenübertragbarkeit ausüben kann. Dazu müssen ihm seine personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format übergeben werden können. Der Betroffene hat auch das Recht, die Übermittlung der personenbezogenen Daten an eine andere verantwortliche Stelle zu verlangen, Art. 20 DSGVO. Diese Anforderung kann insbesondere bei Routen, Zielen, favorisierten Ladesäulen und Daten aus dem Infotainmentsystem für die Betroffenen besonders wichtig sei, soweit diese einem Verantwortlichen bereitgestellt wurden.
D04.05	Konfigurationsmöglichkeiten Der Betroffene SOLL die Möglichkeit haben, durch Konfigurationsmöglichkeiten Einfluss auf die Datenerhebung, -verarbeitung und -nutzung zu nehmen.
D04.05.01	Datenschutzfreundliche Voreinstellungen Wenn Konfigurationsmöglichkeiten bestehen, MÜSSEN diese so voreingestellt sein, dass die Datenerhebung, -verarbeitung und -speicherung sowie ihre Zugänglichkeit auf das erforderliche Maß beschränkt sind, Art. 25 Abs. 2 EU-DSGVO
D04.06	Transparente Verwantwortlichkeit Dem Betroffenen MUSS jederzeit klar sein können, wer für die Datenverarbeitung verantwortlich ist.
D04.07	Datenschutzmanagement Die verantwortliche Stelle MUSS über ein Datenschutzmanagement verfügen, welches auf Mängel beim Schutz personenbezogener Daten reagieren und diese beheben kann. Dazu ist eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen vorzunehmen, Art. 32 Abs. 1 d) EU-DSGVO.
D04.07.01	Regelmäßige Überprüfung und Evaluierung Der Verantwortliche MUSS die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig überprüfen und evaluieren.
D04.07.02	Change Management Werden Mängel bezüglich der Wirksamkeit der technischen und organisatorischen Maßnahmen festgestellt, MUSS der Verantwortliche über Prozesse verfügen, mit denen diese Mängel behoben werden können.
D04.08	Abschaltung Der Betroffene SOLL die Möglichkeit haben, die Erhebung von personenbezogenen Daten zu unterbinden, sofern dies rechtlich möglich ist.

D04.09	Sicherheitsupdates Fahrzeuge, die personenbezogene Daten verarbeiten und unmittelbar oder mittelbar über andere Geräte geeignet sind eine Verbindung über Kommunikationsnetzwerke herzustellen, MÜSSEN eine Möglichkeit vorsehen, dass Sicherheitsupdates erfolgen können.
D04.09.01	Kritische Fehler Updates SOLLEN zeitnah erfolgen, über kritische Fehler SOLLEN Kunden von Herstellern umgehend unterrichtet und über Schutzmaßnahmen unterrichtet werden.
D04.10	Widerspruchsrecht Es MUSS technisch und organisatorisch sichergestellt werden, dass die betroffene Person ihr Widerspruchsrecht ausüben kann, Art. 21 DSGVO. Die Verarbeitung der von dem Widerspruch betroffenen Daten ist einzustellen, wenn der Verantwortliche keine zwingenden schutzwürdigen Gründe für die Verarbeitung nachweisen kann.

8.2.2.4. Integrität

D05	Integrität Systeme und Prozesse MÜSSEN die für sie festgelegten Spezifikationen einhalten. Daten müssen unversehrt, vollständig und aktuell bleiben.
D05.01	Richtigkeit der personenbezogenen Daten Personenbezogene Daten MÜSSEN sachlich richtig sein, Art. 5 Abs. 1 d) EU-DSGVO.
D05.02	Unrichtige Daten Es MUSS sichergestellt werden, dass unrichtige Daten unverzüglich gelöscht oder berichtigt werden.
D05.03	Modifikation personenbezogener Daten Es MUSS gewährleistet sein, dass personenbezogene Daten nicht unbefugt modifiziert werden können.
D05.03.01	Modifikation personenbezogener Daten im Backend Es MUSS gewährleistet sein, dass personenbezogene Daten im Backend nicht unbefugt modifiziert werden können.
D05.03.02	Modifikation personenbezogener Daten im Fahrzeug Es MUSS gewährleistet sein, dass personenbezogene Daten im Fahrzeug nicht unbefugt modifiziert werden können.

8.2.2.5. Verfügbarkeit

D06	Verfügbarkeit Es MUSS sichergestellt werden, dass Daten zur Verfügung stehen und ordnungsgemäß verwendet werden können.
D06.01	Schutz vor zufälligem Verlust oder unbefugter Zerstörung Personenbezogene Daten MÜSSEN vor zufälligem Verlust oder unbefugter Zerstörung geschützt werden.
D06.01.01	Sicherungskopien Personenbezogene Daten SOLLEN durch die Anfertigung von Sicherungskopien geschützt werden, Art. 32 Abs. 1 b) DSGVO.
D06.01.02	Redundanz von Hard- und Software Die Verfügbarkeit von personenbezogenen Daten KANN durch Redundanz von Hard- und Software geschützt werden.

8.2.2.6. Vertraulichkeit

D07	Vertraulichkeit Es MUSS sichergestellt werden, dass keine Unbefugten Kenntnis von personenbezogenen Daten erhalten.
D07.01	Vertraulichkeit während der Übermittlung Die Vertraulichkeit von personenbezogenen Daten MUSS während der Übermittlung sichergestellt werden.
D07.01.01	Verschlüsselung bei Übermittlung Personenbezogene Daten MÜSSEN während der Übermittlung verschlüsselt werden.
D07.01.02	Ende-zu-Ende-Verschlüsselung Personenbezogene Daten SOLLEN während der Übermittlung Ende-zu-Ende verschlüsselt werden.
D07.02	Vertraulichkeit gespeicherter Daten Die Vertraulichkeit von personenbezogenen Daten MUSS während der Speicherdauer gewährleistet sein.
D07.02.01	Zugriffsberechtigungen Es MUSS die Möglichkeit bestehen, für Datenverarbeitungssysteme unterschiedliche Zugriffsberechtigungen zu vergeben.
D07.02.02	Vertraulichkeit gegenüber weiteren Nutzern des Fahrzeugs Es SOLL die Möglichkeit geben, vom Nutzer eingebrachte Daten des Infotainmentsystems zu löschen. Dies gilt insbesondere bei Fahrzeugen von Car-Sharing-Anbietern und Mietwagenfirmen.

8.3. Technische Anforderungen

Basierend auf den Anforderungen aus den Abschnitten 8.2 und 8.1 sowie dem Angreifermodell[20] werden die technischen Anforderungen an ein datenschutzfreundliches und benutzerorientiertes System im Kontext der vernetzten Mobilität in diesem Abschnitt aufgeführt.

8.3.1. Funktionale Anforderungen

Bei allen im Folgenden aufgeführten Daten handelt es sich um personenbezogene Daten.

8.3.1.1. Nutzer Information

Nummer	Kategorie	Beschreibung	Bezug
T01	Datenkategorisierung	Das System „Fahrzeug“ MUSS in die Lage versetzt werden die erhobenen, genutzten oder verarbeiteten Daten nach personenbezogen und nicht personenbezogen zu kategorisieren.	D01.01
T11	Beurteilung des Datenschutzniveaus	Das System Fahrzeug SOLL anhand einer Datenbank beurteilen können, ob an den angegebenen Datenübermittlungsorten ein vergleichbares Datenschutzniveau herrscht. Ist dies nicht der Fall MUSS das System dem Betroffenen eine Warnung ausgeben. Auf Wunsch des Betroffenen KANN das System die Datenweitergabe verhindern.	D01.05

[20] Sinner, Nadine et al. Angreifermodel für Selbstdatenschutz im vernetzten Fahrzeug. 08 20167.

Nummer	Kategorie	Beschreibung	Bezug
T12	Information über Datenempfänger	Für den Betroffenen MUSS nachvollziehbar gespeichert werden, welche Daten an wen übermittelt werden. Dabei MUSS ist es ihm möglich sein, die Weitergabe an bestimmte (Dritt-) Parteien zu unterbinden.	D01.02, D02.01, N02.04(1), N03.01
T13	Information über Datenspeicherung	Die speichernde Stelle SOLL bei der Einhaltung des Gesetztes durch das System unterstützt werden, indem jedes Datum mit der Angabe des Betroffenen und der Information zum Vorliegen einer Einwilligung verknüpft wird.	D02.03

8.3.2. Einwilligungen

Nummer	Kategorie	Beschreibung	Bezug
T02	Zwingende Einwilligung	Das System „Fahrzeug“ MUSS zu jedem Datum EINZELN zuordnen können, ob eine Einwilligung zur Datenerhebung, -nutzung und -verarbeitung vorliegt. Liegt diese Einwilligung nicht vor, muss die Datenerhebung, -nutzung und -verarbeitung technisch unterbunden werden können.	D01.01, N02.01
T03	Aktive Einwilligung	Jedem Datum MUSS per Default „keine Einwilligung“ zugeordnet werden. Die Einwilligung MUSS aktiv durch den Betroffenen erfolgen.	D01.01, (D01.01.01), D04.05.01
T04	Authentifizierung des Einwilligers	Es muss technisch sichergestellt werden, dass die Einwilligung tatsächlich durch den Betroffenen erfolgt ist und auch nur für diesen angewendet wird.	D01.01
T05	Informationen vor Einwilligung	Das System „Fahrzeug“ MUSS den Betroffenen vor Einwilligung informieren über: Welches Datum soll erhoben, genutzt oder verarbeitet werden? Zu welchem Zweck wird das Datum erhoben, genutzt oder verarbeitet? Von wem wird das Datum erhoben, genutzt oder verarbeitet? Dauer der Speicherung, Folgen der Nicht-Einwilligung	D01.01.02, D02.04, D03.01.01/02, N03.03, N03.04, N03.05
T06	Einwilligungsnachweis	Das System „Fahrzeug“ MUSS mit Weitergabe eines Datums an ein anfragendes Zielsystem, dieses Zielsystem über das Vorliegen oder Nicht-Vorliegen einer Einwilligung informieren.	D01.01.03
T07	Einwilligungswiderruf	Alle erteilten Einwilligungen MÜSSEN im System „Fahrzeug“ gespeichert werden. Diese Information muss jederzeit von dem Betroffenen aufrufbar sein. Die Einwilligungen müssen hier wieder auf einfache Weise entzogen werden können. Folgen des Widerrufs müssen dem Fahrer dabei vorher deutlich gemacht werden. Ein Widerruf darf die Ausführung der Anwendung als Ganzes nicht beeinträchtigen.	D01.01.04, D01.01.04.02, D04.08, N02.02, N04.02
T08	Vorausgehende Einwilligungsüberprüfung	Die mit dem Datum mitgelieferte Information zum Vorliegen oder Nicht-Vorliegen einer Einwilligung muss aktuell sein. Vor jeder Weitergabe eines Datums muss das Vorliegen der Einwilligung geprüft werden.	D01.01.04
T09	Datenverarbeitung ohne Einwilligung	Es MUSS sichergestellt werden, dass Daten deren Erhebung, Nutzung oder Verarbeitung erforderlich und vertraglich vereinbart ist auch ohne Einwilligung des Betroffenen weitergegeben werden können.	D01.02

Nummer	Kategorie	Beschreibung	Bezug
T10	Übermittlung von Verarbeitungsorten	Die erhebende, verarbeitende oder nutzende Stelle MUSS Informationen zu allen Datenübermittlungsorten mitsenden.	D01.05, N03.02
T14	Zweckgebundene Einwilligung	Mit jedem angefragten personenbezogenen Datum MUSS der Zweck übermittelt werden (siehe auch T5). Die Einwilligung darf nur für diesen Zweck gelten.	D03.01, D03.01.04
T15	Frühzeitige Anonymisierung/Pseudonymisierung	Personenbezogene Daten MÜSSEN so früh wie möglich pseudonymisiert oder besser anonymisiert werden (z.B. über Aggregation).	D03.03, D03.03.01
T16	Datenintegrität	Die Integrität der im Fahrzeug gespeicherten Daten MUSS sicher gestellt werden.	D05.01.02, D05.01, N04.03
T17	Redundanz	Redundanz in der Serverlandschaft MUSS vorhanden sein. Die redundanten Serverlandschaft soll jeweils durch verschiedene Systeme realisiert werden, sodass ein Systemausfall nur ein Teilsystem beeinflusst.	D06, D06.01, D06.01.01/02
T18	Vertraulichkeit	Kryptografische Maßnahmen müssen sicherstellen, dass personenbezogene Daten nicht von Unbefugten ausgelesen werden.	D07, D07.01, D07.01.01/02, N04.01
T19	Zugriffsberechtigungen	Ein rollenbasiertes Zugriffssystem (RBAC) muss verwendet werden, um den Zugriff auf Daten freizugeben.	D07.02.01, D05.03, D05.03.01/02, N04.01
T20	Einfachheit des HMIs	Es MUSS sichergestellt werden, dass das Datenschutz-HMI einfach zu bedienen ist und der Nutzer nicht durch Anzeigen und Kontrollmöglichkeiten abgelenkt wird.	N01.03, N02.04(2), N03.06/07
T21	Datentrennung	Um Korrelationen unter verschiedenen Datensätzen, die zu unterschiedlichen Zwecken verarbeitet/erhoben werden, zu vermeiden, MÜSSEN Daten getrennt versendet, verarbeitet und gespeichert werden, wenn sie für unterschiedliche Zwecke verwendet werden.	D03.04, D03.05
T22	Gezielte und zuverlässige Löschung bestimmter Datensätze	Es MUSS sichergestellt werden, dass wenn ein Nutzer sich entscheidet bestimmte Datensätze (z.B. lokal eingebracht über das Infotainmentsystem oder im Backend beim Dienstleister) endgültig zu löschen, dass diese Daten nicht wiederhergestellt werden können.	D04.01, D04.01.01, N02.03

8.3.3. Nicht-Funktionale Anforderungen

Die Anforderungen sind so zu wählen, dass sie im System “Fahrzeug” skalierbar sind.

Die Hardware im Fahrzeug *MUSS* es ermöglichen die aufgeführten Anforderungen umzusetzen. Dabei werden, abhängig vom Anwendungsfall, bestimmte Anforderungen an die Hardware gestellt.

Nummer	Kategorie	Beschreibung
NT01	Speicher	Der Speicher im Fahrzeug *MUSS* ausreichend sein.
NT02	Rechenzeit	Berechnungen *MÜSSEN* schnell genug durchgeführt werden können.
NT03	Bandbreite	Die Bandbreite der Kanäle *MUSS* schnell genug sein.
NT04	HSM	Sicherheitskritische Operationen (Verschlüsseln, Signieren) *MÜSSEN* in isolierten Umgebungen (TEE) ausgeführt werden, die von Hardware-Sicherheitsmodulen (HSM) instanziiert werden.

Nummer	Kategorie	Beschreibung
NT05	Echtzeitanforderungen	Abhängig vom Anwendungsfall, *MUSS* das System in einer entsprechenden Zeitspanne (Echtzeit) reagieren.

Basierend auf den hier aufgestellten Anforderungen an ein privatsphäreschützendes System für Fahrzeuge werden in den nachfolgenden Arbeitspaketen Technologien erarbeitet, um die Anwendungsfälle aus Kapitel 3 mit geringem Datenaufkommen zu durchzuführen.

Literaturverzeichnis

ABC4Trust: ABC4Trust – Attribute-based Credentials for Trust. 2014 ⟨URL: www.abc4trust.eu⟩

Acatech (Hrsg.): Privatheit im Internet.Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten. Springer Berlin Heidelberg, 2013

Acquisti, Alessandro/John, Leslie K/Loewenstein, George: What is privacy worth? The Journal of Legal Studies, 42 2013, Nr. 2, 249–274

ADAC: Wo Ihr Auto überall Daten speichert . August 2016, https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/daten_auto_spion.aspx?ComponentId=272538&SourcePageId=6729

Amadeo, Ron: Android Auto secrets hint at vehicle diagnostic app, expanded car integration. http://arstechnica.com/cars/2015/07/android-auto-secrets-hint-at-vehicle-diagnostic-app-expanded-car-integration/, 07 2015

Andy Brenner, Gabriel Peal, Nick Pelly: Google I/O 2014 - Android Auto: Developers, Start Your Engines! https://www.youtube.com/watch?v=9vjntxXCUNA, 2014, Accessed: 2016-11-17

Becker, Ralf/Kefelja, Tobias/Jacqueline, Bredereck: Neuer Entwurf für neues BDSG veröffentlicht (2. und 3. Versuch). https://www.datenschutz-grundverordnung.eu/entwurf-neues-bdsg-veroeffentlicht/

Berker, Thomas/Hartmann, Maren/Punie, Yves: Domestication of media and technology. McGraw-Hill Education (UK), 2005

Best, Kirsty/Tozer, Nathan: Scaling digital walls: Everyday practices of consent and adaptation to digital architectural control. International Journal of Cultural Studies, 16 2013, Nr. 4, 401–417

Bock: § 88. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4

Braun: § 91. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4

Braun: § 96. In Beck'scher TKG-Kommentar. Geppert/Schütz, 2013, 4

Buchner, Benedikt: Datenschutz im vernetzten Automobil. Datenschutz und Datensicherheit - DuD, 39 2015, Nr. 6, 372–377 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0432-6⟩, ISSN 1862–2607

BVerfG: Urteil. 12 1983

Cebulla: Umgang mit Kollateraldaten - Datenschutzrechtliche Grauzone für verantwortliche Stellen. ZD Heft 11 2015

Dahlmann, Don: Wie Apple und Google unsere Autos zu Datensammlern machen. Gründerszene, 10 2015, http://www.gruenderszene.de/allgemein/android-auto-daten

Danezis, George/Lewis, Stephen/Anderson, Ross J: How much is location privacy worth? In WEIS. Band 5, Citeseer 2005

Daniel, J. Solove: I've got nothing to hide'and other misunderstandings of privacy. San Diego Law Review, 44 2007, 745–772, https://ssrn.com/abstract=998565

Dinev, Tamara/Hart, Paul: An Extended Privacy Calculus Model for E-Commerce Transactions. Info. Sys. Research, 17 März 2006, Nr. 1, 61–80 ⟨URL: http://dx.doi.org/10.1287/isre.1060.0080⟩, ISSN 1526–5536

Däubler: BDSG § 4a. In Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG. Däubler/Klebe/Wedde/Weichert, 2014, 4. Auflage

Eckert, Svea/Klofta, Jasmin/Strozyk, Jan Lukas: Nackt im Netz: Auch intime Details von Bundespolitikern im Handel. https://daserste.ndr.de/panorama/archiv/2016/Nackt-im-Netz-Intime-Details-von-Politikern-im-Handel,nacktimnetz110.html, 11 2016

Eckhardt: § 91. In Recht der elektronischen Medien. Spindler/Schuster, 2015, 3. Auflage

Enev, Miro et al.: Automobile Driver Fingerprinting. PoPETs, 2016 2016, Nr. 1, 34–50 ⟨URL: http://www.degruyter.com/view/j/popets.2016.2016.issue-1/popets-2015-0029/popets-2015-0029.xml⟩

Ernst: Kapitel I. Allgemeine Bestimmungen. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1, 10–64

Fabio, Udo Di: Grundgesetz-Kommentar. Maunz/Dürig, 76. EGL 2015, Nr. Art. 2, Rn. 131

Faust: BGB § 449. In Beck'scher Online-Kommentar BGB. Bamberger/Roth, 2015, 37. Edition

FIA: What Europeans think about connected cars. 2016, http://www.fiaregion1.com/download/mycarmydata/mycarmydata-public-survey-infographic.pdf

Frenzel: Art. 6. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1

Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Weiterentwicklung des Strommarktes (Strommarktgesetz). Januar 2016, http://dip21.bundestag.de/dip21/btd/18/073/1807317.pdf

Gola/Klug/Körffer: § 32. In BDSG. Gola/Schomerus, 2015, 12. Aufl.

Google: Datenschutzerklärung. April 2017, https://www.google.com/intl/de/policies/privacy/

Haddon, Leslie: Domestication and mobile telephony. Machines that become us: The social context of personal communication technology, 2003, 43–56

Hansen, Marit: Das Netz im Auto & das Auto im Netz. Datenschutz und Datensicherheit, 39 2015, Nr. 6, 367–371 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0431-7⟩

Harendt, Bertram/Wolf, Catharina: Energierechtliche Einordnung der Ladeinfrastruktur für Elektrofahrzeuge Information über geplante Änderungen des Energierechts im Jahre 2016. Januar 2016, http://schaufenster-elektromobilitaet.org/media/media/documents/dokumente_der_begleit__und_wirkungsforschung/Ergebnispapier_Nr_19__Energierechtliche_Einordnung_der_Ladeinfrastruktur_fuer_Elektrofahrzeuge.pdf

Hargittai, Eszter/Marwick, Alice: "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, 10 2016, Nr. 21, http://ijoc.org/index.php/ijoc/article/view/4655, ISSN 1932–8036

Heyde, C. von der: Die ADM Stichproben für Telefonbefragungen. https://www.adm-ev.de/telefonbefragungen/?L=1%2525252527%252529, 07 2013

Hoffmann, Christian Pieter/Lutz, Christoph/Ranzini, Giulia: Privacy Cynicism : An Approach to Understanding the Institutional Privacy Paradox. In Amsterdam Privacy Conference. APC, Oktober 2015, https://www.alexandria.unisg.ch/242936/, 1–25

Hornung, Gerrit: Der Personenbezug biometrischer Daten. Datenschutz und Datensicherheit (DuD) 28 2004, Nr. 7

Hornung, Gerrit: Verfügungsrechte an fahrzeugbezogenen Daten. Datenschutz und Datensicherheit, 39 2015, Nr. 6, 359–366 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0430-8⟩

Hui, Kai-Lung/Tan, Bernard C. Y./Goh, Chyan-Yee: Online Information Disclosure: Motivators and Measurements. ACM Trans. Internet Technol. 6 November 2006, Nr. 4, 415–441, ISSN 1533–5399

Jenny, Valerian: § 88. In Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Plath, Kai-Uwe, 2016, 1

Karaboga, M. et al.: White Paper Das Versteckte Internet: Zu Hause - Im Auto - Am Körper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt 2 Juli 2015

Kent, Jennifer L.: Still Feeling the Car - The Role of Comfort in Sustaining Private Car Use. Mobilities, 10 2015, Nr. 5, 726–747

Keppeler, Lutz Martin: Was bleibt vom TMG-Datenschutz nach der DS-GVO? - Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz. MMR, 2015, Nr. 12, 779

Kremer, Sascha: Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz? RDV, 2014, 240–252

Krieger-Lamina, Jaro: Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen. 2016

Kühling, J./Martini, Mario/Johanna, Heberlein: Die Datenschutz-Grundverordnung und das nationale Recht – Erste Überlegungen zum innerstaatlichen Regelungsbedarf. http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf

Kühling, Jürgen et al.: DIE DATENSCHUTZ-GRUNDVERORDNUNG und DAS NATIONALE RECHT. 2016, http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf

Lieberman, Jonny: 13 Cool Facts About the 2017 Porsche 911. 05 2015 ⟨URL: http://www.motortrend.com/news/13-cool-facts-about-the-2017-porsche-911/⟩

Masur, P.: Situational Privacy and Self-Disclosure. Disseration in Preparation. Universität Hohenheim,, in preparation

Müller-Peters, H: Der vernetzte Autofahrer–Akzeptanz und Akzeptanzgrenzen von eCall Werkstattvernetzung und Mehrwertdiensten im Automobilbereich. Schriftenreihe Forschung am IVW Köln, Bd, 3 2013, 2013

Nissenbaum, Helen: A contextual approach to privacy online. Stanford University Press, 2011, 32–48

Paal: Art. 12. In Datenschutz-Grundverordnung. Paal/Pauly, 2016, 1

Pape, T. von/Trepte, S./Mothes, C.: Privacy by Disaster? Press Coverage of Privacy and Digital Technology. European Journal of Communication

Ribak, Rivka/Rosenthal, Michele: Smartphone resistance as media ambivalence. First Monday, 20 2015, Nr. 11, http://journals.uic.edu/ojs/index.php/fm/article/view/6307

Richter, Michael/Flückiger, Markus D: Usability Engineering kompakt: benutzbare Produkte gezielt entwickeln. Springer-Verlag, 2013

Roßnagel, Alexander: Grundrechtsausgleich beim vernetzten Automobil. Datenschutz und Datensicherheit - DuD, 39 2015, Nr. 6, 353–358 ⟨URL: http://dx.doi.org/10.1007/s11623-015-0429-1⟩, ISSN 1862–2607

Roßnagel, Alexander: Grundrechtsausgleich beim vernetzten Automobil. Datenschutz und Datensicherheit - DuD, 39 2015, Nr. 6, 353–358, http://dx.doi.org/10.1007/s11623-015-0429-1, ISSN 1862–2607

Rosson, Mary Beth/Carroll, John M.: The Human-computer Interaction Handbook. Hillsdale, NJ, USA: L. Erlbaum Associates Inc., 2003 ⟨URL: http://dl.acm.org/citation.cfm?id=772072.772137⟩, ISBN 0–8058–3838–4. – KapitelScenario-based Design, 1032–1050

Rost, Martin/Pfitzmann, Andreas: Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit, 2009, Nr. 6, 353

Sasse, M. A. et al.: Debunking Security-Usability Tradeoff Myths. IEEE Security Privacy, 14 Sept 2016, Nr. 5, 33–39, ISSN 1540–7993

Schantz, Peter: Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016, Nr. 26, 1841

Schiller, Thomas et al.: Datenland Deutschland – Connected Car. 2015 ⟨URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/manufacturing/150909_DEL-15-5015_Brosch%C3%BCre_DasConnectedCar_rz_WEB-safe.pdf⟩

Schoettle, B./Sivak, M.: A survey of public opinion about connected vehicles in the U.S., the U.K., and Australia. In 2014 International Conference on Connected Vehicles and Expo (ICCVE). Nov 2014, ISSN 2378–1289, 687–692

Scholz: BDSG § 3. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage

Scholz: BDSG § 4a. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage

Scholz: BDSG § 6c. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage

Scholz/Sokol: BDSG § 4. In Bundesdatenschutzgesetz. Simitis, 2014, 3. Auflage

Sheeran, Paschal: Intention—Behavior Relations: A Conceptual and Empirical Review. European Review of Social Psychology, 12 2002, Nr. 1, 1–36, http://dx.doi.org/10.1080/14792772143000003

Sheller, Mimi/Urry, John: Mobile Transformations of 'Public' and 'Private' Life. Theory, Culture & Society, 20 2003, Nr. 3, 107–125 ⟨URL: http://tcs.sagepub.com/content/20/3/107.abstract⟩

Shu, C. W.: Privacy or Performance Matters on the Internet: Revisiting Privacy Toward a Situational Paradigm. In Online Consumer Protection: Theories of Human Relativism. IGI Global, 2009, 214–239

Sinner, Nadine et al.: Angreifermodel für Selbstdatenschutz im vernetzten Fahrzeug. 08 20167

Souza Soares, Philipp Alvares de: BMW liefert Gericht Kundendaten für Bewegungsprofil. 07 2016 ⟨URL: http://www.manager-magazin.de/unternehmen/autoindustrie/bmw-autobauer-liefert-gericht-kundendaten-fuer-bewegungsprofil-a-1104050.html⟩

Tamp, Fabian: Under the Hood of Android Auto. https://www.youtube.com/watch?v=KNKGM4ss5Sc, 2014, Accessed: 2016-11-17

Theobald: EnWG § 3. In Energierecht. Danner/Theobald, 2016, 89. EGL

Thiel, Markus: § 21g. In EnWG. Kment, 2015, 1

ThorstenQuandt/Pape, Thilo von: Living in the Mediatope: A Multimethod Study on the Evolution of Media Technologies in the Domestic Environment. The Information Society, 26 2010, Nr. 5, 330–345, http://dx.doi.org/10.1080/01972243.2010.511557

Trepte, S./Masur, P. K.: Privatheitskompetenz in Deutschland. Ergebnisse von zwei repräsentativen Studien. https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Team_MP/Berichte/Privatheitskompetenz_2015-11-04.pdf, 11 2015

Unabhängige Datenschutzbehörden des Bundes und der Länder/Verband der Automobilindustrie (VDA): Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge. 2016, https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Das Standard-Datenschutzmodell (SDM). https://www.datenschutzzentrum.de/sdm/

Verband der Automobilindustrie (VDA): Datenschutz-Prinzipien für vernetzte Fahrzeuge. 2014 ⟨URL: https://www.vda.de/dam/vda/Medien/DE/Themen/Innovation-und-Technik/Vernetzung/Datenschutz-Prinzipien/VDA-Datenschutz-Prinzipien-2014/vda-datenschutzprinzipien-2014.pdf⟩

Weichert: BDSG § 3. In Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG. Däubler/Klebe/Wedde/Weichert, 2013, 3. Auflage

Weichert, Thilo: Datenschutz im Auto – Teil 1. SVR, 2014, Nr. 6, 201

Wilkens, Andreas: Verkehrsminister Dobrindt will fahrerloses Einparken erlauben. 09 2016 ⟨URL: https://heise.de/-3319487⟩

Wirth, Werner/Von Pape, Thilo/Karnowski, Veronika: An integrative model of mobile phone appropriation. Journal of Computer-Mediated Communication, 13 2008, Nr. 3, 593–617

A. Anhang

A.1. Datentaxonomie der Anwendungsfälle

Hier werden die Datenklassifizierung dokumentiert. Grundlage für die Datenklassifizierungen sind die Use Cases, das Dokumentationsformat wird im Folgenden dargestellt. Für jeden Use Case ist ein solcher Abschnitt inkl. der jeweiligen Tabelle zu erstellen.

A.1.1. Car Sharing (Fahrerprofile, Datenlöschung)

A.1.1.1. Registrierung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Identifizierende Daten	Fahrer	personenbezogen, nicht Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungsinformationen	Name des Fahrers, Adresse des Fahrers, Bezahlinformationen des Fahrers (z.B. VISA-Kartennummer)	personenbezogen, nicht Profilbildungsgeeignet

A.1.1.2. Buchung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Identifizierende Daten	Fahrzeug, Fahrer	personenbezogen, nicht profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer mit Bewegungsinformationen	Kunden-ID, Kennzeichen des Fahrzeugs, Fahrzeugtyp, Bezahlinformationen des Fahrers (z.B. VISA-Kartennummer)	personenbezogen, Profilbildungsgeeignet
Ortungsdaten (Verfügbare Fahrzeuge)	Fahrer, Fahrzeug	nicht personenbeziehbar, nicht Profilbildungsgeeignet	einmalig übertragen, ohne Speicherung	GPS-Daten Fahrer, GPS-Position verfügbare Flotte	personenbeziehbar, Profilbildungsgeeignet

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Buchungs-information	Fahrzeug, Fahrer	personenbeziehbar, Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer mit Bewegungs-informationen	Kennzeichen des Fahrzeugs, Kunden-ID des Fahrers, Bezahl-informationen des Fahrers (z.B. VISA-Kartennummer), Buchungszeit-punkt, Buchungsort, Buchungsdauer, ggf. Handynummer	personenbeziehbar, Profilbildungsgeeignet

A.1.1.3. Fahrt

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Positionsdaten (Geofencing)	Fahrzeug	personenbeziehbar, profilbildungsgeeignet beziehbar	mehrmals übertragen, ohne/mit Speicherung in Profil über Fahrzeug mit Bewegungsinfor-mationen	Position des Fahrzeugs, VIN	personenbeziehbar, profilbildungsgeeignet
Fahrzeug-ent-riegelung (solange nicht direkt)	Fahrzeug	personenbeziehbar, nicht Profilbildungsgeeignet	einmalig übertragen, ohne Speicherung	Zeitpunkt, VIN	personenbeziehbar, profilbildungsgeeignet beziehbar
Nutzungs-information (Checkout)	Fahrzeug	nicht personenbeziehbar, nicht Profilbildungsgeeignet	einmalig übertragen, ohne/mit Speicherung in Profil über Fahrzeug mit Bewegungsinfor-mationen	Zeitpunkt, Position des Fahrzeugs, Fahrzeugzustand (of-fen/abgeschlossen; Tankfüllung, gefahrene Kilometer während der Buchung etc.)	personenbeziehbar, profilbildungsgeeignet beziehbar
Nutzungs-information (Nutzungsprofile)	Fahrzeug, Fahrer	nicht personenbeziehbar, nicht Profilbildungsgeeignet	nicht übertragen, ohne Speicherung	App-Profile, Navigationsziele	personenbeziehbar, Profilbildungsgeeignet

A.1.1.4. Schadensmeldung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Schadensmeldung vor Fahrbeginn	Fahrer, Fahrzeug	personenbeziehbar, nicht Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen	Zeitpunkt, Schadensmeldung, Fahrer ID, Fahrzeugkennung	personenbeziehbar, nicht Profilbildungsgeeignet
Fahrzeugzustand bei Unfall	Fahrzeug	personenbeziehbar, nicht profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen	Schadensart (Komponenteninformation), Zeitpunkt, VIN	personenbeziehbar, nicht Profilbildungsgeeignet

A.1.2. Werkstatt

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (kombiniert)
Fahrzeugzustandsdaten	Fahrzeug, Fahrer	nicht personenbeziehbar, keine besondere Kategorie, profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen (wohl zumindest ob Reparaturbedarf)	Fehlermeldungen, Verschleißdaten, Zähler für Anzahl und Länge Fahrten, Positionsdaten, Batteriezustand, Kilometerstand, Verbrauch, Reifendruck, Navigationsdaten	personenbezogen, keine besondere Kategorie, profilbildungsgeeignet
Abrechnungsdaten (Fernwartung)	Fahrzeug	personenbezogen, keine besondere Kategorie, profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrzeug ohne Bewegungsinformationen	Abrechnungsdaten, Fahrzeugidentifikator, Umfang der gebuchten Leistungen	personenbezogen, keine besondere Kategorie, profilbildungsgeeignet
Unfalldatenschreiberdaten	Fahrzeug, Fahrer	nicht personenbezogen, keine besondere Kategorie, profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen	Geschwindigkeit, Richtung, Beschleunigung, Blinkertätigkeit, Bremstätigkeit, Ort, Zeit, Auslösung von Assistenzsystemen	personenbezogen, keine besondere Kategorie, profilbildungsgeeignet

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (kombiniert)
eCall-Daten (Minimum Data Set)	Fahrzeug, Fahrer	personenbeziehbar, keine besondere Kategorie, profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinformationen (Dauer abhängig von Mitgliedsstaatlichen Regelungen)	Unfallort, Unfallzeitpunkt, Fahrtrichtung, FahrzeugID, Service ProviderID, eCall-Qualifier	personenbezogen, keine besondere Kategorie, profilbildungsgeeignet

A.1.3. Ortung und Reaktion

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Identifizierende Daten	Fahrer	personenbezogen, keine besondere Kategorie, nicht Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungsinformationen	Authentifizierungsdaten (Name, Geburtsdatum, Adresse, ...)	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet
Konfiguration	Fahrzeug, Fahrer	personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungsinformationen	Interessen, Präferenzen, Einschränkungen	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet
Aktionsparameter	Fahrzeug, Fahrer	personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet	mehrmals übertragen, ohne Speicherung ODER einmalig übertragen, mit Speicherung in Profil über Fahrer mit Bewegungsinformationen	Interessen, POI-Daten, Authentifizierungsdaten, Fahrzeugposition	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet
Ortungs- und Routendaten	Fahrzeug, Fahrer	personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in Profil über Fahrer mit Bewegungsinformationen	Position, Zeit, Reiseziel, Reiseroute	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet

A.1.4. Android Auto

Bei der ersten verwendung von Android Auto erscheint ein Hinweiß über die Verwendung on Daten im Fahrzeug. Der Android Auto Sicherheitshinweise besagt: „Möglicherweise werden Fahrzeugdaten von Ihrem Fahrzeug an ihr Telefon gesendet, z.B. Marke, Modell, GPS-Daten, Kraftstofffüllstand, Kilometerzähler, Geschwindigkeit und Gang, Belegung

des Beifahrersitzes und andere Daten zum Zustand Ihres Fahrzeugs und seinen Sensoren. Diese Daten werden nicht mit Ihrem Google Konto verknüpft und entsprechend unserer Datenschutzerklärung (s.[1]) behandelt."

A.1.4.1. Registrierung

Funktionaler Bereich	beschriebenes Objekt	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	Enthaltene Daten	Personenbeziehbarkeit /besondere Kategorie/ Profilbildungseignung (kombiniert)
Identifizierende Daten	Fahrer	personenbezogen, keine besondere Kategorie, profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungs-informationen	Identität des Google-Kontos (Name, Geburtsdatum, Geschlecht, Telefonnummer, Zweit-Email), Geräte-ID (Telefon, PC, ...), IP-Adressen, Cookie-Daten, Standortinforma-tionen, Konten auf dem Gerät	personenbezogen, besondere Kategorie, profilbildungsgeeignet

[1] Google Datenschutzerklärung. April 2017.

A.1.4.2. Fahrt (Navigation, Telefonie, Musik)

Funktionaler Bereich	beschriebenes Objekt	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	Enthaltene Daten	Personenbeziehbarkeit /besondere Kategorie/ Profilbildungseignung (kombiniert)
Ortungs- und Routendaten	Fahrzeug, Fahrer, Mobile Device	personenbeziehbar, Kategorie ableitbar, Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in anonymer Datenbank [2]	Kompass, Gyroskop, Geschwindigkeit (RPM) und Gang, GPS, Kraftstofffüllstand, Kilometerzähler [2][3][4][5][6]	s.o.
Telefoniedaten	Fahrzeug, Fahrer, Mobile Device	personenbeziehbar, Kategorie ableitbar, Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung	Kontaktliste, SMS, Anrufliste	s.o.
Audiodaten	Fahrzeug, Fahrer, Mobile Device	nicht personenbeziehbar, Kategorie ableitbar, Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung	Titel, Playlists, Podcasts	s.o.
Weitere Daten (Funktion unbekannt)	Fahrzeug, Fahrer,Mobile Device	nicht personenbeziehbar, keine besondere Kategorie, nicht Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in anonymer Datenbank [2]	Marke, Modell, Belegung des Beifahrersitzes	s.o.
Unbekannte Daten	Fahrzeug, (Fahrer)	??	??	„[. . .] andere Daten zum Zustand Ihres Fahrzeugs und seinen Sensoren.“[2]	s.o.

A.1.5. Paket Auto

Funktionaler Bereich	beschriebenes Objekt	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	Enthaltene Daten	Personenbeziehbarkeit /besondere Kategorie/ Profilbildungseignung (kombiniert)
Ortungsdaten	Fahrzeug	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet	mehrmals übertragen, ohne Speicherung	Position, Zeit	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet ”
Parkplanung/ Kalender	Fahrzeug	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer	geplante Parkposition zu einem Zeitpunkt in der Zukunft	

[2] Dahlmann, Don Wie Apple und Google unsere Autos zu Datensammlern machen. Gründerszene, 10 2015

[3] Andy Brenner, Gabriel Peal, Nick Pelly Google I/O 2014 - Android Auto: Developers, Start Your Engines! https://www.youtube.com/watch?v=9vjntxXCUNA, 2014.

[4] Tamp, Fabian Under the Hood of Android Auto. https://www.youtube.com/watch?v=KNKGM4ss5Sc, 2014.

[5] Amadeo, Ron Android Auto secrets hint at vehicle diagnostic app, expanded car integration. http://arstechnica.com/cars/2015/07/android-auto-secrets-hint-at-vehicle-diagnostic-app-expanded-car-integration/, 07 2015.

[6] Lieberman, Jonny 13 Cool Facts About the 2017 Porsche 911. 05 2015 ⟨URL: http://www.motortrend.com/news/13-cool-facts-about-the-2017-porsche-911/⟩.

Funktionaler Bereich	beschriebenes Objekt	Personenbeziehbarkeit/ besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	Enthaltene Daten	Personenbeziehbarkeit /besondere Kategorie/ Profilbildungseignung (kombiniert)
Zustellstatus	Fahrzeug, Paket	personenbezogen, keine besondere Kategorie, nicht Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in Profil über Fahrer	Status Kofferraum, Position des Paketzustellers	”

A.1.6. Umgebung/ Parkdienst

A.1.6.1. Datensammlung und Auswertung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Parkplatz-informationen	Umgebung	nicht personenbeziehbar, keine besondere Kategorie, nicht Profilbildungsgeeignet	mehrmals übertragen, mit Speicherung in anonymer Datenbank	erkannte Parklücken, erkannte Parkhausinforma-tionen	nicht personenbeziehbar, keine besondere Kategorie, nicht Profilbildungsgeeignet

A.1.6.2. Dienstnutzung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Ortungs- und Routendaten	Fahrzeug, Fahrer	nicht personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet	mehrmals übertragen, ohne Speicherung	Position, Zeit, Reiseziel, Reiseroute	nicht personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet

A.1.6.3. Parkplatzbuchung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Ortungs- und Routendaten	Fahrzeug, Fahrer	nicht personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrzeug mit Bewegungsinfor-mationen	Position, Zeit, Reiseziel, Reiseroute	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Identifizierende Daten	Fahrzeug, Fahrer	personenbezogen keine besondere Kategorie, nicht Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer mit Bewegungs-informationen	Kennzeichen des Fahrzeugs, Name des Fahrers, Bezahl-informationen des Fahrers (z.B. VISA-Kartennummer)	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet
Bezahl-informationen	Fahrer	personenbezogen , keine besondere Kategorie, nicht Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer mit Bewegungs-informationen	Bezahl-informationen des Fahrers (z.B. VISA-Kartennummer), Parkplatzbuchung	personenbezogen, keine besondere Kategorie, Profilbildungsgeeignet

A.1.7. Verschleißanalyse

Informationen entnommen aus[7].

A.1.7.1. Batterie

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Ladeeigenschaften	Ladesäulen, Energielie-ferant, Fahrzeug, Fahrer	nicht personenbeziehbar	bei Ausschalten der Zündung und Absperren des Fahrzeuges; Profil zu Anzahl, Dauer und Lademenge; Profil zu Ladesäulen	Ladespannung, Qualität der Ladespannung (Ausfälle)	personenbeziehbar (Rückschlüsse auf ein sehr abstraktes Fahrverhalten und das Ladeverhalten)
Batterie-eigenschaften	Fahrzeug	nicht personenbeziehbar	bei Ausschalten der Zündung und Absperren des Fahrzeuges; Profil über Entwicklung des Batteriezustands	Ladezustand, Zelltemperaturen	personenbeziehbar (Rückschlüsse auf Fahrverhalten)
Nutzungsverhalten	Fahrzeug, Fahrer	personenbeziehbar, keine besondere Kategorie	bei Ausschalten der Zündung und Absperren des Fahrzeuges; Profile zu Fahrverhalten	Range Externder Einsatz (Anzahl), Ladestecker eingesteckt (Anzahl), Fahrmodus (ECO/SPORT), Ladelänge, Kilometerstand	personenbeziehbar

[7] ADAC Wo Ihr Auto überall Daten speichert . August 2016.

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Identifizierende Daten	Fahrzeug, Fahrer	personenbeziehbar, keine besondere Kategorie	bei Ausschalten der Zündung und Absperren des Fahrzeuges; Verknüpfung von Profilen	Kennzeichen des Fahrzeugs, Name des Fahrers, VIN	personenbeziehbar, keine besondere Kategorie

A.1.8. Laden und Bezahlen

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Vertrags-information	Halter	personenbeziehbar, keine besondere Kategorie	einmalig übertragen; in Profil über Fahrer ohne Bewegungs-informationen	Vor-& Nachname, Wohnort, Geburtstag, Geschlecht, OEM Provisioning Certificate (Zertifikats-ID,öff. Schlüssel), Bezahl-informationen des Fahrers (z.B. VISA-Kartennummer)	personenbeziehbar, keine besondere Kategorie
Identifikation	Halter, Fahrzeug, CH, MO	personenbeziehbar, keine besondere Kategorie	einmalige Übertragung, dauerhafte Speicherung in Profil über Fahrer ohne Bewegungs-informationen	ID für Freischaltung der Nutzer	personenbeziehbar, keine besondere Kategorie
Abrechnung	Fahrer	personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet	mehrmalige Übertragung (bei jedem Laden und für die Abrech-nung),Profil über Fahrer mit Bewegungsinfor-mationen	Position der Ladestation, Ladelänge, Stomverbrauch, ID	personenbeziehbar, keine besondere Kategorie, Profilbildungsgeeignet

A.1.9. Fahrerverhalten

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Vertrags-information	Fahrer	personenbezogen, nicht Profilbildungsgeeignet	einmalig übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungs-informationen	Vor- & Nachname, Wohnort, Geburtstag, Geschlecht, Fahr-gestellnummer, Führerschein, Informationen über weitere Fahrer, Jahreskilometer	personenbeziehbar, Profilbildungsgeeignet
Fahrzeugzustand	Fahrzeug	nicht personenbezogen, nicht Profilbildungsgeeignet	mehrfach übertragen, mit Speicherung in Profil über Fahrzeug ohne Bewegungsinfor-mationen	Komponentendaten, Fahrzeugdaten	personenbeziehbar, nicht Profilbildungsgeeignet
Fahrverhaltens-informationen	Fahrer, Fahrzeug	personenbeziehbar, Profilbildungsgeeignet	mehrfach übertragen, mit Speicherung in Profil über Fahrer ohne Bewegungs-informationen	Geschwindigkeit, Motorumgrehun-gen, Brems- und Gaspedalstellung, Motortemperatur, Abgaswerte, VIN/KD-ID/OBD-ID	personenbeziehbar, Profilbildungsgeeignet

A.1.10. Fahrerüberwachung

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Müdigkeit	Fahrer	personenbeziehbar, profilbildungsgeeignet	kurzzeitige Speicherung auf Fahrzeug ODER mehrfache Übertragung (Speicherung?)	Augenbewegungen, Innenraumbild, Lenkradwinkel	personenbeziehbar, profilbildungsgeeignet
Alkoholisierung, Drogeneinfluss	Fahrer	personenbeziehbar, profilbildungsgeeignet	kurzzeitige Speicherung auf Fahrzeug ODER mehrfache Übertragung (Speicherung?)	Luftzusammen-setżung, Augenbewegun-gen, Innenraumbild, Lenkradwinkel	personenbeziehbar, profilbildungsgeeignet
Bewusstseins-störungen	Fahrer	personenbeziehbar, profilbildungsgeeignet	kurzzeitige Speicherung auf Fahrzeug ODER mehrfache Übertragung (Speicherung?)	Augenbewegungen, Innenraumbild, Lenkradwinkel	personenbeziehbar, profilbildungsge-eignet

Funktionaler Bereich/ Kategorie	beschriebenes Objekt	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (isolierte Betrachtung)	Übertragung/ Profilbildung	enthaltene Daten	Personenbeziehbarkeit / besondere Kategorie/ Profilbildungseignung (kombiniert)
Abwendung der Aufmerksamkeit von Fahraufgabe	Fahrer	personenbeziehbar, profilbildungsgeeignet	kurzzeitige Speicherung auf Fahrzeug ODER mehrfache Übertragung (Speicherung?)	Augenbewegungen, Innenraumbild, Lenkradwinkel	personenbeziehbar, profilbildungsgeeignet

SeDaFa

2. August 2017

SeDaFa-D1-1.0