baum reiter & collegen
Rechtsanwaltsgesellschaft mbH

Gutachten

Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung

Notwendigkeit, Modell, gesetzliche Grundlagen

Düsseldorf, 15. November 2022

Gefördert durch:

Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Auftraggeber:

Verbraucherzentrale
Bundesverband e.V.
Rudi-Dutschke-Straße 17
10969 Berlin

Autoren und Mitwirkende:

Verfasser: **Rechtsanwalt Prof. Dr. Julius Reiter**
Professor für Wirtschaftsrecht
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für IT-Recht

Rechtsanwalt Dr. Olaf Methner
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Arbeitsrecht
Fachanwalt für IT-Recht

Rechtsanwalt Bénédict Schenkel
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für IT-Recht

Baum Reiter & Collegen Rechtsanwaltsgesellschaft mbH

Standort Düsseldorf
Benrather Schlossallee 101
40597 Düsseldorf

Standort Berlin
Hausvogteiplatz 11a
10117 Berlin

Tel.: 0211 / 836 805-70
E-Mail: kanzlei@baum-reiter.de

In Kooperation mit:

Dr.-Ing. E.h. Jürgen Bönninger
Sachverständiger für das Kraftfahrwesen
Dozent an der Fakultät für Verkehrswissenschaften TU Dresden

INHALTSÜBERSICHT

A. Einführung

Durch den Betrieb moderner Fahrzeuge entstehen große Datenmengen verschiedener Art, bezeichnet als Mobilitätsdaten, wie z. B. Fahrzeugstatus-Informationen, Umgebungszustände, Betriebszustände von Systemkomponenten oder Positionsangaben. Der Fahrzeughersteller nutzt diese Daten zur Produktbeobachtung und -weiterentwicklung. Sie können jedoch auch die Grundlage für digitale Dienstleistungen rund um das Fahrzeug sein, hoheitliches Handeln ermöglichen und fördern oder durch das Anlegen und Analysieren großer Datenpools einen Mehrwert für die Gemeinschaft darstellen.[1] Voraussetzung für das alles ist jedoch, dass Mobilitätsdaten überhaupt zugänglich sind. Aufgrund der aktuellen technischen Gegebenheiten kontrolliert derzeit allein der Fahrzeughersteller faktisch den Datenzugang im Fahrzeug. Gemäß Werkskonfiguration und aufgrund fehlender Schnittstellen sehen vernetzte Fahrzeuge weder für den Fahrzeugnutzer[2] selbst noch für sonstige Dritte einen unmittelbaren Zugriff auf im Fahrzeug generierte Daten vor. Dies führt zur einer faktischen Datenhoheit der Fahrzeugsteller. Daraus resultieren zum einen wettbewerbliche Herausforderungen und Risiken, wie z. B. Risiken für ein Marktversagen, letztlich auch zulasten der Verbraucher. Zum anderen wird der Fahrzeugnutzer in seiner selbstbestimmten Datennutzung eingeschränkt. Hinzu kommt der wichtige Umstand, dass Mobilitätsdaten nach herrschender Auffassung regelmäßig als „personenbezogene Daten“ im Sinne des Datenschutzrechts zu qualifizieren sind, so dass die Verarbeitung von Mobilitätsdaten die konsequente Beachtung von Datenschutzrecht bedingt. Die faktische Datenhoheit der Hersteller begegnet daher auch datenschutzrechtlichen Bedenken.

Die Debatte der letzten Jahre drehte sich mithin um zwei Themenschwerpunkte. Zum einen: Wird der Datenschutz, wie er im Hinblick auf personenbezogene Mobilitätsdaten aus vernetzten Fahrzeugen in praxi gelebt wird, den gesetzlichen Anforderungen gerecht oder bedarf es ergänzender verbindlicher Vorgaben durch Verwaltung oder Gesetzgeber? Zum anderen: Wie wirkt sich die faktische Datenhoheit der Fahrzeughersteller auf Märkte und Verbraucher aus und sollte in den Status quo „Zugang zu Mobilitätsdaten“ regulierend eingegriffen werden? Während die datenschutzrechtliche Diskussion in den letzten beiden Jahren etwas erkaltet ist, befindet sich der politische Diskurs um den Datenzugang auf seinem Höhepunkt.

Im „Ampel“-Koalitionsvertrag der Legislaturperiode 2021-2025 von SPD, B 90/DIE GRÜNEN und FDP wurde vereinbart, dass

[1] Vgl. insoweit die Use Cases unter D.III.

[2] Im Folgenden wird, soweit nicht anders benannt, der Begriff des „Fahrzeugnutzers“ verwandt und dabei unterstellt, dass dieser gleichzeitig Käufer, Fahrer, Halter und Eigentümer des Fahrzeugs ist.

> *zur wettbewerbsneutralen Nutzung von Fahrzeugdaten […] ein Treuhänder-Modell an[gestrebt] [werden soll], das Zugriffsbedürfnisse der Nutzer, privater Anbieter und staatlicher Organe sowie die Interessen betroffener Unternehmen und Entwickler angemessen berücksichtigt*.[3]

Damit sprechen die Regierungsparteien eine (gesetzliche) Änderung an der Dateninfrastruktur dergestalt an, dass nicht mehr nur der Fahrzeughersteller über einen direkten Zugang ins Fahrzeug verfügt, sondern eben auch eine neutrale dritte Stelle. Diese neutrale Stelle sollte sodann als Datentreuhänder die Daten verarbeiten. Gleichzeitig hat sich der europäische Gesetzgeber der Frage des Zugangs zu Mobilitätsdaten angenommen und strebt eine sektorspezifische Regulierung durch Änderung der Typengenehmigungsverordnung[4] an. Mittels Konsultationen, an denen sich die verschiedenen Interessensgruppen entlang der Fahrzeugwertschöpfungskette beteiligen können, ist die Europäische Kommission damit befasst, den Regelungsbedarf festzustellen.[5] Ein Regulierungsvorschlag ist, nach bereits wiederholter Verschiebung, aktuell für das erste Quartal 2023 angekündigt.

Die Frage des Zugangs zu Mobilitätsdaten bleibt jedoch eng verknüpft mit den datenschutzrechtlichen Herausforderungen, die sich bei der Nutzung vernetzter Fahrzeuge stellen. Das Vorliegen der Voraussetzungen einzelner Rechtfertigungstatbestände zur Datenverarbeiten gemäß der DSGVO bleibt umstritten. Insbesondere stellen eine Datenschutz-Informationsüberlastung der betroffenen Person im Fahrzeug sowie die Nutzung eines Fahrzeugs durch verschiedene Fahrer oder Beifahrer sowohl die Wirksamkeit als auch den Sinn- und Zweck der Einwilligung zur Datenverarbeitung in Frage. Der Betroffene erhält überdies nur eingeschränkte Informationen über die tatsächlichen Datenverarbeitungsvorgänge seines Fahrzeugs. Abhilfe schaffen könnten sogenannte Personal Information Management Systeme (PIMS), die bei der Abgabe datenschutzrechtlicher Einwilligungen assistieren, Informations- und Beratungsfunktionen wahrnehmen sowie bei der Wahrnehmung von Datenschutz- und Verbraucherschutzrechten unterstützen.[6]

Die Aufnahme eines Datentreuhänder-Modells in den „Ampel"-Koalitionsvertrag zeigt, dass die Regierung gewillt ist, das Thema „Zugang zu Mobilitätsdaten" anzugehen. Die im Vergleich zu anderen Rohstoffen besonderen Eigenschaften von Daten (keine Abnutzbarkeit, keine Exklusivität, keine Rivalität) streiten gegen eine Verknappung und für eine umfangreiche und trans-

[3] Vgl. Ampel-Koalitionsvertrag 2021-2025, S. 52.

[4] Verordnung (EU) 2018/858.

[5] Siehe hierzu die Initiative der Europäischen Kommission „Zugang zu Fahrzeugdaten, -funktionen und -ressourcen, Ref. Ares(2022)2302201.

[6] Vgl. hierzu z. B. das Positionspapier des Verbraucherzentrale Bundesverband „Fahrerlos alle mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht", 12. Oktober 2021, S. 15.

parente Nutzbarkeit. Neben der Zugangsfrage sollte sich die Bundesregierung jedoch gleichzeitig auch der Defizite annehmen, die bei der Umsetzung von Datenschutzrechten festzustellen sind. Ein „Mobilitätsdatenwächtermodell“, wie es nachfolgend skizziert und beschrieben wird, kann hier als umfassendes Modell für eine verbrauchergerechte Problemlösung herangezogen werden.

B. Gutachterauftrag

In Ansehung der Herausforderungen, die aus Verbrauchersicht beim Umgang mit Mobilitätsdaten bestehen, sowie in Anknüpfung an die Ankündigungen im Koalitionsvertrag, stellt sich für den Verbraucherzentrale Bundesverband e.V. die Frage nach einem Modell, das einen verbrauchergerechten Umgang mit Mobilitätsdaten gewährleistet. In Betracht kommt, soweit erforderlich durch Schaffung entsprechender neuer gesetzlicher Grundlagen, die Einführung eines „Mobilitätsdatenwächters“, der zusammen mit einem Datentreuhänder einen datenschutzkonformen Zugang zu Mobilitätsdaten sicherstellt.

Der erste Hauptteil des Gutachtens definiert den Begriff der Mobilitätsdaten sowie die Datenverarbeitung im Fahrzeug und stellt die Ausgangslage im Hinblick auf den Zugang sowie die datenschutzrechtlichen und wettbewerblichen Herausforderungen dar. Ein Überblick zu den aktuellen Systemen der Fahrzeughersteller zeigt den Status quo aus Verbrauchersicht (siehe unter C).

Aus der Ausgangslage resultiert das Regelungsbedürfnis. Ein zweiter Hauptteil widmet sich daher der Beschreibung eines „Mobilitätsdatenwächtermodells“ im Hinblick auf Struktur und Rollenmodell sowie auf die institutionelle Ausgestaltung, die Qualitätssicherung und die Finanzierung. Das Kapitel schließt mit einer Darstellung ausgewählter Use Cases, auf die das „Mobilitätsdatenwächtermodell“ angewendet werden kann (siehe unter D)

Das Gutachten endet vor einer Zusammenfassung (siehe unter F) mit Vorschlägen für eine gesetzliche Umsetzung des „Mobilitätsdatenwächtermodells“ unter Berücksichtigung sowohl nationaler als auch europäischer Gesetzgebung (siehe unter E).

Die nachfolgenden gutachterlichen Ausführungen verhalten sich indes nicht unmittelbar zu spezielleren Diskussionen um den Zugang, die Verarbeitung und die Nutzung von Mobilitätsdaten, soweit die folgenden Bereiche betroffen sind:

- Unfalldatenspeicher; EDR = Event data recorder; ab 2024 in jedem neu zugelassenen Fahrzeug Pflicht; Speicherung von Unfalldaten im Fahrzeug.

- Fahrmodusspeicher; entspricht DSSAD = Data storage system for automated driving nach ECE Regelung 157; hier sind u.a. die Ausgestaltung des Speicherortes der regi-

onalen oder nationalen Gesetzgebung überlassen; § 63a StVG schreibt eine kurzzeitige Speicherung von Daten, insb. Zeitpunkt, Wechsel zwischen Mensch und System, bei automatisierten Fahrfunktionen vor; diskutiert wird, ob diese Daten auf einem Treuhandserver gespeichert werden sollen.

- Autonomes Fahren; gemäß § 1g StVG i.V.m. Anlage 2 der Autonome Fahrzeug-Genehmigungs- und Betriebsverordnung (AFGBV) werden bestimmte Fahrzeugdaten ereignisbasiert erfasst und sind dem Kraftfahrt-Bundesamt (KBA) zur Erfüllung seiner Aufgaben zugänglich zu machen.

- Mobilitätsdatenverordnung (MDV)[7]; Die MDV regelt die Bereitstellungspflicht von Daten der Mobilitätsanbieter (Betreiber von öffentlichem Nah- und Fernverkehr) zur Ermöglichung einer effizienten, sicheren und umweltverträglichen Mobilität der Zukunft, zur Kontrolle der Einhaltung von Pflichten aus dem Personenbeförderungsgesetz (etwa Rückkehrpflicht) sowie zur Bereitstellung multimodaler Reiseinformationsdienste.

Vorgenannte Themenfelder regeln einzelne Teilbereiche der Verarbeitung von Mobilitätsdaten. Indes verfolgt der vzbv – und so auch dieses Gutachten – aus Verbrauchersicht das Ziel, dass mit dem „Mobilitätsdatenwächtermodell“ der grundsätzliche Umgang mit Mobilitätsdaten festgeschrieben wird.

[7] Verordnung vom 20. Oktober 2021 (BGBl. I S. 4728).

C. Ausgangslage

I. Entstehung und Verarbeitung von Mobilitätsdaten im Fahrzeug

In vernetzten Fahrzeugen verbaute Sensoren und Steuergeräte generieren, insbesondere bei der Bewegung des Fahrzeugs, eine Vielzahl von Daten. Unter der Bezeichnung „Mobilitätsdaten“ werden im hiesigen Kontext die folgenden Datenarten verstanden:[8]

- Fahrzeugdaten (wie Identifizierungsdaten, Leistung, Verbrauch, Abmessungen, Lasten, Achsen, Zustand, Diagnose, Fehler, Störungen, Mängel, Verschleiß, Schäden u. a.)
- Fahrzeugbediendaten (Beschleunigung, Verzögerung, Gierraten, Lenkradwinkel, Betätigung, Fahrmodus u. a.)
- Fahrzeugumgebungsdaten (Daten von Umgebungssensoren wie Kamera, Radar, Lidar sowie zu Temperatur, Position, Witterung, Verkehrsbelastung etc.)
- Infrastrukturdaten (Verkehrszeichen, Lichtsignalanlagen, Baustellen, andere Fahrzeuge u. a.)
- Ereignisdaten (Unfall, Gefahrensituationen)

Bestimmte Daten werden weder im Fahrzeug gespeichert noch nach außen übermittelt, sondern gewährleisten zunächst lediglich die vorgesehenen Fahrzeugfunktionen (insb. Fahrfunktion, Entertainment, Komfort, sonstige digitale Serviceangebote). Indes kann soweit erforderlich eine Speicherung von Mobilitätsdaten im Fahrzeug selbst mittels flüchtiger oder fester Speicher vorgesehen sein.[9] Darüber hinaus kommt eine Übertragung von Mobilitätsdaten nach außen per Mobilfunkschnittstelle (over-the-air) in Betracht. Die Daten können dann extern weiterverarbeitet werden.

Mobilitätsdaten weisen regelmäßig einen Personenbezug auf, so dass das Datenschutzrecht auf sie anzuwenden ist.[10] Darüber hinaus und soweit nicht anders dargestellt, gelten die nachfolgenden Ausführungen auch für Daten ohne Personenbezug.

II. Zugang zu Mobilitätsdaten

Entlang der Fahrzeugwertschöpfungskette und darüber hinaus haben sich Interessensgruppen herausgebildet, die einen Zugang zu Mobilitätsdaten begehren. Unter folgenden Gruppen kann differenziert werden:

---

[8] Vgl. entsprechend zur Kategorisierung von Mobilitätsdaten die Studie Denker et al. für das Bundesministerium für Verkehr und digitale Infrastruktur in „Eigentumsordnung für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive“, 2017, S. 20.

[9] Vgl. hierzu Bönninger in zfs 2014, 184.

[10] Siehe näher unter C.III.1.

- Fahrzeughersteller
- Fahrzeugnutzer
- Dritte: Andere Teilnehmer am Straßenverkehr (z. B. Fußgänger, Radfahrer), ÖPNV, Straßenbaulastträger, Infrastruktureinrichtungen, Behörden (für Genehmigung, Marktüberwachung, Produktbeobachtung), Organe der Rechtspflege (z. B. Staatsanwaltschaft), Prüforganisationen, Sachverständige, wissenschaftliche Forschungseinrichtungen, Versicherer, Plattformbetreiber, sonstige Dienstleister (Werkstätten, Pannenservice, Navigationsdienste, Konsumanbieter, Entertainmentanbieter)

Allerdings wird der Zugang zu Mobilitätsdaten technisch und damit faktisch im Wesentlichen von dem jeweiligen Fahrzeughersteller kontrolliert. Die Zugangsmöglichkeiten des Fahrzeugnutzers oder sonstiger Dritter ist begrenzt, wie sich aus den nachfolgenden Ausführungen ergibt.

1. Faktische Datenhoheit der Fahrzeughersteller

Bedingt durch die technischen Gegebenheiten im Fahrzeug kontrolliert der jeweilige Fahrzeughersteller den Datenzugang im Fahrzeug. Soweit das Fahrzeug über eine Mobilfunkschnittstelle verfügt, werden die Daten ausschließlich auf einen herstellereigenen Server übertragen.[11] Dritte sind für einen Zugang auf die Weiterleitung durch den Fahrzeughersteller angewiesen oder müssen sich auf einen (begrenzten) Datenzugang über die OBD II-Schnittstelle beschränken (sog. faktische Datenhoheit der Fahrzeughersteller). Der Fahrzeughersteller begründet seinen exklusiven Datenzugang mit unüberwindbaren Cyberrisiken, die entstehen, wenn eine Datenschnittstelle im Fahrzeug für Dritte geöffnet würde. Dritten könne mithin kein direkter Schnittstellenzugang zu Mobilitätsdaten gewährt werden.[12]

2. Fehlende Datenhoheit der Verbraucher

Gemäß Werkskonfiguration und aufgrund fehlender Schnittstellen sehen vernetzte Fahrzeuge auch für den Fahrzeugnutzer (i. d. R. ein Verbraucher) selbst keinen Zugriff auf die im Fahrzeug generierte Daten vor. Neben der fehlenden Schnittstelle wiegt zudem schwer, dass für den durchschnittlichen Fahrzeugnutzer nicht ersichtlich ist, welche Daten überhaupt durch das Fahrzeug generiert, im Fahrzeug gespeichert oder extern übermittelt werden. Insoweit besteht für den Fahrzeugnutzer keine Transparenz. Dies führt zu Folgeproblemen, soweit es z. B. um die Wahrnehmung der eigenen Datenschutzrechte geht.[13]

---

[11] Vgl. zuletzt VDA in seinem Positionspapier „ADAXO: Automotive Data Access – Extended and Open - VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten“, vom 12.01.2022, S. 10.

[12] Derweil geht ein überwiegender Teil der Studien und Stellungnahmen, die sich mit dem Zugang zu Fahrzeugdaten beschäftigen, davon aus, dass bestehende Cyberrisiken überwunden werden könnten, vgl. etwa FIGIEFA et al. „Secure On-board Telematics Platform Approach, Januar 2021; Europäische Kommission in Access to In-vehicle data and Resources, 2017, S. 12.

[13] Vgl. zu den datenschutzrechtlichen Herausforderungen unter C.III.

Ein zweckmäßiger und durchsetzbarer Anspruch auf Datenzugang und/oder Datenweitergabe zugunsten des Fahrzeugnutzers lässt sich nach aktuellem Stand auch nicht aus gesetzlichen Vorschriften herleiten. Ansprüche aus dem Sachenrecht sind praxistauglich kaum begründbar. Insbesondere besteht nach der h. M. an Daten kein Eigentum nach § 903 BGB, da es sich bei Daten nicht um Sachen i. S. v. § 90 BGB handelt.[14] Die konsequente Anwendung von Datenschutzrecht führt gegenüber der verantwortlichen Stelle zu Abwehrrechten.[15] Positive Verfügungsrechte (wie etwa die Ermöglichung des Zugangs) an Daten dürften bei Beachtung des „Volkszählungsurteils" des BVerfG aus dem Datenschutzrecht als solches jedoch nicht ableitbar sein.[16] Über Art. 20 DSGVO besteht nunmehr eine Möglichkeit zugunsten des Betroffenen, „seine" bei der verantwortlichen Stelle (hier: der Fahrzeughersteller) gespeicherten Daten an eine dritte Stelle portieren zu lassen. Der Anspruch aus Art. 20 DSGVO ist in der Praxis aber noch weitestgehend unerprobt. Insoweit soll an dieser Stelle nicht ausgeschlossen werden, dass die Vorschrift gewissen Datenzugangsbegehren abhelfen kann. Soweit jedoch, z. B. zur Umsetzung eines bestimmten digitalen datenbasierten Geschäftsmodells, ein wiederholter Datenzugang in (sehr) kurzen Intervallen benötigt wird, dürfte die Berufung auf Art. 20 DSGVO als alleinige Anspruchsgrundlage unzureichend bleiben.[17]

3. Beschränkter Datenzugang für Dritte

Dritte können, in Entsprechung zum Fahrzeugnutzer, mangels Schnittstelle nicht selbst unmittelbar auf Mobilitätsdaten im Fahrzeug zugreifen. In Betracht kommt die Nutzung der OBD-II Schnittstelle, über die durch den Anschluss sog. Dongles gewisse Daten ausgelesen werden können. Mittels im Dongle installierter SIM-Karte oder durch Verbindung mit dem Smartphone können die verfügbaren Daten dann auch an Dritte übermittelt werden. Im Vergleich zur Gesamtheit der im Fahrzeug generierten Daten sind die über die OBD-II-Schnittstelle verfügbaren Daten jedoch sehr begrenzt.[18] Die OBD-II-Schnittstelle dürfte demnach – verglichen mit den Möglichkeiten des Fahrzeughersteller – keinen gleichwertigen Datenzugang bieten.

Für Dritte kommt ein Zugang zu Mobilitätsdaten direkt beim Fahrzeughersteller auf vertraglicher Grundlage nur in Betracht, soweit dies von dem jeweiligen Fahrzeughersteller angeboten

[14] Vgl. bereits Hornung/Goeble in CR 2015, 265, 268.

[15] Siehe hierzu ausführlicher unter III.

[16] Gemäß dem BVerfG besteht kein „Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über seine Daten", vgl. Urteil vom 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

[17] Vgl. zu den Grenzen von Art. 20 DSGVO im Hinblick auf den Zugang zu Mobilitätsdaten Klink-Straub/Straub, in: ZD 2018, S. 459; entsprechend Reiter in DAR, 2022, 122, 123.

[18] Überdies besteht bei den Fahrzeugherstellern die Tendenz, die über die OBD-II-Schnittstelle verfügbaren Informationen auf das gesetzliche Minimum zu beschränken, vgl. mit diesem Hinweis bereits Hoegaerts/Schönenberger in: The automotive digital transformation and the economic impacts of existing data access models, 2019, S. 42

wird. Unter der Bezeichnung „NEVADA-Share & Secure“ hatte der Verband der Automobilindustrie e.V. (VDA) bereits im Jahre 2017 sein Konzept für einen Datenzugang zugunsten Dritter vorgestellt. Mit dem Nachfolge-Konzept ADAXO[19] hat der VDA Ende 2021 das NEVADA-Konzept konkretisiert. Beide Konzepte, deren Umsetzung für die Fahrzeughersteller freiwillig bleibt, haben gemein, dass eine Weiterleitung von Daten an Dritte über den Fahrzeughersteller erfolgen soll. Im Falle einer privatwirtschaftlichen Datenanfrage werden vertragliche Konditionen zur Ausgestaltung des Datenzugangs von jedem Fahrzeughersteller nach eigenem Ermessen gestellt. Die Fahrzeughersteller entscheiden mithin über Qualität (z. B. Zeitpunkt der Datenweitergabe und Datenformat), Quantität (z. B. Arten von Fahrzeugdaten, einzeln oder nur im Paket) und Preis (z. B. Höhe, ggf. Rabatte) der Daten. Auch soweit sich ein Fahrzeughersteller dafür entscheidet, das ADAXO-Konzept umzusetzen, bleibt es dabei, dass die im Fahrzeug generierten Daten ausnahmslos zunächst auf den jeweiligen Herstellerserver übertragen werden.[20] Somit verbleibt die faktische Datenhoheit beim Fahrzeughersteller. Entsprechend kritisch wurde das ADAXO-Konzept seitens der Branchenverbände aufgefasst.[21] Gegenüber den Fahrzeugherstellern besteht der Vorwurf, dass sie nicht ausreichend transparent offenlegen, welche Arten von Daten im Fahrzeug tatsächlich anfallen und demnach zur Verfügung stehen könnten. Die Fahrzeughersteller selbst hätten, verglichen mit den über das ADAXO-Konzept zur Verfügung stehenden Daten, Zugriff auf einen deutlich größeren Datenpool.

Fahrzeughersteller haben gemäß Art. 61 Abs. 1 i.V.m. Anhang X der Verordnung (EG) Nr. 2018/858 unabhängigen Wirtschaftsakteuren[22] (wie z. B. freie Reparatur- und Wartungsbetriebe) uneingeschränkten, standardisierten und diskriminierungsfreien Zugang insbesondere zu Fahrzeug-OBD-Informationen[23] sowie zu Reparatur- und Wartungsinformationen[24] zu gewähren. Allerdings sind die verfügbaren Daten per gesetzlicher Definition beschränkt.[25] Sodann normiert die Verordnung nicht ohne Weiteres einen Datenzugang per Mobilfunkschnittstelle in kurzen Intervallen oder gar in Echtzeit, wobei es hierauf für die Umsetzung datenbasierter Geschäftsmodelle regelmäßig maßgeblich ankommen kann. Die Verordnung zielt im Kern darauf ab, z. B. freien Werkstätten den Zugang zu Reparatur- und Wartungsmärkten für

[19] ADAXO = Automotive Data Access – Extended and Open.

[20] Vgl. VDA in seinem Positionspapier „ADAXO: Automotive Data Access – Extended and Open - VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten“, vom 12.01.2022, S. 10.

[21] Vgl. das Positionspapier des ZDK/ADAC/GDV et al. „Gleichberechtigter Zugang zum vernetzten Fahrzeug – Mobilitätsbranche fordert sektorspezifische Regelung“, vom 20.01.2022.

[22] Vgl. die Legaldefinition in Art. 3 Nr. 45 der Verordnung (EG) Nr. 2018/858.

[23] Vgl. die Legaldefinition in Art. 3 Nr. 49 der Verordnung (EG) Nr. 2018/858.

[24] Vgl. die Legaldefinition in Art. 3 Nr. 48 der Verordnung (EG) Nr. 2018/858.

[25] Eine Konkretisierung, welche Einzeldaten unter „Fahrzeugreparatur- und –Wartungsinformationen“ sowie „Fahrzeug-OBD-Informationen“ fallen, enthält Anhang X zur Verordnung (EG) Nr. 2018/858.

Fahrzeuge zu ermöglichen, indem den Werkstätten sämtliche Informationen überlassen werden, die für die Wartung oder Reparatur eines Fahrzeugs erforderlich sind. Demgegenüber ist ein Datenzugang für die Umsetzung digitaler, datenbasierter Geschäftsmodelle in dem Regelungswerk nicht angelegt. Für sonstige Dritte, die in der Verordnung (EG) Nr. 2018/858 nicht als Anspruchsberechtigte geführt sind, stellt dieser Datenzugangsanspruch ohne keine Lösungsoption dar.

Im Zuge des GWB-Digitalisierungsgesetzes[26] wurde der Missbrauchstatbestand gemäß § 19 Abs. 2 Nr. 4 GWB in Bezug auf den Zugang zu wettbewerbsrelevanten Daten ergänzt. § 19 Abs. 2 Nr. 4 GWB geht von dem Missbrauch einer marktbeherrschenden Stellung eines Unternehmens nunmehr insbesondere auch dann aus, wenn sich das marktbeherrschende Unternehmen weigert, einem dritten Unternehmen Datenzugang zu gewähren, die Gewährung des Datenzugangs allerdings für eine Tätigkeit auf einem vor- oder nachgelagerten Markt objektiv notwendig ist und die Weigerung des Zugangs den wirksamen Wettbewerb auf diesem Markt auszuschalten droht. Die (vertragliche) Überlassung der Daten bewirkt sodann, zur Erfüllung des Anspruchs aus § 33 Abs. 1 GWB, die Auflösung der Missbrauchshandlung. Insoweit besteht ein Kontrahierungszwang. Fraglich ist jedoch, ob und inwieweit einzelne Fahrzeughersteller als marktbeherrschende Unternehmen nach § 18 Abs. 1 GWB zu qualifizieren sind. Sodann würde sich die Frage anschließen, ob und inwieweit die etwaige Verweigerung des Zugangs zu Mobilitätsdaten gegenüber dritten Servicedienstleistern eine Missbrauchshandlung i.S.v. § 19 Abs. 2 Nr. 4 GWB darstellt. Gemäß aktuellem Stand ist die Begründung des Zugangsanspruchs aus § 19 Abs. 2 Nr. 4 GWB generell und so auch im Hinblick auf den Zugang zu Mobilitätsdaten beim Fahrzeughersteller noch mit erheblichen Unsicherheiten behaftet. Entsprechende Rechtsprechung oder Entscheidungen der zuständigen Behörde in Bezug auf den Zugang zu Daten liegen noch nicht vor. Der (neu gefasste) § 19 Abs. 2 Nr. 4 GWB wird sich somit in der Praxis zunächst erst noch beweisen müssen.[27]

III. Datenschutzrechtliche Herausforderungen

1. Mobilitätsdaten als personenbezogene Daten

Gemessen an der Legaldefinition in Art. 4 Nr. 1 Hs. 1 DSGVO, handelt es sich nach h. M. bei Mobilitätsdaten regelmäßig um „personenbezogene Daten“. Denn bei der Übertragung von Daten per Mobilfunkschnittstelle oder durch eine Verknüpfung der Daten mit der Fahrzeugidentifikationsnummer (FIN) oder dem Kfz-Kennzeichen wird regelmäßig eine Verknüpfung

[26] Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen vom 18.01.2021 (BGBl. I S. 2).

[27] Vgl. zum Datenzugangsanspruch nach § 19 Abs. 2 Nr. 4 GWB Huerkamp/Nuys in: NZKart 2021, 327; Weber in: WRP 2020, 559; mit Bezug auf Fahrzeugdaten Schenkel in „Neuer kartellrechtlicher Datenzugangsanspruch am Beispiel von Fahrzeugdaten“, Festschrift für Dr.-Ing. E.h. Jürgen Bönninger, S. 227ff.

zum individuellen Fahrzeug und damit zu dessen Fahrer/Halter hergestellt.[28] Dies führt zu einer konsequenten Anwendung von Datenschutzrecht zugunsten des datenschutzrechtlich Betroffenen gegenüber der verantwortlichen Stelle, die Mobilitätsdaten verarbeitet. Bei der Bestimmung, wer datenschutzrechtlich betroffen ist, kommt es letztlich nicht entscheidend darauf an, wer die Mobilitätsdaten erzeugt, sondern auf welche Person die verantwortliche Stelle die Daten beziehen kann.[29] Verantwortliche Stelle ist nach Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde oder Einrichtung, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Vorliegend kommen als verantwortliche Stelle in erster Linie die Fahrzeughersteller sowie auch alle sonstigen Dritten in Betracht, die Mobilitätsdaten z. B. durch Speicherung, Analysen oder Weiterleitung verarbeiten.

2. Unscharfe Rechtfertigungstatbestände zur Datenverarbeitung

Im Datenschutzrecht gilt das Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO), d.h. die Verarbeitung von Daten ist nur dann erlaubt, wenn das Gesetz eine solche ausdrücklich zulässt. Fehlt es an einer Rechtsgrundlage zur Datenverarbeitung, kann der Betroffene insbesondere die Löschung der Daten verlangen (Art. 17 DSGVO), was sich für die verantwortliche Stelle nachteilig auf die wirtschaftlichen Nutzungsmöglichkeiten auswirkt.

In Betracht kommt eine Datenverarbeitung zunächst zur Vertragserfüllung (Art. 6 Abs. 1 Satz 1 Lit. b DSGVO), zur Erfüllung einer gesetzlichen Pflicht (Art. 6 Abs. 1 Satz 1 Lit. c DSGVO) oder zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 Satz 1 Lit. f DSGVO) der verantwortlichen Stelle. Soweit keiner der genannten Rechtfertigungsgründe vorliegt, kann eine Datenverarbeitung auf der Grundlage einer ausdrücklichen Einwilligung des Betroffenen gerechtfertigt sein (Art. 6 Abs. 1 Satz 1 Lit. a DSGVO). Vorgenannte Rechtfertigungstatbestände haben ihre Grenzen. In Diskussion steht, inwieweit z. B. die Fahrzeughersteller als verantwortliche Stellen diese Grenzen überschreiten.[30]

a. Vertragserfüllung

So darf eine Verarbeitung personenbezogener Daten zur Vertragserfüllung nur insoweit erfolgen, als eine solche erforderlich ist, d. h. wenn ein unmittelbarer sachlicher Zusammenhang

[28] Vgl. nur die Gemeinsame Erklärung zu den datenschutzrechtlichen Aspekten bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie/VDA, 2016.

[29] Vgl. zum datenschutzrechtlich „Betroffenen“ im vernetzten Fahrzeug z. B. Störing/Eilers, in: PinG 2015, 118, 120.

[30] Vgl. insb. zu den Grenzen der Vertragsdatenverarbeitung und Einwilligung in Bezug auf Fahrzeugdaten Brink/Hertfelder, in: Einwilligung und Vertragsdatenverarbeitung, erschienen in: Roßnagel/Hornung (Hrsg.), Grundrechtsschutz im Smart Car, 2019, S. 75ff.

zwischen dem Vertragszweck und der Datenverarbeitung besteht.[31] Soweit also eine Datenverarbeitung zur Erbringung der vertraglichen Leistung gar nicht erforderlich ist, ist dieser Rechtfertigungsgrund nicht einschlägig. Dies dürfte regelmäßig für die Verarbeitung von Daten gelten, die zur Produktverbesserung oder Werbezwecken durchgeführt werden. Im Zeitpunkt des Fahrzeugkaufs schließt der Kunde regelmäßig nicht nur einen Kaufvertrag, sondern gleichzeitig womöglich eine Vereinbarung über datenbasierte Zusatzdienstleistungen mit dem Fahrzeughersteller selbst oder dritten Dienstleistern ab. Die Frage der Rechtfertigung zur Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 Lit. b DSGVO stellt sich dann für jedes einzelne Vertragsverhältnis. Dabei ist es problematisch, dass einzelne Dienste gegebenenfalls nur schwer voneinander abgegrenzt werden können und der Fahrzeugnutzer als betroffene Person kaum nachvollziehen kann, welche Daten denn nun für welchen Dienst tatsächlich erforderlich sind. Sodann besteht im Zusammenhang mit vernetzten Fahrzeugen die Problematik, dass ein Fahrzeug nicht nur von dem Vertragspartner der Kauf- und Dienstleistungsverträge genutzt wird (sog. Dual Use-Konstellationen). Soweit ein Dritter das Fahrzeug nutzt und die bei der Nutzung generierten Daten auf diesen Dritten beziehbar sind, dürfte eine Rechtfertigung über Art. 6 Abs. 1 Satz 1 Lit. b DSGVO bereits nicht mehr in Betracht kommen.

b. Wahrung berechtigter Interessen

Gemäß Art. 6 Abs. 1 Lit. f DSGVO ist eine Datenverarbeitung rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Einschränkend sind dabei im Rahmen einer Abwägung die Interessen des Betroffenen (Grundrechte und Grundfreiheiten) zu berücksichtigen. Was genau unter „berechtigten Interessen“ zu verstehen ist, bleibt derweil offen. In Betracht kommen sowohl wirtschaftliche und rechtliche als auch ideelle Interessen der verantwortlichen Stelle. Gemäß der Erwägungsgründe 47 und 49 DSGVO kann in der Datenverarbeitung zur Betrugsprävention, Direktwerbung oder zur Optimierung von IT-Systemen ein berechtigtes Interesse i.S. der Vorschrift liegen. Ob eine Rechtfertigung zur Datenverarbeitung nach Art. 6 Abs. 1 Lit. f DSGVO zu bejahen ist, hängt letztlich von der Abwägung mit den Interessen des Betroffenen ab. Insoweit zielt Art. 6 Abs. 1 Lit. f DSGVO auf einen Interessenausgleich zwischen verantwortlicher Stelle und Betroffenem ab.[32] Auch bei der Verarbeitung von Mobilitätsdaten kann ein berechtigtes Interesse der verantwortlichen Stelle eine Datenverarbeitung legitimieren. Der Tatbestand kommt insbesondere dann zum Tragen, wenn weder eine Vertragsdatenverarbeitung, eine gesetzliche Pflicht oder eine Einwilligung die Verarbeitung rechtfertigen. Denkbar ist eine Anwendung von Art. 6 Abs. 1 Lit. f DSGVO, wenn z. B. im Rahmen eines Pay-as-you-drive-Versicherungstarifs nicht der Vertragspartner, sondern ein Dritter das Fahrzeug nutzt. Ferner kann, soweit eine Interessenabwägung zugunsten von Fahrzeughersteller oder sonstiger verantwortlicher

[31] Vgl. Kühling/Buchner, DS-GVO BDSG, Kommentar, 3. Auflage 2020, Art. 6 DSGVO Rn. 32a m.w.N.

[32] Vgl. insoweit z. B. BGH, Beschluss v. 27. Juli 2020, Az. VI ZR 476/18, wo es um die Suchergebnisanzeige von Internet-Suchmaschinen ging.

Stellen ausgeht, Art. 6 Abs. 1 Lit. f DSGVO in Bezug auf Produktneuentwicklung, Produktbeobachtung, Produktneuentwicklung, Werbung oder sonstige interne Zwecke relevant sein. Gemäß Art. 13 Abs. 1 Lit. d bzw. Art. 14 Abs. 2 Lit. b DSGVO ist die verantwortliche Stelle verpflichtet, den Betroffenen über bestehende überwiegende Interessen zu informieren. Der Betroffene kann dann nach Art. 21 Abs. 1 S. 1 DSGVO der auf Art. 6 Abs. 1 Lit. f DSGVO gestützten Datenverarbeitung widersprechen. Entsprechende Bedeutung kommt den Informationspflichten gegenüber dem betroffenen Fahrzeugnutzer zu.

c. Einwilligung des Betroffenen

Soweit nicht bereits anderweitig die Datenverarbeitung legitimiert ist, kommt, eine Einwilligung des Betroffenen zur Rechtfertigung in Betracht (Art. 6 Abs. 1 Satz 1 Lit. a DSGVO). Der Betroffene kann also frei entscheiden, ob und wie seine Daten verarbeitet werden. Für eine Wirksame Einwilligung müssen die Voraussetzungen aus Art. 4 Nr. 11, Art. 7 und Art. 8 DSGVO vorliegen. Neben Fragen zu Zeitpunkt, Form und Transparenz[33] der Einwilligungserklärung sowie deren Widerrufbarkeit, ist maßgeblich, dass die Einwilligung freiwillig, informiert und zweckgebunden abgegeben wird.

Die Einwilligung gilt nur dann als **freiwillig** abgegeben, wenn der Betroffene eine echte oder freie Wahl hatte und somit in der Lage war, die Einwilligung zu verweigern oder zurückzuziehen, ohne dabei Nachteile zu erleiden.[34] „Nachteile“ i. d. S. können bei Überrumplung, einseitiger Beratung oder übermäßigen Anreizen anzunehmen sein.[35] Weiter kommt es bei der Frage der Freiwilligkeit darauf an, ob die Erfüllung eines Vertrags (z. B. über eine Dienstleistung) womöglich von der Einwilligung zu einer Datenverarbeitung abhängig gemacht wird, wobei die von der Einwilligung betroffenen Daten für die Erfüllung des Vertrags gar nicht erforderlich sind (sog. *Kopplungsverbot*, vgl. Art. 7 Abs. 4 DSGVO). Der Betroffene soll insoweit davor geschützt werden, dass er für ihn ggf. maßgebliche vertragliche Leistungen nur dann in Anspruch nehmen kann, wenn er gleichzeitig in eine sonstige Datenverarbeitung einwilligt. Die Wirksamkeit der Einwilligung kann mangels Freiwilligkeit auch dann in Frage stehen, wenn ein *Machtungleichgewicht* zwischen Betroffenem und verantwortlicher Stelle besteht, wobei ein solches Ungleichgewicht auch zwischen Unternehmern und Verbrauchern bestehen kann. Dies kann etwa der Fall sein, wenn die verantwortliche Stelle hinsichtlich einer Dienstleistung eine Monopolstellung hat oder der Verbraucher auf das Produkt angewiesen ist.[36]

---

[33] Transparenz nach Art. 7 Abs. 2 DSGVO, etwa durch gestalterische Hervorhebung und unmissverständlicher Sprache, vgl. Kühling/Buchner, DS-GVO BDSG, Kommentar, 3. Auflage 2020, Art. 7 DSGVO Rn. 25f.

[34] Vgl. Erwägungsgrund 42 DSGVO.

[35] Vgl. Wolff/Brink, BeckOK Datenschutzrecht, 37. Edition, 2021, Art. 7 Rn. 38.

[36] Vgl. Wolff/Brink, BeckOK Datenschutzrecht, 37. Edition, 2021, Art. 7 Rn. 50.

Die Einwilligung gilt nur dann als **informiert** abgegeben, wenn die betroffene Person die Tragweite der Einwilligung eindeutig und klar erkennen konnte. Dazu muss sie vorab über die verantwortliche Stelle, die Datenarten, die Verarbeitungsarten, die Verarbeitungszwecke und ggf. über Datenübermittlung an Dritte informiert werden. Bei der Prüfung von Umfang sowie Art und Weise der Informationserteilung sind das genutzte Kommunikationsmittel (z. B. Papier, Smartphone, Bildschirm im Fahrzeug) und seine Geeignetheit zu berücksichtigen. Derselbe Informationstext kann somit bezogen auf das eine Kommunikationsmittel gesetzeskonform sein, bezogen auf ein anderes Mittel möglicherweise aber nicht.[37]

Schließlich hängt die Wirksamkeit der Einwilligungserklärung von ihrer **Bestimmtheit und Zweckbindung** ab. Sämtliche Verarbeitungszwecke sind dem Betroffenen darzulegen, idealerweise in der Einwilligungsklausel selbst, damit es aus dessen Sicht zu keiner überraschenden Datennutzung kommt. Eine pauschale Einwilligung ohne Bezugnahme auf bestimmte Verarbeitungszwecke dürfte jedenfalls stets unwirksam sein.[38] Die genauen Mindestinhalte bzw. der Detaillierungsgrad der Einwilligungsklausel sind letztlich auch in Abhängigkeit der jeweiligen Anwendungssituation zu bestimmen.[39]

Auch im Hinblick auf die Verarbeitung von Mobilitätsdaten kann es zur Rechtfertigung auf eine wirksame Einwilligung ankommen. Dabei ist stets die Doppelrolle der Fahrzeughersteller als Hersteller/Verkäufer von Fahrzeugen zum einen und als Dienstleistungsanbieter zum anderen zu beachten. Insoweit kommen zunächst Rechtfertigungsgründe zur Datenverarbeitung nach Art. 6 Abs. 1 Lit. b, f DSGVO in Betracht. Dies gilt auch für sonstige Dienstleister, die mit dem betroffenen Fahrzeugnutzer einen Vertrag schließen. Bedarf es aber einer Einwilligung, sind im Hinblick auf die Datenverarbeitung rund um das vernetzte Fahrzeug die Wirksamkeitsvoraussetzungen zu hinterfragen. Ein Augenmerk ist dabei auf das Kopplungsverbot zu legen, etwa wenn die Abgabe einer Einwilligungserklärung Bedingung für den bloßen Fahrzeugverkauf ist. Auch ein Machtungleichgewicht zwischen Fahrzeughersteller und Kunde ist nicht ausgeschlossen, wenn z. B. der Fahrzeughersteller alleiniger Anbieter einer digitalen Dienstleistung ist. Besondere Anforderungen stellen sich im Hinblick auf Bestimmtheit, Zweckbindung und Informiertheit der Einwilligung in die Verarbeitung von Mobilitätsdaten. Für den durchschnittlichen Fahrzeugnutzer dürfte es kaum möglich sein, zwischen den verschiedenen Datenverarbeitungszwecken zu differenzieren oder aber nachzuvollziehen, welche Fahrzeugfunktionen oder digitalen Dienste von welchen Verarbeitungsvorgängen abhängen. Entsprechende Bedeutung kommt der Informationserteilung gegenüber dem Fahrzeugnutzer zu, die insbesondere darauf abgestimmt sein muss, ob der Fahrzeugnutzer die Informationen in Pa-

[37] Vgl. Schantz/Wolff, Neues Datenschutzrecht, 2017, S. 170.

[38] Vgl. Kühling/Buchner, DS-GVO BDSG, Kommentar, 3. Auflage 2020, Art. 7 DSGVO Rn. 76.

[39] Vgl. Kühling/Buchner, DS-GVO BDSG, Kommentar, 3. Auflage 2020, Art. 7 DSGVO Rn. 65.

pierform, über den Bildschirm im Fahrzeug (wobei es hier dann auch auf die jeweilige Bildschirmgröße abkommt) oder sein Smartphone erhält. Insoweit ist auch einer **Informationsüberlastung** des Betroffenen vorzubeugen, die den Betroffenen letztlich auch daran hindert, seine Datenschutzrechte angemessen ausüben zu können.[40] Herausfordernd sind zudem das Hinzutreten neuer Verarbeitungszwecke (im Hinblick derer eine separate Einwilligung erforderlich wäre), der Widerruf bestehender Einwilligungen sowie erneut der Umstand, dass Fahrzeuge von unterschiedlichen Personen genutzt werden, die allesamt betroffene Personen i. S. d. Datenschutzrechts sein können, nicht jedoch zwingend einzeln ihre Einwilligung zur Datenverarbeitung erklärt haben (sog. Dual Use-Konstellationen). Damit in der Praxis personenbezogene Mobilitätsdaten nicht auch ohne gesetzliche Rechtfertigung verarbeitet werden, ist demnach jedenfalls ein angemessenes Einwilligungsmanagement erforderlich. In Frage steht, ob ein solches seitens der Fahrzeughersteller selbst überhaupt zufriedenstellend angeboten werden kann. Vorliegend wird daher die Einführung eines verbrauchergerechten Personal Information Management Systems (PIMS) befürwortet, das auch ein solches Einwilligungsmanagement übernehmen kann.[41]

3. Durchsetzungsdefizite

Im Bereich des Datenschutzrechts besteht bekanntermaßen ein Durchsetzungsdefizit, das sowohl die behördliche als auch die private Rechtsdurchsetzung betrifft. Gemäß der DSGVO stehen einer betroffenen Person verschiedene Rechte zu, wie insbesondere das Recht auf Auskunft (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Löschung („Recht auf Vergessenwerden", Art. 17 DSGVO) sowie das Recht auf Datenübertragbarkeit (Art. 20 DSGVO). Soweit der Betroffene seine Rechte nicht wahrnimmt, ist dies zum einen dem Umstand geschuldet, dass er seine Rechte (infolge von formal/inhaltlich ungeeigneter Informationen) gar nicht kennt. Zum anderen stehen bei der Geltendmachung von Datenschutzrechten Aufwand und Nutzen aus Sicht des Betroffenen in einem ungünstigen Verhältnis. Ein strukturelles Ungleichgewicht zwischen dem Betroffenen als Verbraucher und der verantwortlichen Stelle als Unternehmen (ggf. ein Großkonzern), hohe Kosten und ein nicht unerheblicher Zeitfaktor halten den Betroffenen von einer Rechtsdurchsetzung ab. Auch im Hinblick auf dieses datenschutzrechtliche Durchsetzungsdefizit könnte ein Personal Information Management Systems (PIMS) aus Verbrauchersicht unterstützend wirken.[42]

---

[40] Dies gilt insbesondere auch im Hinblick auf die Datenschutzhinweise nach Art. 13, 14 DSGVO; vgl. zu dem Problem der datenschutzrechtlichen Informationsüberlastung Specht-Riemenschneider/Kerber in „Datentreuhänder – Ein problemlösungsorientierter Ansatz", 2022, S. 25ff.

[41] Vgl. zu dieser Problemstellung im Allgemeinen die Datenethikkommission der Bundesregierung in „Gutachten der Datenethikkommission", Oktober 2019, S. 133; siehe zudem ausführlicher unter D.I.4.b.

[42] Vgl. insoweit auch Specht-Riemenschneider/Kerber in „Datentreuhänder – Ein problemlösungsorientierter Ansatz", 2022, S. 29.

IV. Risiko eines Marktversagens zulasten der Verbraucher

Auf Märkten, die auf der Ressource Mobilitätsdaten basieren, stehen sich Fahrzeughersteller und mit ihnen verbundene Unternehmen auf der einen Seite und sonstige Dienstleister auf der anderen Seite als Wettbewerber gegenüber. Der Fahrzeughersteller ist dabei nicht nur als Fahrzeugproduzent und -verkäufer tätig, sondern bietet darüber hinaus auch Komplementärdienstleistungen an. Aus den aktuell beschränkten Möglichkeiten des Datenzugangs für den Fahrzeugnutzer sowie auf B2B-Ebene resultieren für nachgelagerte Märkte der Fahrzeugbranche (insbesondere Märkte für digitale, mobilitätsdatenbasierte Dienstleistungen) das Risiko einer Beschränkung der Wettbewerbsfunktionen. Dies birgt das Risiko für ein Marktversagen, was sich zum Nachteil der Fahrzeugnutzer (Verbraucher) auswirkt. Der beschränkte Datenzugang kann für dritte Dienstleister im Hinblick auf Märkte für digitale, mobilitätsdatenbasierte Komplementärdienstleistungen als **Eintrittsbarriere** wirken. Weniger Anbieter auf diesen Märkten können zu weniger Wettbewerb führen. Dies birgt die Gefahr, dass **keine neuen, innovativen Technologien** entwickelt werden. Die Auswahl der Endkunden aus neuen, innovativen digitalen Angeboten verschiedener Anbieter wird eingeschränkt **(Beschränkung der Wahlfreiheit des Verbrauchers)**.

Zwar können Mobilitätsdaten im Rahmen des ADAXO-Konzepts theoretisch auch von Dritten abgerufen werden. Durch die konkreten herstellerspezifischen Strukturen und vertraglichen Bedingungen im Hinblick auf Quantität, Preis und Qualität für einen Datenzugang ist es dem Fahrzeughersteller allerdings potenziell möglich, die Anzahl von Wettbewerbern für eine bestimmte mobilitätsdatenbasierte Dienstleistung zu begrenzen. Im Extremfall kann sogar, soweit die relevanten Daten nicht anderweitig beschafft werden können, der vollständige Ausschluss anderer Wettbewerber herbeigeführt werden. So ist es denkbar, dass relevante Daten von den Fahrzeugherstellern auch auf Nachfrage überhaupt nicht oder nur zu einem Preis angeboten werden, der im Hinblick auf bestimmte Geschäftsmodelle keine wirtschaftliche Nutzung zulässt. Auch das Datenformat und der Zeitpunkt der Datenlieferung können darüber entscheiden, ob die Daten für den avisierten Verwendungszweck überhaupt nutzbar sind. Scheitern Unternehmen bei der Datenbeschaffung, werden sie sich zwangläufig anderen Projekten zuwenden. Der Fahrzeughersteller bleibt als gegebenenfalls einziger Wettbewerber zurück.

Vorgenannte Wettbewerbsbeschränkungen können sich insbesondere negativ auf die Technologieentwicklung und die Wahlfreiheit von Verbrauchern auswirken. Eine Bündelung bestimmter Angebote bei nur wenigen marktmächtigen Unternehmen birgt die Gefahr, dass diese Unternehmen bewusst keine Neuentwicklungen vorantreiben, weil jede Neuentwicklung das bereits wirtschaftlich erfolgreiche Geschäftsmodell gefährden könnte. Aufgrund des fehlenden

Drucks seitens anderer Wettbewerber entscheiden sich Unternehmen womöglich für den Status quo und gegen Innovation.[43] Überdies beschränken weniger Anbieter auf bestimmten Märkten die Möglichkeiten zur Entwicklung innovativer Ideen und dort relevanter Geschäftsmodelle. Am Ende der Wertschöpfungskette steht der Fahrzeugnutzer als Verbraucher. Dieser möchte unter verschiedenen Angeboten das für ihn passendste und preiswerteste auswählen. Soweit jedoch lediglich digitale Angebote einiger weniger Dienstleister (darunter der Fahrzeughersteller) am Markt verfügbar sind, wird der Verbraucher in seiner Wahlfreiheit eingeschränkt.[44] Schließlich birgt ein beschränktes Angebot die Gefahr eines Konditionenmissbrauchs, indem für den Verbraucher nachteilige AGBs gestellt werden, die mangels alternativer Angebote vom Verbraucher akzeptiert werden.[45]

Der Staat kann sich dazu entschließen, in Märkte regulierend einzugreifen, wenn er die Risiken für ein Marktversagen erkennt und nicht davon auszugehen ist, dass sich die betreffenden Märkte von selbst regulieren. In Ansehung der politischen Auseinandersetzung mit dem Thema auf nationaler und europäischer Ebene scheint der Gesetzgeber die Gefahr eines Marktversagens immerhin erkannt zu haben. Auch insoweit soll das Modell eines „Mobilitätsdatenwächters“ einen Lösungsweg aufzeigen.

V. Systeme der Fahrzeughersteller

Für einen Überblick zum Status quo wurden die Systeme ausgewählter Fahrzeughersteller begutachtet. Dabei standen die folgenden Aspekte im Vordergrund:

- die Möglichkeiten zur Vornahme von Datenschutzeinstellungen im Fahrzeug;
- das verfügbare digitale, datenbasierte Dienstleistungsangebot;
- die Datenzugangsmöglichkeiten des Fahrzeugnutzers.

Datenzugangsmöglichkeiten zugunsten des Fahrzeugnutzers sind in den untersuchten Systemen nicht vorgesehen, das heißt es besteht für den Fahrzeugnutzer selbst keine Möglichkeit per Anzeige oder gar Download einen Überblick zu den verarbeiteten Mobilitätsdaten zu erhalten.

Mithilfe der herstellereigenen Systeme kann der Fahrzeugnutzer verschiedene datenbasierte Dienstleistungen nutzen. Allerdings werden die verfügbaren Dienste ganz überwiegend von dem jeweiligen Fahrzeughersteller selbst angeboten. Angebote von Drittanbietern finden in

[43] Vgl. zum Zusammenhang zwischen bestreitbaren Machtpositionen und innovativer Unternehmensführung bereits Schweitzer et al. in „Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen“, 2018, S. 28.

[44] Vgl. insoweit Martens/Mueller-Langer, in „Access to digital car data and competition in aftermarket maintenance service“, Journal of Competition Law & Economics, 2020, S. 130.

[45] Vgl. in diesem Zusammenhang das Verfahren des Bundeskartellamts gegen Facebook, Az. B6-22/16.

den Systemen indes kaum Berücksichtigung.[46] Dies überrascht auch insoweit nicht, als dass die Aktivitäten zur Entwicklung neuer innovativer Geschäftsmodelle durch Drittanbieter zurzeit noch verhalten sind. Dies dürfte zum einen an dem Umstand liegen, dass die Anzahl zugelassener vernetzter Fahrzeuge noch verhältnismäßig gering ist. Zum anderen entscheiden sich Unternehmen aber auch in Ansehung der komplizierten und uneinheitlichen Bedingungen eines Datenzugangs gegen entsprechende Investitionen.

Die Datenverarbeitungsvorgänge werden seitens der Fahrzeughersteller in umfangreichen Datenschutzhinweisen bereitgestellt. Dabei wird in erster Linie auf eine Verlinkung auf hinterlegte PDF-Dokumente zurückgegriffen, wobei die Dokumente mitunter nur tief im Menü zu finden sind und einen Umfang von rund 30 Seiten haben. Aus den Datenschutzhinweisen ergeben sich die verschiedenen, datenbasierten Dienstleistungen, die dort im Einzelnen mit Hinweis auf die Datenverarbeitungsvorgänge erläutert werden. Ob die Erläuterungen korrekt und vollständig sind, kann nicht überprüft werden, da die Verarbeitungsvorgänge insoweit nicht transparent nachvollziehbar sind. Die gewählte Darstellungsform der Datenschutzhinweise gegenüber dem Fahrzeugnutzer veranschaulicht noch einmal deutlich das oben angesprochene Risiko einer Informationsüberlastung des Betroffenen.[47] Nur in seltenen Fälle wird ein Fahrzeugnutzer die umfangreichen Datenschutzinformationen tatsächlich zur Kenntnis nehmen. Die Informationserteilung gegenüber den betroffenen Personen wirkt damit sehr starr und wird den flexiblen und dynamischen Datenverarbeitungsprozessen nur schwer gerecht werden können.

Für bestimmte Verarbeitungsvorgänge, wie z. B. zum Zwecke der Produktverbesserung, werden mitunter separate Einwilligungserklärungen angefragt, wobei die Informationen zur Einwilligung und die Einwilligungserklärung selbst erneut in PDF-Dokumenten hinterlegt sind. Ein anderer Anbieter verzichtet weitestgehend auf separate Einwilligungserklärungen und rechtfertigt stattdessen entsprechende Datenverarbeitungsvorgänge mit der Wahrung seiner Berechtigten Interessen gemäß Art. 6 Abs. 1 Lit. f DSGVO. Auch der Problematik „Mehrpersonenkonstellation“ wird in verschiedener Weise Rechnung, aber nicht ausreichend getragen. So werden die Fahrzeugnutzer z. B. lediglich darauf hingewiesen, dass sie selbst andere Fahrer vor Fahrtantritt über die Datenverarbeitung informieren müssen. Von anderer Stelle wird die Verarbeitung personenbezogener Daten anderer Fahrzeugnutzer erneut über Art. 6 Abs. 1 Lit. f DSGVO gerechtfertigt. Ein einheitliches datenschutzkonformes Vorgehen unter den verantwortlichen Stellen dürfte allerdings vorzugswürdig sein.

Die Durchsicht der Fahrzeugsysteme zeigt, dass den oben beschriebenen datenschutzrechtlichen Herausforderungen sowie auch den Risiken für ein Marktversagen weiterhin begegnet

[46] Die Ausnahme bilden hier die Entertainment- und Navigationsangebote großer Plattformbetreiber wie etwa Google oder Apple.

[47] Siehe hierzu unter C.III.2.c.

werden sollte. Insoweit schließen sich nunmehr Ausführungen zu einem Modell an, das einen datenschutzkonformen, treuhänderischen Datenzugang zu Mobilitätsdaten gewährleistet.

D. Mobilitätsdatenwächter: Modell für einen datenschutzkonformen, treuhänderischen Datenzugang

Den Risiken für ein Marktversagen sowie den datenschutzrechtlichen Defiziten beim Umgang mit personenbezogenen Mobilitätsdaten, wie in der Ausgangslage dargestellt, soll abgeholfen werden. Zu diesem Zweck wurde das Modell eines „Mobilitätsdatenwächters“ entwickelt, das zum einen den datenschutzkonformen Umgang mit Mobilitätsdaten gewährleistet und zum anderen einen fairen und diskriminierungsfreien Zugang zu Mobilitätsdaten ermöglicht.

Für die Darstellung des Modells wird zunächst eine Beschreibung der Struktur und des Rollenmodells zugrunde gelegt. Aus der Beschreibung gehen die beteiligten Stellen sowie ihre Funktionen und Aufgaben hervor (siehe unter I). Der Beschreibung des Rollenmodells folgen Ausführungen zur institutionellen Ausgestaltung, Qualitätssicherung und Finanzierung von „Mobilitätsdatenwächter“ und „Datentreuhänder“ an (siehe unter II). Das Kapitel schließt mit einer Darstellung der relevanten Use Cases, wobei den Use Cases strukturell jeweils das Rollenmodell des „Mobilitätsdatenwächters“ zugrunde gelegt wird (siehe unter III).

I. Struktur und Rollenmodell

Die Struktur und das Rollenmodell des „Mobilitätsdatenwächters“ zeigen die beteiligten Stellen sowie ihre Funktionen und Aufgaben auf (vgl. Abbildung 1). Beteiligte sind der „Fahrzeugnutzer“, „Dritte“, der „Datentreuhänder“ sowie der „Mobilitätsdatenwächter“. Der „Fahrzeugnutzer“ und „Dritte“ sind insoweit miteinander verbunden, als dass auf der einen Seite die „Dritten“ den Datenzugang begehren und auf der anderen Seite der „Fahrzeugnutzer“ möglicherweise gewillt ist, die sein Fahrzeug betreffenden Daten auch zur Verfügung zu stellen. Für diesen Fall muss dies dem Fahrzeugnutzer aber auch organisatorisch und technisch möglich sein. Um an dieser Stelle der exklusiven Datenhoheit der Fahrzeughersteller zu begegnen, soll anstelle des Fahrzeugherstellers einem „Datentreuhänder“ technisch der unmittelbare Datenzugang gewährt werden. Ein unmittelbarer Datenzugang des Fahrzeugherstellers, wie er aktuell besteht, soll nur für wettbewerblich nicht relevante Daten (z. B. rein technische Daten zur Produktsicherheit oder für elementare Fahrzeugfunktionen) in Betracht kommen. Der „Datentreuhänder“ empfängt die Daten aus dem Fahrzeug und kann diese, je nach Anwendungsfall und Bedarf, zwischenspeichern und an den Datenempfänger („Dritte“) weiterleiten. Über die Information, ob, inwieweit und an wen Mobilitätsdaten weitergegeben werden dürfen/sollen, verfügt nicht der „Datentreuhänder“, sondern der „Mobilitätsdatenwächter“. Dieser Betreibt ein Personal Information Management System (PIMS), in dem der Fahrzeugnutzer seine Datenverarbeitungspräferenzen hinterlegen und sämtliche Datenverarbeitungsvorgänge transparent nachverfolgen kann. Soweit nun ein „Dritter“ beim „Datentreuhänder“ um Überlassung bestimmter Mobilitätsdaten bittet, fragt der „Datentreuhänder“ beim „Mobilitätsdatenwächter“ nach, ob seitens des dispositionsbefugten „Fahrzeugnutzers“ eine Autorisierung vorliegt. Ist dies der Fall, führt der „Datentreuhänder“ den gewünschten Datentransfer durch. In Betracht kommt nicht nur die Datenübermittlung aus dem Fahrzeug in Richtung „Dritte“. Auch auf dem

umgekehrten Wege können – soweit auch hier eine Autorisierung vorliegt – über den „Datentreuhänder“ Informationen (z. B. auch Updates) in das Fahrzeug übermittelt werden.

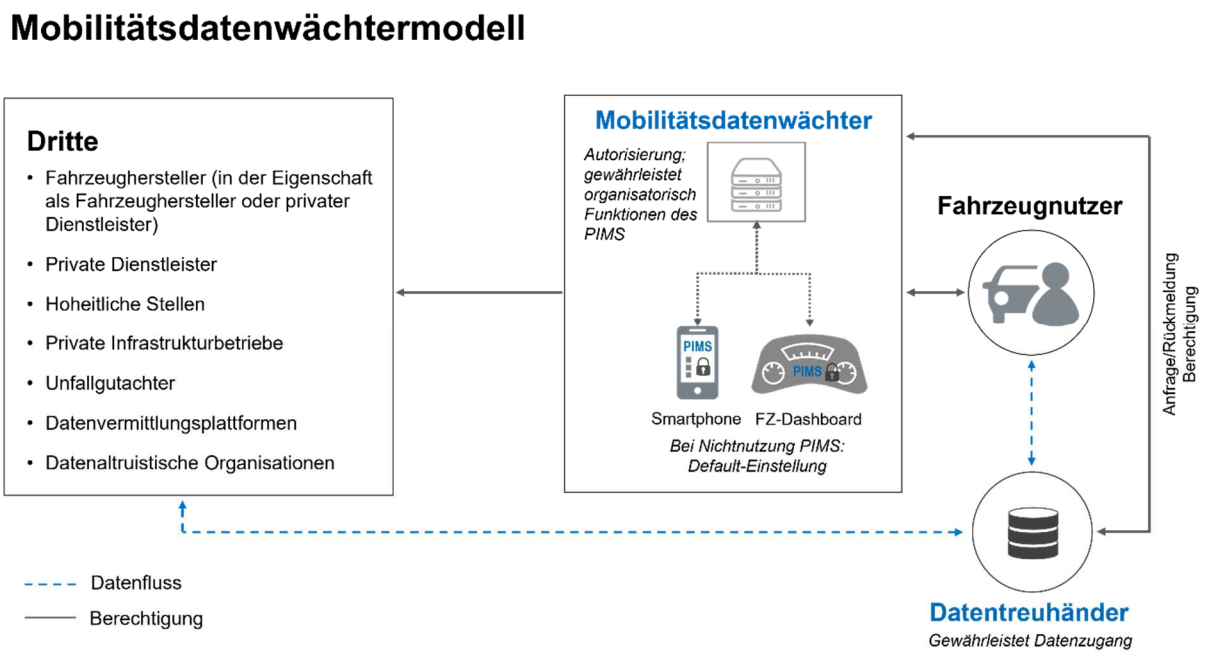

Abbildung 1: Struktur und Rollenmodell des „Mobilitätsdatenwächters“

Die vorangestellte Struktur sowie das Rollenmodell gemäß Abbildung 1 werden nachfolgend im Einzelnen näher erläutert. Dabei liegt der Schwerpunkt der Beschreibung zum einen auf der Tätigkeit des „Datentreuhänders“, der den Zugang zu Mobilitätsdaten in technischer Hinsicht gewährleistet. Zum anderen gilt die Aufmerksamkeit dem „Mobilitätsdatenwächter“ im engeren Sinne, der in Verbindung mit dem Datentreuhänder mithilfe eines Personal Information Management Systems (PIMS) den kontrollierten und transparenten Umgang mit Mobilitätsdaten gemäß den Vorgaben des Fahrzeugnutzers sicherstellen soll.

1. Fahrzeugnutzer

Im Zentrum des „Mobilitätsdatenwächters“ steht der „Fahrzeugnutzer“, denn die relevanten Mobilitätsdaten beziehen sich auf das Fahrzeug sowie in der Folge gegebenenfalls auf seine Person. In rechtlicher Hinsicht kann es einen Unterschied bedeuten, ob der Fahrzeugnutzer gleichzeitig oder alternativ Käufer, Eigentümer, Halter oder bloßer Fahrer bzw. Beifahrer des Fahrzeugs ist (wobei weiterhin in den vorliegenden Ausführungen gilt, dass, soweit nicht anders differenziert wird, einheitlich der Begriff des „Fahrzeugnutzers“ verwendet wird[48]). Für die Anwendung des Datenschutzrechts kommt es weniger auf die vorgenannte Einordnung, sondern in erster Linie darauf an, auf welche Person sich die Mobilitätsdaten eines Fahrzeugs beziehen. Insoweit ist es im Kern auch nicht entscheidend, wer das jeweilige Mobilitätsdatum

[48] Vgl. hierzu bereits Fn. 2.

z. B. durch Bewegung des Fahrzeugs erzeugt hat.[49] Der Fahrzeugnutzer möchte transparent darüber informiert bleiben sowie darüber disponieren können, ob, inwieweit, wann und durch welche Stelle die das Fahrzeug betreffenden Mobilitätsdaten verarbeitet werden. Dazu gehört zum einen, dass der Fahrzeugnutzer Dritte von einer Datenverarbeitung ausschließen kann. An dieser Stelle kommt es auf eine konsequente Anwendung von Datenschutzrecht an, die angesichts der oben genannten Herausforderungen[50] in Frage steht. Zum anderen muss es dem Fahrzeugnutzer möglich sein, aktiv und selbstbestimmt veranlassen zu können, dass die das Fahrzeug betreffenden Daten ausgewählten Dritten gegen Geld[51], gegen Dienstleistung[52] oder als Spende[53] zur Verfügung stehen können. Jedenfalls soweit die Daten keinen Personenbezug aufweisen oder es um die aktive, selbstbestimmte Datenweitergabe geht, besteht aus Sicht des Fahrzeugnutzers nach aktuellem Rechtsstand eine Regelungslücke. Entscheidend ist, wer faktisch den Datenzugang kontrolliert.[54] Diese Regelungslücke soll nunmehr durch die Einführung des „Mobilitätsdatenwächters“ geschlossen werden.

2. Dritte

Zu den „Dritten“ zählen im vorliegenden Kontext alle Stellen, die auf faktischer, vertraglicher oder gesetzlicher Grundlage Mobilitätsdaten verarbeiten. Zu nennen sind zunächst:

- Private Dienstleister für Mobilitätsdienstleistungen (im Hinblick auf mobilitätsdatenbasierte Geschäftsmodelle wie z. B.: Werkstatt, Pannenservice, Navigationssystemanbieter, Kfz-Versicherer);
- Hoheitliche Stellen;
- Infrastrukturbetriebe;
- Unfallgutachter;
- Datenvermittlungsplattformen;
- Datenaltruistische Organisationen.

Nach hiesigem Verständnis zählt zu den „Dritten“ auch der Fahrzeughersteller (OEM) selbst, der sich aktuell nur insoweit von den übrigen Dritten darin unterscheidet, dass er faktisch, d. h.

[49] Vgl. hierzu bereits unter C.2.1.

[50] Vgl. unter C.III.

[51] Schätzungen zum Wert der Daten eines Fahrzeugs sind nur schwer möglich. Konservativ wurden die Informationen mit einem Betrag von rund 350 Euro jährlich beziffert, vgl. Denker et al. für das Bundesministerium für Verkehr und digitale Infrastruktur in: „Eigentumsordnung für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive“, 2017, S. 73.

[52] Vgl. zu „Daten als Entgelt“ Zdanowiecki in DSRITB, 2018, 559.

[53] Z. B. als Datenspende für das Gemeinwohl.

[54] Nach aktuellem Stand der jeweilige Fahrzeughersteller, vgl. hierzu bereits unter C.II.2.

in technischer Hinsicht bereits unmittelbar auf die Daten im Fahrzeug zugreifen kann. Insbesondere unter Berücksichtigung wettbewerblicher Aspekte besteht jedoch keine Veranlassung, dem Fahrzeughersteller neben den sonstigen Dritten bei der Frage des Datenzugangs eine Sonderstellung einzuräumen. Der „Datentreuhänder", der gemäß dem hier aufgezeigten Modell den Zugang zu Fahrzeugdaten in technischer Hinsicht gewährleisten soll, wird seine Dienstleistung nur entgeltlich anbieten können.[55] Dies jedoch führt zu ungleichen Ausgangsbedingungen für den Aufbau datenbasierter Geschäftsmodelle, wenn der Fahrzeughersteller, der ein entsprechendes Geschäftsmodell anstrebt, die relevanten Daten ohne Zusatzkosten erhält. Für den Fahrzeughersteller und die sonstigen „Dritten" sollten daher beim Zugang zu Mobilitätsdaten grundsätzlich dieselben Bedingungen gelten. Ein unmittelbarer Datenzugang des Fahrzeugherstellers in der aktuellen technischen Ausgestaltung kann nur dann in Betracht kommen, wenn die betreffenden Daten im Verhältnis zu sonstigen „Dritten" wettbewerblich nicht relevant sind. Zu denken ist z. B. an Daten, die das Produkt „vernetztes Fahrzeug" als solches betreffen, wie etwa rein technische Daten zur Produktsicherheit oder zu Zwecken der Produktbeobachtung und Produktweiterentwicklung. Aber auch für solche Daten gilt: Zugunsten des Fahrzeugherstellers existiert dem Grunde nach kein Anspruch auf einen Zugang zu Mobilitätsdaten. Das Fahrzeug muss auch ohne Datenaustausch mit dem Fahrzeughersteller sicher bewegt werden können.[56] Im Übrigen obliegt dem Fahrzeugnutzer die Entscheidung, ob er im Hinblick auf bestimmte Daten einer Übertragung an den Fahrzeughersteller zustimmt.[57]

3. Datentreuhänder

a. Aufgaben

In Ansehung des exklusiven Datenzugangs der Fahrzeughersteller und der daraus resultierenden wettbewerblichen Gefahren, besteht die Aufgabe des „Datentreuhänders" darin, den allgemeinen Zugang zu Mobilitätsdaten in technischer Hinsicht zu gewährleisten. Mit dem Hinweis auf unüberwindbare Cyberrisiken lehnen die Fahrzeughersteller derzeit einen generellen Datenzugang zugunsten dritter Stellen ab.[58] Durch den Zugang über besondere treuhänderische Stellen, die alle IT-Sicherheitsanforderungen erfüllen, kann aber bestehenden Cyberrisiken begegnet werden. Die Einbindung eines Datentreuhänders zur Lösung der Frage „Zugang

[55] Vgl. hierzu auch unter D.I.3 und D.II.2

[56] Eine andere Frage ist, ob zur Gewährleistung erweiterter Fahrfunktionen das Fahrzeug mit dem Fahrzeughersteller online verbunden sein muss.

[57] Im Rahmen der Diskussion ist allerdings darauf zu achten, dass aufgrund zukünftiger Datenzugangsmodalitäten aus Sicht der Fahrzeughersteller nicht die Anreize für eine zukünftige Datengenerierung in Fahrzeugen verloren gehen. Indes ist davon auszugehen, dass vernetzte Fahrzeuge auch ohne einen exklusiven Datenzugang des Fahrzeugherstellers zukünftig Daten generieren werden.

[58] Siehe dazu bereits unter C.II.1.

zu Mobilitätsdaten“ wurde als ein mögliches Szenario bereits beschrieben[59] und entspricht insoweit dem Willen der deutschen Regierungsparteien.[60] Per gesetzlicher Regelung wären Fahrzeughersteller dazu zu verpflichten, ihre Fahrzeuge so auszustatten, dass denjenigen Stellen, welche die Rolle des „Datentreuhänders“ wahrnehmen, Zugang zum Fahrzeug gewährt werden muss.

Soweit datenschutzrechtlich zur Beachtung des Grundsatzes der Datenminimierung geboten (Art. 5 Abs. 1 Lit. c DSGVO) oder im Rahmen eines Use Cases ausdrücklich vorgesehen, dürfen personenbezogene Daten nur anonymisiert verarbeitet werden. Unter anonymisierten Daten sind Informationen zu verstehen, die sich von Anfang an oder nachträglich nicht auf eine natürliche Person beziehen lassen. Neben der Gewährleistung des Datenzugangs sollte es der „Datentreuhänder“ sein, der – soweit erforderlich – für den ordnungsgemäßen technischen Vorgang einer nachträglichen Anonymisierung Sorge trägt. Als neutrale Stelle ist der „Datentreuhänder“ für diese Aufgabe besonders geeignet, da er – anders als die datenempfangene Stelle – keine Eigeninteressen verfolgt, die den Anonymisierungsvorgang gefährden könnten.[61]

Nur soweit erforderlich und möglich, hält der „Datentreuhänder“ Mobilitätsdaten gespeichert auf einem Server vor. Ansonsten leitet der „Datentreuhänder“ die Daten nach dem Abruf aus dem Fahrzeug lediglich direkt an den berechtigten „Dritten“ weiter. Ebenfalls zur Förderung des Grundsatzes der Datenminimierung sollten Daten, soweit eine Datenverarbeitung (z. B. per App) auch direkt im Fahrzeug möglich ist, das Fahrzeug gar nicht erst verlassen.[62] Der „Datentreuhänder“ entscheidet zudem nicht selbst über das „Ob“ einer Datenweitergabe. Die Information, ob eine Autorisierung seitens des Fahrzeugnutzers oder eine sonstige gesetzliche Grundlage vorliegt, fragt der „Datentreuhänder“ beim „Mobilitätsdatenwächter“ ab.

---

[59] Vgl. zuletzt Specht-Riemenschneider/Kerber in „Datentreuhänder – Ein problemlösungsorientierter Ansatz“, 2022, S. 59ff.; im Hinblick auf die Wahrnehmung hoheitlicher Aufgaben das Papier der deutschen Prüforganisationen „Position zum Zugang zu Fahrzeugdaten über die Remote-Fahrzeugschnittstelle (Over-the-Air) für hoheitliche Aufgaben“, 29. März 2019, Punkt 2; Martens/Mueller-Langer in „Access to digital car data and competition in aftersales services“, 2018, S. 17f.

[60] Vgl. den Ampel-Koalitionsvertrag 2021-2025, S. 52.

[61] Zu den Schwierigkeiten einer Anonymisierung im Fahrzeug selbst oder einer Entfernung des Personenbezugs während der Datenübertragung vgl. Kumpf in „Smart Cars – eine datenschutzrechtliche Analyse“, 2017, S. 85.

[62] An dieser Stelle zeigen sich Überschneidungen mit der in der politischen Diskussion reklamierten fahrzeuginternen „Offenen Telematik-Plattform“ (OTP), vgl. Martens/Mueller-Langer in „Access to digital car data and competition in aftersales services“, 2018, S. 12f.

b. IT-Sicherheit

Ein „Datentreuhänder“, dem der Fahrzeughersteller im Rahmen des Mobilitätsdatenwächtermodells Zugang ins Fahrzeug zu gewähren hat, muss alle IT-Sicherheitsanforderungen erfüllen, die insbesondere zur Verhinderung von Hackerangriffen auf das Fahrzeug erforderlich sind. Dabei werden auch technische Vorgaben der Fahrzeughersteller zu beachten sein. Die Erfüllung der Sicherheitsanforderungen müssen seitens der Fahrzeughersteller geprüft werden. Soweit alle Voraussetzungen erfüllt sind, gibt der Fahrzeughersteller den Zugang frei. Zur Gewährleistung eines erfolgreichen Freigabeprozesses müssen die Anforderungen seitens der Fahrzeughersteller eindeutig und klar formuliert, zweckmäßig sowie verhältnismäßig sein.

c. Wettbewerbliche Aspekte

Die Einbindung des „Datentreuhänders“ in das Mobilitätsdatenwächtermodell dient der Vermeidung wettbewerblicher Gefahren, die sich letztlich auch nachteilig auf Verbraucher auswirken können. Durch die Einbindung des „Datentreuhänders“ verliert der Fahrzeughersteller seine exklusive Entscheidungshoheit über Quantität, Preis und Qualität der Daten. Dabei müsste jedoch technisch sichergestellt sein, dass es dem Fahrzeughersteller nicht möglich ist, den Datenfluss zwischen Fahrzeug und „Datentreuhänder“ zu beschränken. Zur Vermeidung, dass die Weiterleitung von Mobilitätsdaten erneut nur über eine (wenn auch neutrale) einzige Stelle erfolgt (hier nämlich der „Datentreuhänder“), wäre die Einrichtung bzw. Gründung mehrerer „Datentreuhänder“ erforderlich. Die verschiedenen „Datentreuhänder“ stehen dann untereinander in Wettbewerb. Fahrzeugnutzer bzw. Dritte können dann auf der Grundlage von Preis und Qualität der Leistung wählen, mithilfe welchen „Datentreuhänders“ die Datenübermittlung erfolgen soll. Schließlich hängen faire Wettbewerbsbedingungen auf mobilitätsdatenbasierten Anschlussmärkten davon ab, ob der Fahrzeughersteller, soweit es sich um wettbewerbsrelevante Daten handelt, seinen exklusiven direkten Datenzugang aufgeben muss und Zugang zu Mobilitätsdaten, wie andere Dritte, lediglich (kostenpflichtig) über den „Datentreuhänder“ erhält.

4. „Mobilitätsdatenwächter“

a. Autorisierungsstelle

In Entsprechung zur Darstellung der Aufgaben des „Datentreuhänders“[63] nimmt der „Mobilitätsdatenwächter“ die Funktion der Autorisierungsstelle wahr. Der „Datentreuhänder“ selbst entscheidet nicht über die Art oder den Umfang der Datenweiterleitung, sofern nicht der „Mobilitätsdatenwächter“ die Freigabe signalisiert hat. Hingegen hat der „Mobilitätsdatenwächter“ zu keinem Zeitpunkt physischen Zugriff auf die Daten. Die Aufgabentrennung zwischen „Datentreuhänder“ (Zugang zum Fahrzeug, Datenweiterleitung) und „Mobilitätsdatenwächter“ (Autorisierung) gewährleistet die Neutralität beim Umgang mit Mobilitätsdaten. Interessenkonflikte

[63] Vgl. unter D.I.3.a.

werden dadurch vermieden, dass derjenige, der technisch über einen Datenzugang verfügt, selbst nicht über Art und Umfang der Datenverarbeitung entscheidet und demjenigen, der zu Letzterem befugt ist, die Daten nicht zugänglich sind.

Der „Mobilitätsdatenwächter" autorisiert zum einen die Datenverarbeitung, wenn der Fahrzeugnutzer entsprechend eingewilligt hat. Zum anderen prüft der „Mobilitätsdatenwächter", ob die Voraussetzungen gesetzlicher Vorschriften erfüllt sind, die den Anspruch einer dritten Stelle (regelmäßig hoheitliche Stelle) auf einen Datenzugang (ohne Einwilligung) begründen.

Zur geordneten, transparenten, und informierten Erfassung der Nutzerpräferenzen betreibt der „Mobilitätsdatenwächter" ein Personal Information Management System (PIMS). Auch dadurch soll den datenschutzrechtlichen Herausforderungen, die sich beim Umgang mit Mobilitätsdaten stellen[64], begegnet werden.

b. Betrieb eines Personal Information Management Systems (PIMS)

(1) Definition und Funktionen

Personal Information Management Systeme (PIMS) sind technische Hilfsmittel, die Nutzern dabei helfen sollen, Datenverarbeitungen besser anweisen, kontrollieren und steuern zu können.[65] Vorgenannte Definition beschreibt Sinn und Zweck eines PIMS, gibt jedoch noch keinen Aufschluss über die konkreten Funktionen, die bereitgestellt werden sollten, um die Zielsetzung zu erreichen. Insoweit handelt es sich bei einem PIMS um kein fertiges oder starres System. Vielmehr sind zahlreiche Funktionen denkbar, deren Implementierung vom konkreten Anwendungsfall abhängt.[66] *Krämer* fasst die Funktionalitäten wie folgt zusammen:[67]

- Zentralisierte Ausübung von Datenschutzrechten: Insb. Einwilligungsmanagement zur Datenverarbeitung gegenüber unterschiedlichen datenverarbeitenden Instanzen.
- Datenmanagement: Persönlicher Datenspeicher, insb. in der Cloud, Zusammenführung verschiedener Datenquellen, Datenkonvertierung, Datentreuhänderschaft.
- Identitätsmanagement: Identifizierung des Nutzers bei verschiedenen Onlinedienste;

[64] Siehe hierzu bereits unter C.III.

[65] Vgl. entsprechender Definition auch Krämer in „Digitale Selbstbestimmung durch Personal Information Management Systems?", Januar 2022, S. 4; Stellungnahme des Verbraucherzentrale Bundesverband „Neue Datenintermediäre – Anforderungen des vzbv an Personal Information Management Systeme (PIMS) und Datentreuhänder", 12. September 2020, S. 6.

[66] Vgl. mit einem Überblick zu den möglichen Funktionen eines PIMS vgl. Poikola et al. „MyData – an introduction to human-centric use of personal data", 2020, S. 38ff.

[67] Vgl. in „Digitale Selbstbestimmung durch Personal Information Management Systems?", Januar 2022, S. 5.

- Transparenz und Nachvollziehbarkeit: Schaffung von Transparenz und Nachvollziehbarkeit aller datenschutzrechtlich relevanten (Verarbeitungs)Vorgänge (z. B. über einen Aktivitätenlog); soweit gewünscht, Funktionserweiterung auf nicht-personenbezogene Daten.
- Auswertung und Monetarisierung von Daten: Datenanalyse, Datenaufbereitung, Datenmonetarisierung.

Basisfunktionalitäten eines jeden PIMS dürften jedoch, insbesondere zur konsequenten Beachtung und Durchsetzung von Datenschutzrecht, die Integration eines Einwilligungsmanagements sowie die Gewährleistung von Transparenz und Nachvollziehbarkeit aller Datenverarbeitungsvorgänge (ggf. im Hinblick auf personenbezogene sowie auch auf nicht-personenbezogene Daten) sein. Indem die betroffenen Nutzer eines PIMS ihre digitalen Aktivitäten nachvollziehen und kontrollieren können, wird gleichzeitig unrechtmäßigen Datenverarbeitungen vorgebeugt. Dies stärkt das Vertrauen des Einzelnen in die Nutzung digitaler vernetzter Systeme, eine Voraussetzung, die auch für die Weiterentwicklung des Ökosystems „vernetztes Fahrzeug“ grundlegend ist.

(2) Voraussetzungen

Die erfolgreiche Implementierung eines PIMS setzt, neben Organisation und Finanzierung[68], standardisierte technische Voraussetzungen[69] sowie vor allem eine Kooperationspflicht der Datenverarbeiter mit dem PIMS voraus. Letztgenannter Punkt mündet in eine rechtliche Verpflichtung aller datenverarbeitenden Stellen, den betroffenen Personen z. B. die Vornahme der gewünschten Datendispositionen (Einwilligungsmanagement), die Kenntnisnahme datenschutzrechtlicher Informationen, die Nachvollziehbarkeit sämtlicher Verarbeitungsvorgänge oder die Wahrnehmung der sonstigen Datenschutzrechte über das PIMS zu ermöglichen.[70] Dem Datenverarbeiter ist es in der Folge verboten, mit der betreffenden Person am PIMS vorbei zu interagieren.[71] Die freiwillige Nutzung eines PIMS dürfte indes mit hoher Wahrscheinlichkeit wegen fehlender Akzeptanz auch auf Betroffenenseite zum Misserfolg führen. Datendispositionen, Datenschutzinformationen sowie Verarbeitungsvorgänge wären auch bei teilweiser Nutzung des PIMS weiterhin nicht zentralisiert zugänglich. Das Interesse der Nutzer, das PIMS (als ein weiteres System unter vielen) zu nutzen, ginge verloren.

---

[68] Siehe hierzu später unter D.II.

[69] Vgl. hierzu an dieser Stelle nur Specht-Riemenschneider/Kerber in „Datentreuhänder – Ein problemlösungsorientierter Ansatz“, 2022, S. 34.

[70] Vgl. mit entsprechender Darstellung die Datenethikkommission der Bundesregierung in „Gutachten der Datenethikkommission“, Oktober 2019, S. 134.

[71] Vgl. mit dieser Konsequenz auch Specht-Riemenschneider/Kerber in „Datentreuhänder – Ein problemlösungsorientierter Ansatz“, 2022, S. 33.

(3) Anforderungen in Bezug auf Mobilitätsdaten

Im Rahmen des Mobilitätsdatenwächtermodells geht es um die Einführung eines PIMS, das nicht allgemeingültig, sondern speziell im Hinblick auf die Verarbeitung von Mobilitätsdaten entwickelt und genutzt werden soll. In Entsprechung dazu sind passende, sektorspezifische Mindestfunktionalitäten des PIMS auszuwählen. In Anbetracht der datenschutzrechtlichen Herausforderungen, die sich bei der Verarbeitung von Mobilitätsdaten stellen, sowie unter Berücksichtigung der zugewiesenen Aufgaben des „Datentreuhänders“ kommen in erster Linie nachstehende PIMS-Funktionen in Betracht:

1. Ein wirksames und nutzerfreundliches Einwilligungsmanagement;
2. Eine transparente und nachvollziehbare Darstellung aller Verarbeitungsvorgänge;
3. Assistenz zur Durchsetzung von Datenschutzrechten.

In der nachfolgenden Übersicht wird, in Anknüpfung an die obigen Ausführungen unter C.III, dargestellt, welche der genannten PIMS-Funktionen den jeweiligen datenschutzrechtlichen Problemstellungen begegnen soll.

		MOBILITÄTSDATENSPEZIFISCHE HERAUSFORDERUNGEN BEI DER DATENVERARBEITUNG
PIMS FUNKTIONEN	**Einwilligungsmanagement**	• Überblick über bereits erteilte/widerrufene Einwilligungen oder eingelegte Widersprüche gegen Datenverarbeitungsvorgänge • Einhaltung der Wirksamkeitsvoraussetzungen datenschutzrechtlicher Einwilligungserklärungen, insb.: - *Freiwilligkeit:* Insb. Beachtung des Kopplungsverbots u. Verhinderung von Machtungleichgewichten. - *Informiertheit:* Vollständige Informationen zur Datenverarbeitung; adäquate Darstellung in Abhängig des genutzten Kommunikationsmittels (Papier, Smartphone, Fahrzeugdisplay usw.). - *Bestimmtheit und Zweckbindung:* Je Verarbeitungszweck ist eine separate Einwilligung erforderlich. • Mehrpersonenkonstellationen (Dual Use)
	Transparenz und Nachvollziehbarkeit von Verarbeitungsvorgängen	• Für den Fahrzeugnutzer muss nachvollziehbar sein, - welche Mobilitätsdaten, - von welcher Stelle, - zu welchem Zweck, - auf welcher gesetzlichen Grundlage verarbeitet werden. • Erteilung verständlicher Datenschutzinformationen (Art. 13, 14 DSGVO), angepasst an das

		(technische) Kommunikationsmittel (Papier, Smartphone, Fahrzeugdisplay usw.).
	Durchsetzung von Datenschutzrechten	• Ausgleich bestehender Durchsetzungsdefizite, insb. im Hinblick auf folgende datenschutzrechtlichen Ansprüche: - Recht auf Auskunft (Art. 15 DSGVO; ggf. bereits durch „Transparenz- und Nachvollziehbarkeitsfunktion“ erfüllt); - Recht auf Berichtung (Art. 16 DSGVO); - Recht auf Löschung („Recht auf Vergessenwerden“, Art. 17 DSGVO); - Recht auf Datenübertragbarkeit (Art. 20 DSGVO).

Ein großer Mehrwert des Einwilligungsmanagements besteht darin, dass der Betroffene einen Überblick über bereits erteilte oder bereits widerrufene Einwilligungen i.S.v. Art. 6 Abs. 1 Satz 1 Lit. a, Art. 7 DSGVO erhält. Gleichzeitig sollte sich das Management auch auf Widersprüche nach Art. 21 Abs. 1 S. 1 DSGVO im Hinblick auf die nach Art. 6 Abs. 1 Lit. f DSGVO gerechtfertigten Datenverarbeitungen beziehen. Bei der Gestaltung des PIMS sollte zudem schwerpunktmäßig darauf geachtet werden, dass durch standardisierte Darstellungen alle Wirksamkeitsvoraussetzungen für eine Einwilligung (insb. Freiwilligkeit, Informiertheit, Bestimmtheit und Zweckbindung) vorliegen. Soweit im PIMS keine Einstellungen vorgenommen werden, gelten die betroffenen-„freundlichsten“ Default-Einstellungen (insoweit wird dem datenschutzrechtlichen Grundsatz „Privacy by Default“ gemäß Art. 25 Abs. 2 DSGVO Rechnung getragen). Das Einwilligungsmanagement sollte sich auch auf nicht-personenbezogene Daten beziehen. Zwar betrifft dies nicht mehr die datenschutzrechtliche Ebene. Jedoch sollte bei der Gestaltung und der Einführung eines PIMS innerhalb des speziellen Kontextes „Mobilitätsdaten“ gleichzeitig dafür Sorge getragen werden, dass dem Fahrzeugnutzer, der häufig auch Eigentümer des Fahrzeugs ist, die vollständige Datenhoheit aller in seinem Fahrzeug generierten Daten übertragen wird.

Das Einwilligungsmanagement kann schließlich mit der weiteren PIMS-Funktion hinsichtlich Transparenz und Nachvollziehbarkeit von Verarbeitungsvorgängen verknüpft werden. Danach muss für den Fahrzeugnutzer jederzeit transparent nachvollziehbar sein, welche Mobilitätsdaten von welcher Stelle zu welchem Zweck auf welcher gesetzlichen Grundlage verarbeitet werden. Zur Erläuterung der Verarbeitungsvorgänge sollten im PIMS verständliche Datenschutzinformationen, angepasst an das (technische) Kommunikationsmittel (Papier, Smartphone, Fahrzeugdisplay usw.) abrufbar sein. Durch die Anforderung, dass jedem datenschutzrechtlich relevanten Verarbeitungsvorgang eine gesetzliche Grundlage zugeordnet sein muss, würde auch noch einmal ersichtlich, welche Verarbeitungsvorgänge von einer expliziten Einwilligung gedeckt sein sollen. Bestehende Diskrepanzen zwischen mithilfe des Einwilligungsmanagements erteilten Einwilligungen und tatsächlichen Verarbeitungsvorgängen, die auf einer Einwilligung beruhen sollen, würden (automatisiert) sichtbar.

Die Assistenz bei der Durchsetzung von datenschutzrechtlichen Ansprüchen (insb. Recht auf Auskunft, Recht auf Berichtung, Recht auf Löschung, Recht auf Datenübertragbarkeit) kann sich in einem ersten Schritt insbesondere auf die Einrichtung einer standardisierten Kommunikation für die Geltendmachung beziehen. So stellt es für Betroffene bereits eine erhebliche Erleichterung dar, wenn die Geltendmachung eines Rechts „per Knopfdruck" ausgelöst werden kann. Damit ist die erste Hürde genommen. Weitere Elemente, wie etwa beratende Dienstleistungselemente oder die Einrichtung einer speziellen Schlichtungsstelle, wären denkbare und insoweit wünschenswerte Ergänzungen.

Neben den passenden PIMS-Funktionen kommt es für den Erfolg des Systems maßgeblich auf eine nutzergerechte Bedienoberfläche an. Durch ein strukturiertes Menü, selbsterklärende (bzw. kurz erläuterte) Symbolleisten (z. B. Toolbars), Schaltflächen (z. B. Buttons), Schalter und Regler (z. B. Schieberegler) oder sonstige Auswahllisten muss es dem Nutzer z. B. ohne Weiteres möglich sein, seine bevorzugten Einstellungen vorzunehmen oder die gesuchten Informationen abzurufen. Dabei muss die Oberfläche neutral gestaltet sein, damit eine Systemnutzung ohne Beeinflussung durch die Interessen einer datenverarbeitenden Stelle (sog. „Dark Patterns") gewährleistet ist. Die Bedienung des PIMS sollte von verschiedener Stelle aus möglich sein. In Betracht kommt zunächst eine Bedienung im Fahrzeug selbst über das Fahrzeugdisplay (sog. „Daten-Cockpit"). Gleichzeitig sollte jedoch auch eine Bedienbarkeit über den PC oder das Smartphone ermöglicht werden. Die Bedienbarkeit über eine Smartphone App hätte im Rahmen einer erweiterten Funktionalität den Vorteil, dass die auf dem Smartphone gespeicherten Einstellungen in jedes (kompatible) vernetzte Fahrzeug mitgenommen werden können.[72] Das für den Nutzer fremde Fahrzeug kann sich dann mit dem Smartphone verbinden. Die PIMS-Einstellungen werden berücksichtigt. Auf diese Weise könnte auch dem Problem, dass ein Fahrzeug durch verschiedene datenschutzrechtlich betroffene Personen (d. h. Fahrer / Beifahrer / Halter / Käufer / Eigentümer) genutzt werden kann (Mehrpersonenkonstellationen), begegnet werden.

(4) Hilfsweise: Anpassung der fahrzeugherstellereigenen Systeme

Für den Fall, dass die Einrichtung des Mobilitätsdatenwächters nicht in der vorangestellten Ausgestaltung umgesetzt würde, kämen hilfsweise, jedenfalls zur Begegnung der datenschutzrechtlichen Herausforderungen, verbindliche Vorgaben zur Anpassung der herstellereigenen Systeme in Betracht. Auch in den verschiedenen Systemen könnte ein verbessertes Einwilligungsmanagement integriert werden. Durch eine nutzergerechte, strukturierte Bedienoberfläche können dem Nutzer datenschutzrechtliche Informationen leichter und transparenter zugänglich gemacht werden. Zweckmäßige Funktionen sollten ihn bei der Geltendmachung

[72] Vgl. mit diesem Ansatz bereits das Positionspapier des Verbraucherzentrale Bundesverband „Fahrerlos alle mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht", 12. Oktober 2021, S. 15.

seiner Datenschutzrechte unterstützen. Die Vorgaben würden daher im Kern auf dieselben Funktionalitäten abzielen, die auch für das beschriebene PIMS vorgesehen sind. Die verbindlichen Vorgaben gegenüber den Fahrzeugherstellern würden der konsequenten Einhaltung des Datenschutzrechts dienen und die generellen Regelungen der DSGVO mit Blick auf den speziellen Bereich der Mobilitätsdaten konkretisieren. Der Nachteil einer bloßen Anpassung der herstellereigenen Systeme liegt in der fehlenden Neutralität des Fahrzeugherstellers. Eine zuständige Behörde (d.h. in der Regel der jeweils für den Fahrzeughersteller örtlich zuständige Landesdatenschutzbeauftrage) sollte daher insoweit die vorschriftsmäßige Umsetzung durch die Fahrzeughersteller überwachen und sicherstellen.

II. Institutionelle Ausgestaltung, Qualitätssicherung und Finanzierung

Die konkreten Aufgaben des „Datentreuhänders“ und des „Mobilitätsdatenwächters“ werden aktuell noch von keiner Stelle wahrgenommen. Es stellt sich daher im Rahmen einer institutionellen Ausgestaltung, Qualitätssicherung und Finanzierung des Mobilitätsdatenwächtermodells die Frage, welche bestehenden oder neu zu schaffenden Organisationen die beschriebenen Aufgaben übernehmen könnten bzw. sollten. In Betracht kommen zunächst Unternehmen aus der Privatwirtschaft. Alternativ könnte sich der Staat dieser Aufgaben annehmen. Bei der Auswahl ist zu berücksichtigen, dass der Staat mit der Umsetzung des Mobilitätsdatenwächtermodells regulierend tätig wird, und zwar zum einen gegen ein Versagen mobilitätsdatenbasierter Märkte und zum anderen zur konsequenten Beachtung und Durchsetzung von Datenschutzrecht. Unter Beachtung des Grundsatzes der Marktfreiheit wird der Staat zur Vermeidung von Marktversagen nur soweit als nötig eingreifen, solange sich die Märkte im Übrigen von selbst regulieren. Vor allem muss der Staat bei seiner Regulierungstätigkeit das Verhältnismäßigkeitsprinzip (Art. 20 GG) beachten. Soweit bestehendes Regulierungsrecht nicht ausreicht, um die bezweckten Ziele zu erreichen, wird der Staat nur insoweit nachbessern, als dies zwingend erforderlich und angemessen ist.

1. Mobilitätsdatenwächter

Im vorliegenden Modell fungiert der „Mobilitätsdatenwächter“ als Autorisierungsstelle gegenüber dem „Datentreuhänder“. Für diese Aufgabe ist vor allem die Einrichtung von Schnittstellen erforderlich, damit „Mobilitätsdatenwächter“ und „Datentreuhänder“ miteinander kommunizieren können. Im Schwerpunkt betreibt der „Mobilitätsdatenwächter“ allerdings ein Personal Information Management System (PIMS), dessen Aufbau und Betrieb verglichen mit dem Autorisierungsprozess die deutlich umfangreichere Aufgabe darstellt. Maßgeblich muss sich die Auswahl einer passenden Institution zur Wahrnehmung der Aufgaben des „Mobilitätsdatenwächters“ also daran orientieren, wer zum Aufbau und Betrieb eines PIMS geeignet ist.

Zur Erbringung der Aufgaben des „Mobilitätsdatenwächters“ kommen dem Grunde nach sowohl private Unternehmen als auch staatliche Stellen in Betracht. Für ein privates Unternehmen spricht zunächst, dass der staatliche Eingriff weniger intensiv ausfällt und sich auf die

zwingende Einbindung eines „Mobilitätsdatenwächters“ beschränkt. Hierzu kommt, dass private Unternehmen grundsätzlich gute Investoren sind und das Potential haben, auf komplexen Märkten der Datenwirtschaft innovativ tätig zu sein. Gegen die Überlassung der Aufgaben an ein privates Unternehmen spricht allerdings die perspektivische Finanzierbarkeit, die zudem wirtschaftlich dem zwingenden Gebot der Vermeidung von Interessenkollisionen entgegenstehen könnte. Auch wenn PIMS bereits seit einigen Jahren als geeignetes Mittel zur Umsetzung von Datenschutzrecht angesehen werden, hat sich bislang kein wirtschaftlich tragfähiges Geschäftsmoll etablieren können.[73] Vorliegend sind es zunächst nur die Fahrzeughersteller und Dritte, die das spezielle mobilitätsdatenbasierte PIMS vorschalten müssten. Die Fahrzeugnutzer werden voraussichtlich nicht dazu bereit sein, für die Nutzung des PIMS ein Entgelt zu bezahlen. Aufgrund der verhältnismäßig geringen Anzahl von Fahrzeugherstellern und Dritten ist eine Finanzierung von dieser Seite aus mangels Skalierbarkeit kaum denkbar. Soweit ein „Datentreuhänder“ später die Autorisierung beim „Mobilitätsdatenwächter“ anfragt, könnte für diesen Vorgang ein Entgelt verlangt werden. Die potentielle Häufigkeit von Autorisierungsanfragen ließe wohl auch eine Skalierung zu. Bis es dazu kommt, bedürfte es allerdings einer nicht unerheblichen Vorfinanzierung, die private Investoren abschrecken könnte. Zwar wäre es denkbar, dem Finanzierungsproblem durch staatliche Subventionierung bereits anerkannter oder zertifizierter PIMS privater Betreiber zu begegnen.[74] Zu beachten ist jedoch, dass private Unternehmen in der Regel kein Interesse an Neutralität haben, sondern wirtschaftliche Eigeninteressen verfolgen, wohingegen der Staat Aufgaben ohne Gewinnerzielungsabsicht wahrnehmen kann. Allerdings soll gerade ein neutrales Auftreten gegenüber Fahrzeugnutzer, Fahrzeughersteller und sonstigen Dritten grundlegende Eigenschaft des „Mobilitätsdatenwächters“ sein. Durch die Neutralität soll insbesondere vermieden werden, dass die Nutzer des PIMS durch dessen Ausgestaltung unbewusst fremdbestimmt entscheiden (sog. „Dark Patterns“). Das PIMS muss ein Hilfsmittel sein, das ausschließlich die selbstbestimmte Entscheidungshoheit unterstützt.[75] Dies ist bei Unternehmen, die wirtschaftliche Eigeninteressen verfolgen, im Grundsatz nicht gewährleistet.

Aus der Sicht des Gesetzgebers erscheint es daher vertretbar, selbst hoheitlich tätig zu werden und nicht darauf zu vertrauen, dass die Privatwirtschaft den „Mobilitätsdatenwächter“ mit den gewünschten Funktionen bereitstellt. Will der Staat hoheitlich tätig werden, so hat er die Möglichkeiten, dies als Behörde oder im Wege mittelbarer Staatsverwaltung zu tun. Vorliegend würde sich die Gründung einer Gesellschaft im Eigentum des Bundes anbieten. Als sodann

[73] Vgl. Krämer in „Digitale Selbstbestimmung durch Personal Information Management Systems?“, Januar 2022, S. 16; bereits der Europäischer Datenschutzbeauftrage (EDSB), Stellungnahme 9/2016, 2016, S. 15.

[74] Vgl. mit diesem Ansatz Specht-Riemenschneider/Kerber in „Datentreuhänder – Ein problemlösungsorientierter Ansatz“, 2022, S. 41.

[75] Vgl. entsprechend die Datenethikkommission der Bundesregierung in „Gutachten der Datenethikkommission“, Oktober 2019, S. 133.

beliehene Stelle könnte die Gesellschaft die Aufgaben des „Mobilitätsdatenwächters“ wahrnehmen. Wegen des Betriebs eines PIMS und des datenschutzrechtlichen Schwerpunkts könnte die Rechts- und Fachaufsicht des Mobilitätsdatenwächters nach einer entsprechenden Gesetzesänderung zur Zuständigkeit beim Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) angesiedelt sein.[76]

Die Begründung des staatlichen „Mobilitätsdatenwächters“ schließt nicht aus, dass private Unternehmen parallel eine entsprechende Stelle gründen. Mehrere „Mobilitätsdatenwächter“ könnten in wettbewerblicher Hinsicht nebeneinander betrieben werden. Die Fahrzeughersteller könnten sich entscheiden, mit welchem Wächter sie zusammenarbeiten wollen. Allerdings sollten Zulassung und Betrieb weiterer „Mobilitätsdatenwächter“ zur Einhaltung der Qualitäts- und Neutralitätsstandards einem angemessenen Zertifizierungs- und Überwachungssystem unterworfen werden.[77]

2. Datentreuhänder

Für die Wahrnehmung der Aufgaben des „Datentreuhänders“ sind parallel zum „Mobilitätsdatenwächter“ entsprechende Überlegungen anzustellen. Im Vergleich zum Betrieb eines PIMS erscheint die private Finanzierung einer Unternehmung für den Betrieb eines Datentreuhänders realistischer. Private Plattformen für die Vermittlung von Mobilitätsdaten sind bereits am Markt tätig und könnten womöglich dies geforderten Aufgaben übernehmen. Jedoch ist auch Kern des hier dargestellten „Datentreuhänders“ seine neutrale Stellung. Es gilt zu vermeiden, dass ggf. anstelle der Fahrzeughersteller der „Datentreuhänder“ interessengeleitet technisch über den Datenzugang entscheidet. Es ist mithin zweifelhaft, ob in Ansehung der wettbewerblichen Ziele der Einführung eines „Datentreuhänders“ die Übertragung der Aufgabe auf eine private Stelle überhaupt geeignet ist. Vielmehr dürfte, wie beim „Mobilitätsdatenwächter“ der Fall, die Einbindung einer staatlichen Stelle erforderlich sein. Der „Datentreuhänder“ könnte ebenfalls als beliehene Stelle tätig werden. Die Aufsicht wäre durch das Bundesministerium für Verkehr und digitale Infrastruktur als oberste Bundesbehörde wahrzunehmen. Soweit zweckmäßig könnte die Aufsichtsbehörde ihre Aufgaben delegieren und ein spezielles Aufsichtsgremium einsetzen.

Auf lange Sicht betrachtet sollte auch der staatliche „Datentreuhänder“ die Aufgabe nicht exklusiv wahrnehmen. Wie auch für den „Mobilitätsdatenwächter“ dargestellt, stünde es privaten Unternehmen grundsätzlich frei, ebenfalls „Datentreuhänder“ im Rahmen des Mobilitätsdatenwächtermodells zu werden, wobei auch hier zur Einhaltung der Qualitätsstandards ein ange-

[76] Vgl. insoweit auch die Informationen des BfDI „Vernetzte Fahrzeuge – Datenschutz im Auto“, 2020.

[77] Vgl. mit dem dringenden Hinweis auf ein Zertifizierungs- und Überwachungssystem, gerade wenn ein PIMS an der Stelle der Betroffenen agieren, die Datenethikkommission der Bundesregierung in „Gutachten der Datenethikkommission“, Oktober 2019, S. 133.

messenes Zertifizierungs- und Überwachungssystem zu etablieren wäre. Mehrere „Datentreuhänder" könnten im gegenseitigen Wettbewerb nebeneinander betrieben werden. Die „Dritten" könnten wählen, mit welchem „Datentreuhänder" sie zusammenarbeiten wollen. Insoweit ist beim Aufbau von „Datentreuhänder" und „Mobilitätsdatenwächter" auf eine ausreichende Interoperabilität zwischen allen Systemen zu achten.

III. Use Cases

In den letzten Jahren haben sich bereits verschiedene Use Cases herausgebildet, die auf dem Zugang und der Nutzung von Mobilitätsdaten beruhen. Repräsentativ sollten nachfolgend fünf Use Cases aufgezeigt werden, welche die Interessen der Fahrzeughersteller, der Privatwirtschaft, des Gemeinwohls sowie von hoheitlichen Stellen betreffen.

1. „Pay-as-you-drive"

Die Versicherungsbranche ist ständig daran interessiert, Daten zu den versicherten Objekten oder Personen zu sammeln, um durch erweiterte Risikoanalysen eine genauere, für die Versichertengemeinschaft gerechtere Tarifierung vornehmen zu können. Im Bereich Kfz-Versicherung ist die Branche schon seit einigen Jahren darum bemüht, Zugang zu Mobilitätsdaten zu erhalten, um anhand dieser Daten ein neues Geschäftsmodell zu etablieren. Unter der Bezeichnung „Pay-as-you-drive-Tarif" (oder auch „Telematiktarif") wird Fahrzeughaltern das Angebot unterbreitet, dass bei der Berechnung der Höhe der Versicherungsprämie insbesondere auch die individuellen Fahrgewohnheiten einbezogen werden. Anhand der Fahrgewohnheiten kann der Versicherer das Risiko eines Versicherungsfalls genauer bewerten. Kriterien sind z. B. der persönliche Fahrstil (Kurvengeschwindigkeiten, Beachtung von Geschwindigkeitsbeschränkungen, Brems- und Beschleunigungsverhalten), die bevorzugten Routen (vornehmlich Stadt-, Überland- oder Autobahnfahrten) oder Fahrzeiten (Tag- oder Nachtfahrten). Die vorgenannte Art und Weise der Tarifierung wird den Kunden bereits angeboten.[78]

[78] Vgl. etwa entsprechende Angebote der Signal Iduna Gruppe (www.sijoux.de) oder der Generali Deutschland AG (www.generali.de/telematik).

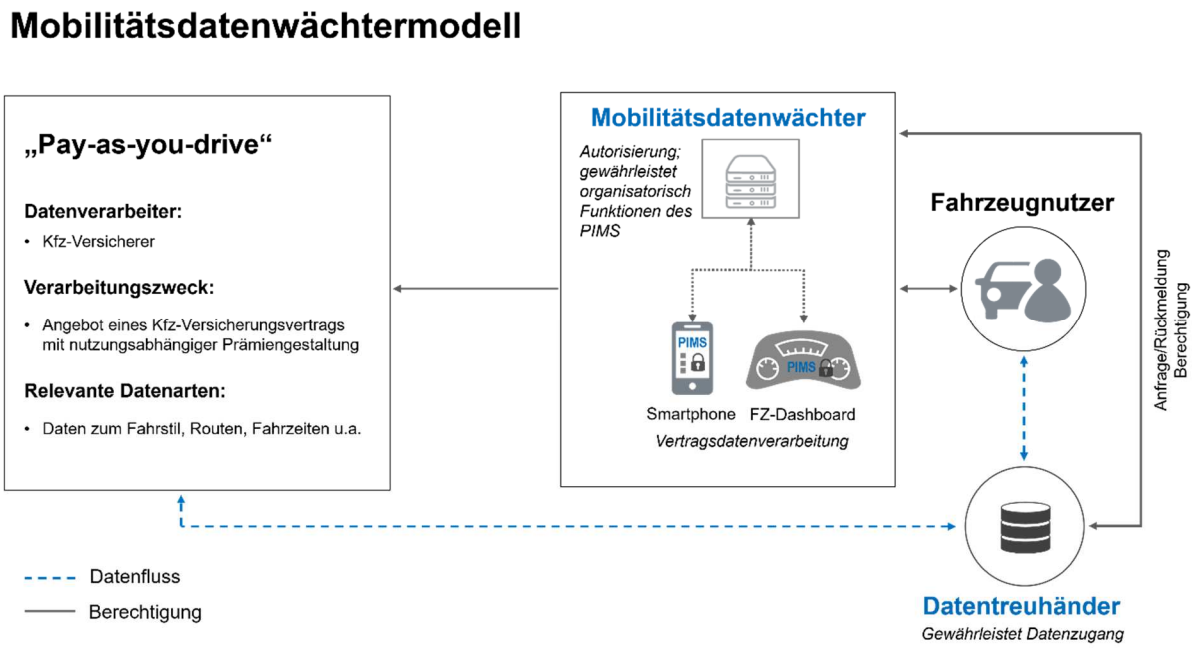

Abbildung 2: Mobilitätsdatenwächter Use Case "Pay-as-you-drive"

Abbildung 2 zeigt, wie sich das Geschäftsmodell „Pay-as-you-Drive“ in die Struktur des Mobilitätsdatenwächters einfügt. Da auch Kfz-Versicherer über keinen direkten Zugang zu Mobilitätsdaten im Fahrzeug verfügen, greifen die Versicherer aktuell entweder auf die Sensorik aus dem Smartphone des Versicherungsnehmers zurück oder nutzen die OBD-II-Schnittstelle. An diese Schnittstelle können mit eigenen Sensoren ausgestattete Zusatzgeräte (sog. Dongles) angeschlossen werden, die sodann alle über die Schnittstelle verfügbaren und für den Versicherer relevanten Daten per Mobilfunk übermitteln. Allerdings ist der Einsatz sog. Dongles ein Kostenfaktor, der eingepreist werden muss. Ansonsten muss der Versicherungsnehmer überhaupt dazu bereit sein, sein Smartphone (soweit er überhaupt eines besitzt) zu diesem Zweck verwenden zu wollen. Insoweit würde der „Datentreuhänder“ den Datenzugang verlässlich ermöglichen, und zwar zu denselben Konditionen wie denjenigen des Fahrzeugherstellers, der ggf. bereits selbst seinen Kunden im Zuge des Fahrzeugkaufs entsprechende Tarife anbietet. Im Hinblick auf die Datenverarbeitung muss der Kfz-Versicherer das geltende Datenschutzrecht beachten. Für die Rechtfertigung der Datenverarbeitung zur Tarifierung dient in erster Linie die vertragliche Vereinbarung (Kfz-Versicherungsvertrag) zwischen Versicherer und Versicherungsnehmer. Die Problematik einer Fahrzeug Mehrpersonennutzung stellt sich im Besonderen auch hier, da bei der Datenverarbeitung der Fokus auf Bewegungs- und Verhaltensdaten liegt. Wird das Fahrzeug nicht durch den Versicherungsnehmer (als Vertragspartner) selbst geführt, stellt sich für jeden sonstigen Fahrzeugnutzer erneut die Frage nach einer Rechtfertigung zur Datenverarbeitung. In der Praxis behilft sich die Branche mit einem Rückgriff auf Art. 6 Abs. 1 Lit. f DSGVO (Wahrung berechtigter Interessen), da aus Sicht des Versicherers eine verlässliche Vertragserfüllung nur dann möglich ist, wenn eine kontinuierliche Datenerfassung zur Fortbewegung des versicherten Fahrzeugs erfolgt. Soweit jedoch Art. 6

Abs. 1 Lit. f DSGVO nicht einschlägig wäre, bliebe nur der Weg über die Einwilligung.[79] Der Mobilitätsdatenwächter kann an dieser Stelle für Kontrolle und Transparenz sorgen.

2. Remote-Diagnose

Mithilfe der im Fahrzeug verbauten Sensoren und Steuergeräte können auf der Grundlage verschiedener Fahrzeugdaten wie z. B. zur Leistung, Verbrauch, Zustand, Fehlern, Störungen, Mängel, Verschleiß und sonstigen Schäden beim Betrieb des Fahrzeugs Unregelmäßigkeiten oder die Abnutzung von Bauteilen festgestellt werden. Die Sensoren überwachen permanent die Ordnungsgemäßheit der Fahrzeugsysteme. Fehlerzustände können erfasst und im Fehlerspeicher des Fahrzeugs abgelegt werden. In der analogen Welt erhielt zunächst nur der Fahrzeugnutzer Kenntnis über die Fehlermeldung, etwa durch Aktivierung der entsprechenden Warnlampen. In der Werkstatt, die sodann auf Initiative des Fahrzeugnutzers aufgesucht wurde, konnte dann mithilfe der OBD-II-Schnittstelle der Fehler ermittelt werden. Soweit nun im Fahrzeug eine Mobilfunkschnittstelle verbaut ist und die relevanten Daten an einen Dienstleister (freie Werkstatt, Pannendienst, Fahrzeughersteller) übertragen werden können, kann dieser Dienstleister (in Ergänzung zum internen Fahrzeugsystem) die Fahrzeugfunktionen überwachen und im Falle von Unregelmäßigkeit den Fahrzeugführer informieren oder sogar bereits Online-Hilfe anbieten. Die Information erfolgt idealerweise über das Fahrzeugdisplay und kann um Angebote für einen Wartungs- oder Reparaturtermin ergänzt werden.

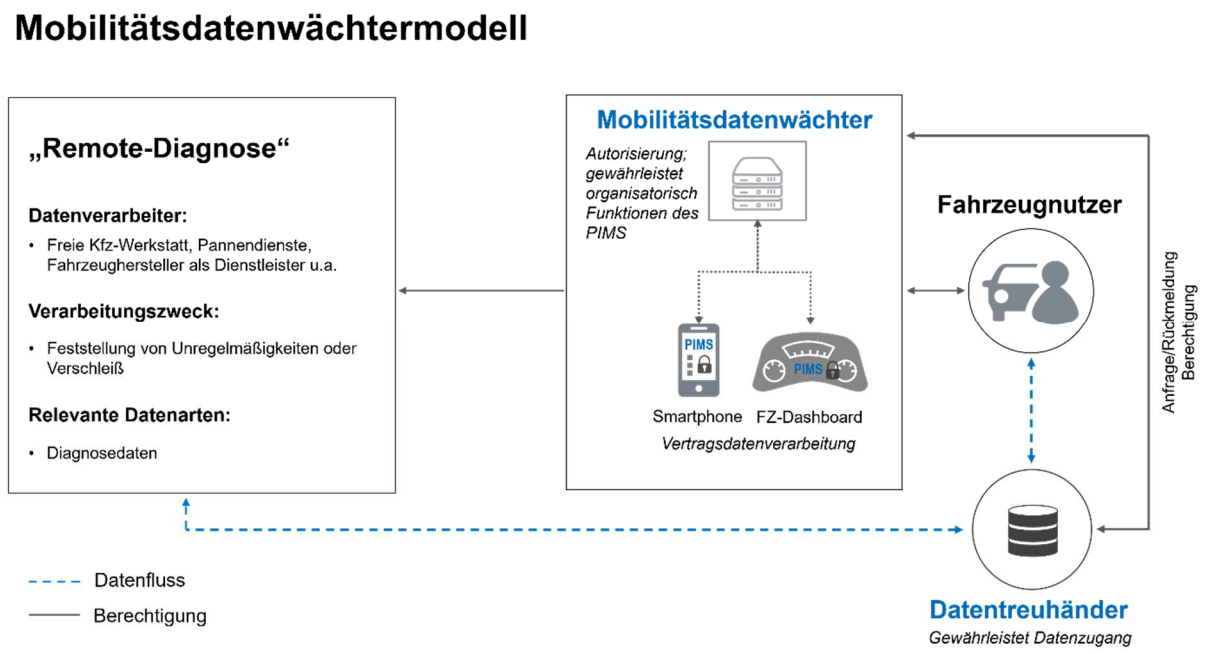

Abbildung 3: Mobilitätsdatenwächter Use Case "Remote-Diagnose"

[79] Vgl. ergänzend zu den datenschutzrechtlichen Aspekten nur Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302.

Abbildung 3 zeigt, wie sich das Geschäftsmodell „Remote-Diagnose“ in die Struktur des Mobilitätsdatenwächters einfügt. Dritte, welche die Dienstleistung „Remote Diagnose“ anbieten wollen, benötigen hierfür den Zugang zu vorgenannten Fahrzeugdaten. Dieser Zugang wird über den „Datentreuhänder“ gewährleistet. Insbesondere bei dem Angebot „Remote-Diagnose“ kommt es darauf an, dass die Bedingungen des Datenzugangs für alle Dienstleister dieselben sind. Dies gilt im Besonderen für den Zeitpunkt der Datenübermittlung und die Möglichkeit, mit dem Kunden im Fahrzeug oder auch außerhalb Kontakt aufzunehmen. Soweit es sich bei den relevanten Fahrzeugdaten um personenbezogene Daten handelt, sind die datenschutzrechtlichen Vorgaben zu beachten. Der Vertrag hinsichtlich der Dienstleistung „Remote-Diagnose“ bildet die Rechtfertigung zur Datenverarbeitung durch den Anbieter. Die Problematik der Mehrpersonennutzung stellt sich auch hier. Insoweit kann erneut der Mobilitätsdatenwächter für die notwendige Transparenz und Kontrolle sorgen.

3. Datenspende für das Gemeinwohl

Durch das Konzept der Datenspende sollen für im allgemeinen Interesse liegende Ziele (für das Gemeinwohl) Daten zur Verfügung gestellt werden, etwa für die Verbesserung öffentlicher Dienstleistungen, für die Bekämpfung des Klimawandels oder für die sonstige Forschung (insb. im Gesundheitswesen[80]). Auch die Ziele Nachhaltigkeit und Sicherheit in der Mobilität, Unfallforschung, Verbesserung der Verkehrsinfrastruktur sowie die Ausarbeitung von Mobilitätskonzepten in Städten können durch die Sammlung und Auswertung großer Datenmengen maßgeblich gefördert werden.

[80] Vgl. insoweit ausführlich für das Bundesministerium für Gesundheit Strech et al. in „Datenspende – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen“, 2020.

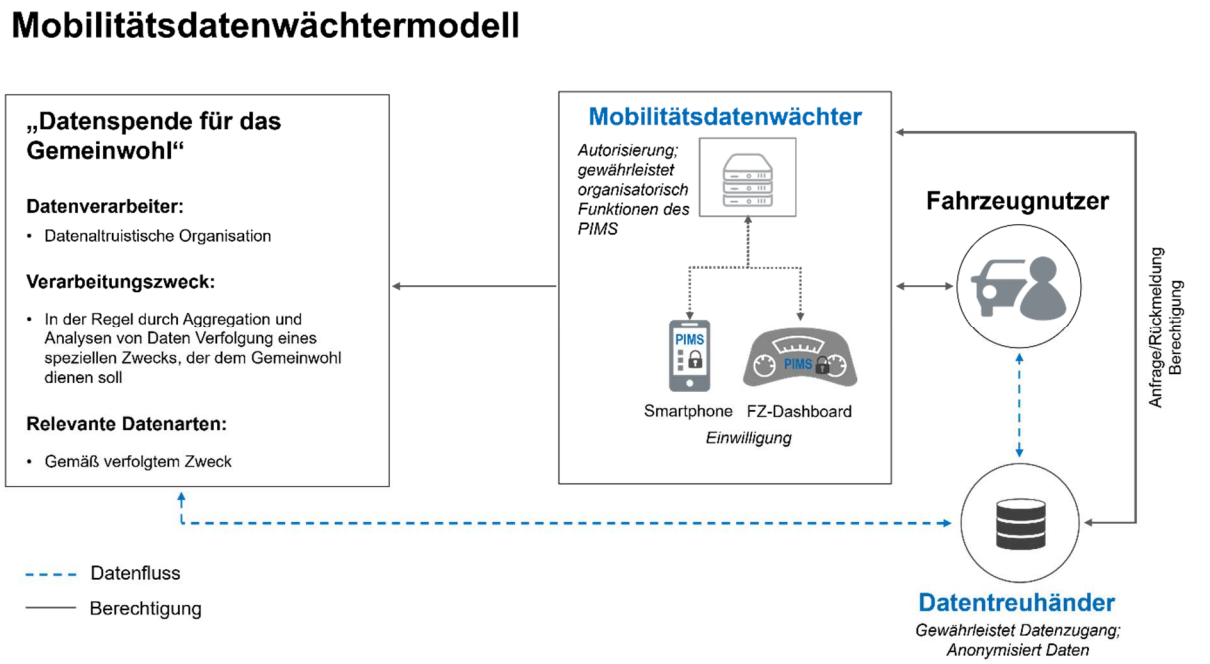

Abbildung 4: Mobilitätsdatenwächter Use Case "Datenspende für das Gemeinwohl"

Datenspenden sind nur dann möglich, wenn seitens des Betroffenen über die Daten verfügt, insbesondere wenn eine Weiterleitung an ausgesuchte Dritten (hier z. B. datenaltruistische Organisationen) überhaupt veranlasst werden kann. Das Mobilitätsdatenwächtermodell wird, wie Abbildung 4 zeigt, dieser Notwendigkeit gerecht, indem der „Datentreuhänder“ den fahrzeugherstellerunabhängigen Datenzugang im Fahrzeug gewährleistet. Um den datenschutzrechtlichen Anforderungen zu entsprechen, könnten die betroffenen Personen (Datenspender) jeweils in den Verarbeitungsvorgang einwilligen, vorausgesetzt der Nutzungszweck der Datenspende steht bereits ausreichend konkret fest. Alternativ kommt insbesondere auch eine Anonymisierung der Daten in Betracht, bevor die Datenspende an den Empfänger übermittelt wird. Den Anonymisierungsvorgang sollte der Datentreuhänder als neutrale Stelle vornehmen.[81]

Zuletzt wurde das Thema Datenspende durch den Data Governance Act[82] aufgegriffen und im Hinblick auf die Tätigkeit sog. datenaltruistischer Organisationen (Art. 18 DGA) konkretisiert. Organisationen, die Datenspenden entgegennehmen, um sie einem bestimmten Zweck zuzuführen, können sich als datenaltruistische Organisation eintragen lassen. In diesem Fall soll

[81] Vgl. hierzu bereits unter D.I.3.a.; derweil bleibt es im Hinblick auf die Verarbeitungstätigkeit des „Datentreuhänder“ dabei, dass dieser eine Einwilligung des Betroffenen benötigt, soweit eine Anonymisierung noch nicht durchgeführt wurde.

[82] Verordnung (EU) 2022/868.

das Vertrauen in derartige Organisationen dadurch gestärkt werden, dass ihnen besondere Transparenz-, Berichts- und Informationspflichten auferlegt werden.[83]

4. Wahrnehmung hoheitlicher Aufgaben

Soweit die öffentliche Hand (zulässigerweise) gedenkt, mit einem digitalen, datenbasierten Dienstangebot am Wirtschaftsleben teilzunehmen, steht sie mit den sonstigen Dritten, die einen Datenzugang begehren, in einer Reihe. Aber eben auch die Wahrnehmung bestimmter hoheitlicher Aufgaben im Bereich des staatlichen Ordnungsrechts hängt von einem verlässlichen Zugang zu Mobilitätsdaten ab. So können Mobilitätsdaten im Rahmen strafrechtlicher Ermittlungsverfahren als Beweismittel eine Rolle spielen.[84] Prüforganisationen müssen sich zur weiteren ordnungsgemäßen Durchführung von Hauptuntersuchungen daran anpassen, dass die sicherheitsrelevanten, softwarebasierten Systeme vernetzter Fahrzeuge ggf. ständigen Anpassungen unterliegen (z. B. durch Updates zur Fehlerbehebung, Funktionsverbesserungen oder –erweiterungen). Aus Sicht der Prüforganisationen ist es daher erforderlich, dass die Software eines Fahrzeugs sowie dessen elektronischen und vernetzten Bauteile nicht nur periodisch, sondern möglichst kontinuierlich unter Rückgriff auf sicherheits- und umweltrelevanten Fahrzeugdaten überprüft werden können. Weiter regelt z. B. § 63a Abs. 2 StVG im Hinblick auf Fahrzeuge mit hoch- und vollautomatisierten Fahrfunktionen zu Kontrollzwecken die Weitergabe bestimmter ereignisbezogener Daten[85] u. a. an die für die Ahnung von Verkehrsverstößen zuständigen Behörden. Gemäß § 1g StVG i.V.m. Anlage 2 AFGBV werden bestimmte Fahrzeugdaten ereignisbasiert erfasst und sind dem Kraftfahrt-Bundesamt (KBA) zur Erfüllung seiner Aufgaben zugänglich zu machen.

[83] Diese Pflichten stehen durchaus im Einklang mit den Funktionen des „Mobilitätsdatenwächters“, vgl. entsprechend unter E.II.1.

[84] Z. B. bei Maßnahmen nach §§ 94 ff. StPO.

[85] Positions- und Zeitangaben gemäß den Vorgaben von § 63a Abs. 1 StVG.

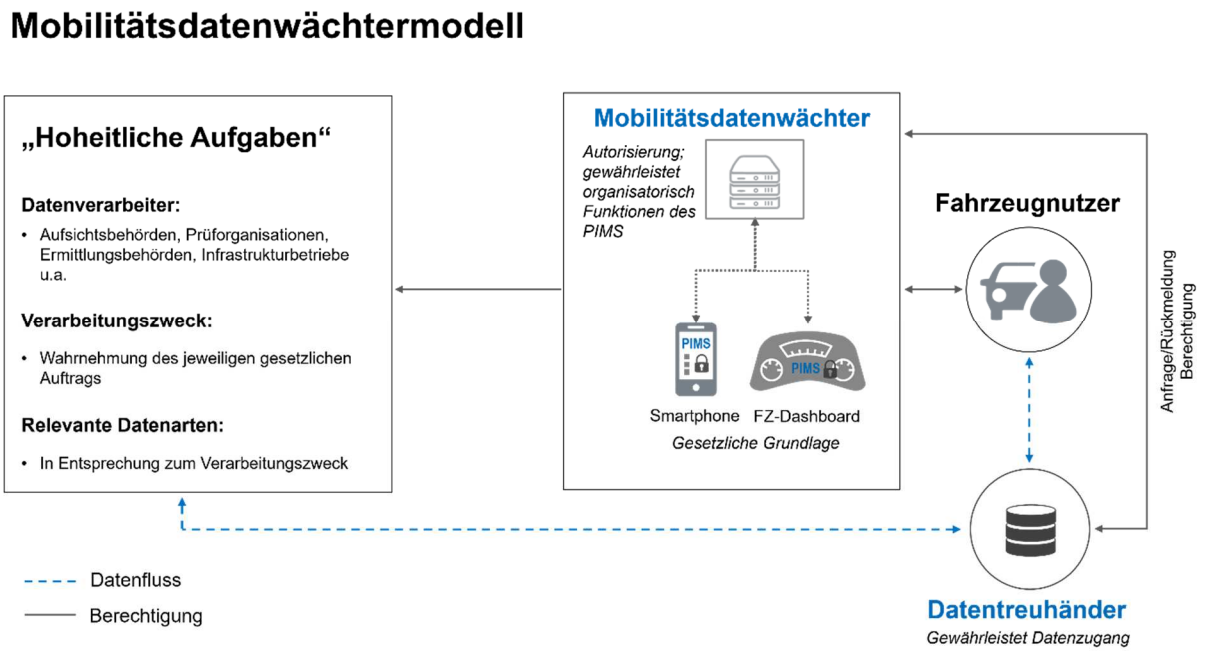

Abbildung 5: Mobilitätsdatenwächter Use Case "Wahrnehmung hoheitlicher Aufgaben"

Voraussetzung für die effiziente Wahrnehmung vorgenannter hoheitlicher Aufgaben ist jedoch ein entsprechender Zugang zu den jeweils relevanten Mobilitätsdaten. Diesen kann grundsätzlich auch der „Datentreuhänder“ gewährleisten, wie Abbildung 5 zeigt.[86] Dabei fällt dem „Mobilitätsdatenwächter“ weiterhin die Aufgabe zu, den Datenzugang auf Anfrage des „Datentreuhänders“ freizugeben. Im Kontext hoheitlicher Aufgaben wird für eine Berechtigung der Datenfreigabe auch das Vorliegen von Einwilligungserklärungen eine maßgebliche Rechtsgrundlage darstellen. Im Rahmen strafrechtlicher Ermittlungen bleibt allerdings die Einhaltung der strafprozessualen Vorschriften, insbesondere des Nemo-tenetur-Grundsatzes (§§ 55 Abs. 1, 136 Abs. 1 S. 2, 163a Abs. 4 S. 2, 243 Abs. 5 S. 1 StPO) zu beachten. Hier dürfte weiterhin nur über die Sicherstellung und Auslesung von Datenträgern gemäß §§ 94 ff. StPO der Zugang zu den Mobilitätsdaten möglich sein. Im Übrigen sorgt der „Mobilitätsdatenwächter“ auch im Bereich hoheitlicher Aufgaben gegenüber dem Fahrzeugnutzer für die notwendige Transparenz, indem er dem Nutzer die Information bereitstellt „ob“ und „inwieweit“ zur Erfüllung hoheitlicher Aufgaben auf sein Fahrzeug bzw. seine Person betreffende Mobilitätsdaten zugegriffen wurde.

[86] Ein entsprechendes Konzept für einen Datenzugang wurde seitens der Prüforganisationen unter der Bezeichnung „Trust Center“ bereits seit längerem gefordert, vgl. das Papier der deutschen Prüforganisationen „Position zum Zugang zu Fahrzeugdaten über die Remote-Fahrzeugschnittstelle (Over-the-Air) für hoheitliche Aufgaben“, 29. März 2019.

5. Produktsicherheit und Produktentwicklung

Fahrzeughersteller sowie ihre Zulieferer sind ständig damit befasst, ihre Produkte und Services weiterzuentwickeln sowie deren Qualität zu verbessern, um schließlich den Kundenbedürfnissen noch besser nachkommen zu können. Für diese Zwecke möchten Fahrzeughersteller und Zulieferer auf Daten aus dem Fahrzeug und aus weiteren vom Fahrzeugnutzer aktivierten Dienste zugreifen, um eine Auswertung vornehmen zu können. Relevant sind dabei u. a. Informationen zum technischen Zustand des Fahrzeugs (Diagnosedaten), Umgebungsdaten, Infrastrukturdaten oder Kommunikationsdaten.

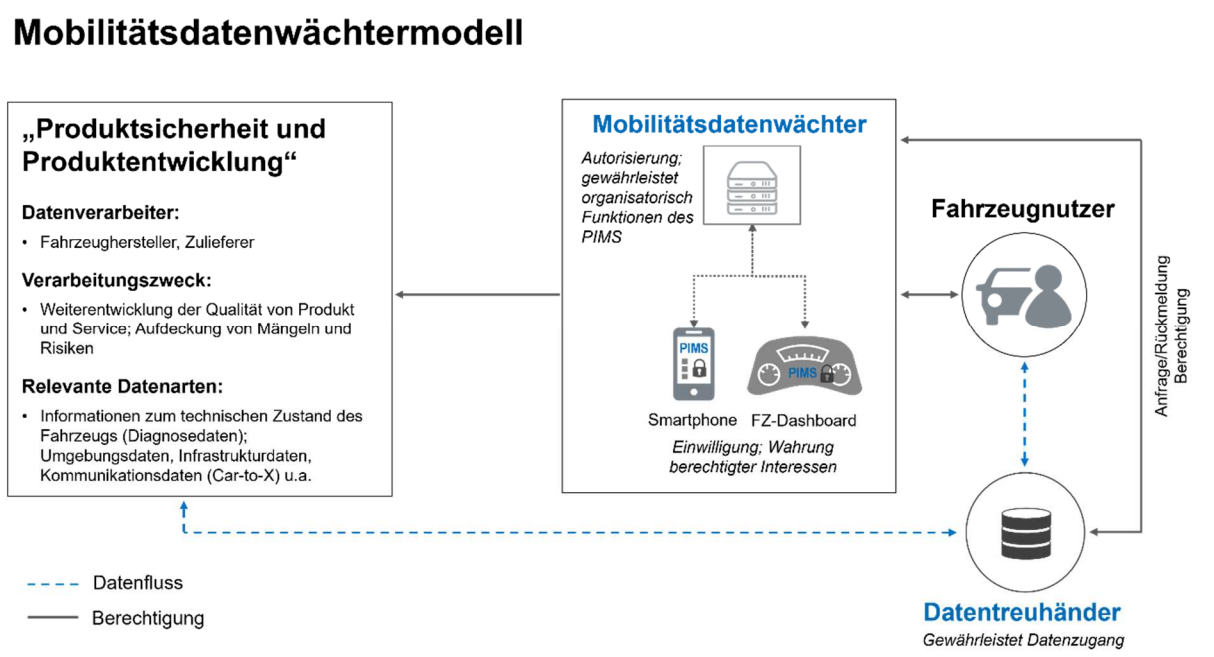

Abbildung 6: Mobilitätsdatenwächter Use Case "Produktsicherheit und Produktentwicklung"

Die Datenverarbeitung zum Zwecke von „Produktsicherheit und Produktentwicklung“ lässt sich, wie Abbildung 6 zeigt, ebenfalls interessengerecht über die Struktur des Mobilitätsdatenwächtermodells abbilden. Auch aus wettbewerblichen Gründen sollten für den Fahrzeughersteller und die sonstigen „Dritten“ beim Zugang zu Mobilitätsdaten grundsätzlich dieselben Bedingungen gelten.[87] Weiterhin gilt: Zugunsten des Fahrzeugherstellers existiert dem Grunde von vornherein nach kein Anspruch auf einen Zugang zu Mobilitätsdaten. Es sollte daher dem Fahrzeugnutzer auch im Hinblick auf Daten zur Produktsicherheit und Produktweiterentwicklung überlassen bleiben, ob er in eine Übertragung an den Fahrzeughersteller einwilligt. „Datentreuhänder“ und „Mobilitätsdatenwächter“ könnten daher auch in Bezug auf diese Art von Daten ihre Aufgaben gerechtfertigt erfüllen.

[87] Ein unmittelbarer Datenzugang des Fahrzeugherstellers, so wie er aktuell technisch besteht, kann nur im Falle wettbewerblicher Irrelevanz in Betracht kommen, vgl. bereits unter D.I.2.

E. Gesetzliche Umsetzung

I. Nationale Gesetzgebung

Soweit der europäische Gesetzgeber Regelungen im Sinne des hier vorgestellten Mobilitätsdatenwächtermodells nicht vorantreibt, kann der deutsche Gesetzgeber auf nationaler Ebene tätig werden. Als passender Regelungsbereich bietet sich das von der Regierung für das Jahr 2024 angekündigte „Mobilitätsdatengesetz“ an. Schwerpunktmäßig würde es dort auf die folgenden Regelungsbereiche ankommen:

- In Bezug auf den „Datentreuhänder“:

  - Die Definition des „Datentreuhänders“ und seiner Aufgaben;
  - Die Verpflichtung der Fahrzeughersteller, ihre Fahrzeuge so auszustatten, dass denjenigen Stellen, welche die Rolle des „Datentreuhänders“ wahrnehmen, Zugang zum Fahrzeug gewährt werden kann;
  - Die Eindeutige und klare Formulierung der an den „Datentreuhänder“ zu stellenden IT-Sicherheitsanforderungen;
  - Die Einrichtung einer beliehenen Stelle mit dem Auftrag des Aufbaus und Betriebs eines „Datentreuhänders“.

- In Bezug auf den „Mobilitätdatenwächter“:

  - Die Definition des „Mobilitätsdatenwächters“ und seiner Aufgaben;
  - Eine Kooperationspflicht der Datenverarbeiter mit dem „Mobilitätsdatenwächter“ (d. h. insb. mit dem PIMS);
  - Die Interoperabilität bei der Zusammenarbeit zwischen (verschiedenen) „Mobilitätsdatenwächter(n)“ und „Datentreuhänder(n)“
  - Ein Zertifizierungs- und Überwachungssystem im Falle der Gründung weitere „Mobilitätsdatenwächter“;
  - Einrichtung einer beliehenen Stelle mit dem Auftrag des Aufbaus und Betriebs eines „Mobilitätsdatenwächters“.

Soweit europäisches Recht dem nicht entgegensteht (siehe hierzu sogleich), könnte der deutsche Gesetzgeber in Entsprechung zum Gesetz zum autonomen Fahren[88] auch im Hinblick auf die Verarbeitung und den Schutz von Mobilitätsdaten eine Vorreiterrolle einnehmen.

[88] Gesetz v. 12.07.2021 (BGBl. I S. 3108).

II. Beachtung von EU-Recht

1. Data Governance Act (DGA)

Eine wichtige Säule der europäischen Datenstrategie[89] bildet der Data Governance Act (DGA)[90], der darauf abzielt, die Verfügbarkeit von Daten zur gemeinsamen Verwendung und wirtschaftlichen Nutzung zu erhöhen und damit den europäischen Märkten einen Wettbewerbsvorteil bei datenbasierten Innovationen zu verschaffen. Neben der Bereitstellung von Daten der öffentlichen Hand (Art. 3ff. DGA) schafft der DGA Vorgaben für sog. Datenvermittlungsdienste (Art. 10ff. DGA) sowie einen Regelungsrahmen für datenaltruistische Organisationen (Art. 16ff. DGA). Indes lassen sich aus dem DGA keine Datenzugangsansprüche herleiten.

Datenvermittlungsdienste sind, vorbehaltlich einzelner Bereichsausnahmen, alle Dienste, mit denen durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen (vgl. Art. 2 Nr. 11 DGA). Soweit ein solcher Datenintermediär in den Anwendungsfall von Art. 10 DGA fällt, muss er nach Art. 12 DGA verschiedene Verhaltenspflichten wie Neutralität, Verbot von Kopplungsgeschäften, Interoperabilität, Diskriminierungsverbot sowie Überwachungs- und Sicherheitspflichten erfüllen. Es soll an dieser Stelle nicht abschließend festgestellt werden, ob der „Datentreuhänder“ i.S. des hier vorgestellten Modells gemessen an der Definition sowie an Sinn und Zweck der Vorschrift ebenfalls Datenintermediär i.S. des DGA ist. Der Hauptaufgabe des „Datentreuhänders“ ist es, den Datenzugang ins Fahrzeug zu gewährleisten. Erst daraus folgen die Aufgabe bzw. die Notwendigkeit der Datenweiterleitung. Soweit allerdings der DGA Anwendung findet, wären seitens des „Datentreuhänders“ die Verhaltenspflichten gemäß Art. 12 DGA zwingend zu beachten. Soweit dies nicht der Fall ist, sollten für den „Datentreuhänder“ die auch für ihn zweckmäßigen Pflichten analog zu Art. 12 DGA festgeschrieben werden.

Durch den Regelungsrahmen für datenaltruistische Organisationen soll eine transparente Datenverarbeitung sichergestellt werden. Insbesondere sind umfassende Informationspflichten gegenüber dem Betroffenen (Zweck, Ort der Verarbeitung) zu erfüllen (Art. 20, 21 DGA). Zudem ist ein europäisches Einwilligungsformular vorgesehen (vgl. Art. 25 DGA). In Ansehung der Eigenschaften und Pflichten eines Datenintermediärs, der (im Hinblick auf Datenspenden) besonderen Transparenz- und Berichtspflichten sowie einer standardisierten Einwilligungserklärung erscheinen die Regelungen, wie sie vorliegend für den kontrollierten, treuhänderischen

[89] Vgl. Mitteilung der Europäischen Kommission COM/2020/66 final.

[90] Verordnung (EU) 2022/868.

Umgang mit Mobilitätsdaten dargestellt wurden, nur konsequent und stehen insoweit insbesondere im Einklang mit der verfolgten europäischen Datenstrategie. Insoweit wird eine nationale Umsetzung des Mobilitätsdatenwächtermodells durch den Regelungsrahmen des DGA unterstützt und ergänzt, ist aber jedenfalls nicht gesperrt.

2. Data Act-Entwurf

Als weitere Säule der europäischen Datenstrategie hat die Europäische Kommission den Entwurf einer Verordnung zur Regelung des fairen Zugangs zu und der Nutzung von Daten (sog. „Data Act“) vorgelegt. Nach dem bisherigen Entwurf sollen Großunternehmen dazu verpflichtet werden, ihre Produkte und damit verbundene Dienstleistungen derart zu gestalten, dass der Zugang für Nutzer zu den durch sie generierten Daten sowie die Weitergabe an Dritte möglich ist (vgl. Art. 3-5 Data Act-Entwurf). Der Data Act zielt damit insbesondere auf den Zugang zu Daten aus IoT-Produkten ab, zu denen grundsätzlich auch vernetzte Fahrzeuge zählen.

Der Data Act soll sektorübergreifend gelten. Entsprechend ist für einzelne Branchen zu hinterfragen, ob die Regelungen passend und ausreichend sind. Im Hinblick auf den Zugang zu Mobilitätsdaten bestehen hier Zweifel. In erster Linie bliebe es bei der faktischen Datenhoheit der Fahrzeughersteller, da durch den Data Act die Datenarchitektur nicht verändert wird. Zudem regelt der Data Act keinen Zugang zu Funktionen und Ressourcen des Fahrzeugs, so dass die Installation von Software im Fahrzeug sowie eine direkte Kommunikation mit dem Fahrzeugnutzer problematisch bleibt. Eine sektorspezifische Regulierungslösung, wie sie aktuell auf EU-Ebene diskutiert wird und sie das hier vorgestellte Mobilitätsdatenwächtermodell darstellen würde, dürfte damit weiterhin notwendig bleiben.[91]

3. (Potentielle) Sektorspezifische Regelung

In Ansehung des geplanten Regelungsrahmens des Data Acts wäre eine sektorspezifische Regelung für einen Zugang zu Mobilitätsdaten sowohl auf europäischer als auch auf nationaler Ebene möglich. Aktuell hat sich der europäische Gesetzgeber dieser Frage angenommen und strebt eine sektorspezifische Regulierung durch Änderung der Typengenehmigungsverordnung[92] an. Ob neben einer solchen europäischen Regelung andere oder weitergehende Datenzugangsmöglichkeiten durch nationale Gesetzgebung vorgeschrieben werden können, hängt davon ab, ob und inwieweit der europäische Gesetzgeber mit der Änderung der Typengenehmigungsverordnung eine Vollharmonisierung vornehmen wird. Im europäischen Gesetzgebungsprozess für eine sektorspezifische Regulierung sollte sich die Bundesregierung dafür einsetzen, dass dort die Einführung eines PIMS mitgeregelt wird. Falls die Bemühungen hier nicht erfolgreich sind, käme jedenfalls hinsichtlich der Einführung eines PIMS weiterhin eine nationale Regelung in Betracht.

[91] Vgl. insoweit auch Kerber/Gill in „Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations“, 2022, S. 3f.

[92] Verordnung (EU) 2018/858; vgl. Fn. 5.

F. Abschließende Zusammenfassung

Abschließend lassen sich die folgenden Feststellungen zusammenfassen:

- In vernetzten Fahrzeugen verbaute Sensoren und Steuergeräte generieren, insbesondere bei Bewegung des Fahrzeugs, eine Vielzahl von Daten (Mobilitätsdaten). Hierzu zählen Fahrzeugdaten, Fahrzeugbediendaten, Fahrzeugumgebungsdaten, Infrastrukturdaten oder Ereignisdaten. Eine Speicherung im Fahrzeug kommt flüchtig oder mittels fester Speicher in Betracht. Darüber hinaus können die Daten per Mobilfunkschnittstelle (over-the-air) an externe Stellen übertragen werden.

- Entlang der Fahrzeugwertschöpfungskette begehren die Fahrzeughersteller, die Fahrzeugnutzer und sonstige Dritte (insb. Versicherer, Werkstätten, Pannenservices, Behörden, Prüforganisationen, Infrastruktureinrichtungen u.a.) Zugang zu Mobilitätsdaten. Indes liegt aufgrund der derzeit gewählten Datenarchitektur die faktische Datenhoheit beim Fahrzeughersteller. Gemäß der Werkskonfiguration und aufgrund fehlender Schnittstellen sehen vernetzte Fahrzeuge aktuell auch für den Fahrzeugnutzer selbst keinen Zugriff auf die im Fahrzeug generierte Daten vor. Ein Anspruch des Fahrzeugnutzers auf Datenzugang und/oder Datenweitergabe lässt sich, soweit überhaupt zweckmäßig, nur in den engen Grenze des Art. 20 DSGVO begründen. Für sonstige Dritte kommt eine Datenverarbeitung über die OBD-II-Schnittstelle oder unter Zuhilfenahme des Smartphones in Betracht. Darüber hinaus können Mobilitätsdaten, soweit dies im Rahmen des ADAXO- bzw. ExVe-Konzepts angeboten wird, über den Fahrzeughersteller zu seinen Bedingungen (bzgl. Preis, Quantität und Qualität der Daten) angefordert werden. Auch für Dritte sind die rechtlichen Möglichkeiten zur Begründung eines Datenzugangsanspruchs sehr begrenzt. Ein Datenzugang für die Umsetzung digitaler, datenbasierter Geschäftsmodelle ist in Art. 61 Verordnung (EG) Nr. 2018/858 nicht angelegt. Die rechtlichen Hürden zur Durchsetzung kartellrechtlicher Datenzugangsansprüche im Rahmen der Marktmissbrauchsvorschriften sind hoch.

- Gemessen an der Legaldefinition in Art. 4 Nr. 1 Hs. 1 DSGVO handelt es sich nach h. M. bei Mobilitätsdaten regelmäßig um „personenbezogene Daten“. In der Folge muss jede Datenverarbeitung durch eine gesetzliche Grundlage gerechtfertigt sein. In Betracht kommt eine Datenverarbeitung zur Vertragserfüllung, zur Erfüllung einer gesetzlichen Pflicht oder zur Wahrung berechtigter Interessen der verantwortlichen Stelle. Hilfsweise kann die Datenverarbeitung auf der Grundlage einer ausdrücklichen Einwilligung des Betroffenen legitimiert sein. Vorgenannte Rechtfertigungstatbestände haben ihre Grenzen. In Diskussion steht, inwieweit die verantwortlichen Stellen diese Grenzen überschreiten. Im Fokus stehen dabei die Wirksamkeitsvoraussetzungen einer Einwilligungserklärung, insb. im Hinblick auf Freiwilligkeit, Informiertheit sowie Bestimmtheit und Zweckbindung.

Durch zu umfangreiche und unübersichtliche Datenschutzinformationen besteht in der Praxis das Risiko einer Informationsüberlastung des Betroffenen, so dass dieser die Informationen gar nicht mehr zur Kenntnis nimmt und somit auch nicht informiert einwilligen kann. Datenschutzverstöße werden von den Betroffenen aber hingenommen, indem sie aus Unkenntnis, Zeit- und Kostengründen ihre Datenschutzrechte nicht wahrnehmen.

- Auf Märkten, die auf der Ressource Mobilitätsdaten basieren, stehen sich Fahrzeughersteller und mit ihnen verbundene Unternehmen auf der einen Seite und sonstige Dienstleister auf der anderen Seite als Wettbewerber gegenüber. Der Fahrzeughersteller ist dabei nicht nur als Fahrzeugproduzent und -verkäufer tätig, sondern bietet darüber hinaus auch Komplementärdienstleistungen an. Aus den aktuell beschränkten Möglichkeiten des Datenzugangs für den Fahrzeugnutzer sowie auf B2B-Ebene resultiert für nachgelagerte Märkte der Fahrzeugbranche das Risiko einer Beschränkung der Wettbewerbsfunktionen (insb. Beschränkung von Innovation und der Wahlfreiheit von Verbrauchern). Dies birgt das Risiko für ein Marktversagen, was sich zum Nachteil der Fahrzeugnutzer (insbesondere Verbraucher) auswirkt.

- Eine Durchsicht fahrzeuginterner Systeme zeigt, dass die Möglichkeiten zur Vornahme von Datenschutzeinstellungen im Fahrzeug beschränkt sind. Das verfügbare digitale, datenbasierte Dienstleistungsangebot besteht nahezu nur aus Angeboten des jeweiligen Fahrzeugherstellers. Eigene Datenzugangsmöglichkeiten des Fahrzeugnutzers über Schnittstellen sind nicht vorgesehen. Daraus ergibt sich, dass den datenschutzrechtlichen Herausforderungen sowie den Risiken für ein Marktversagen weiterhin begegnet werden muss.

- Beteiligte des „Mobilitätsdatenwächtermodells“ sind „Fahrzeugnutzer“, „Dritte“, der „Datentreuhänder“ sowie der „Mobilitätsdatenwächter“. Nach hiesigem Verständnis zählt zu den „Dritten“ auch der Fahrzeughersteller selbst, der sich von den übrigen Dritten nur darin unterscheidet, dass er faktisch, d. h. in technischer Hinsicht bereits unmittelbar auf die Daten im Fahrzeug zugreifen kann. Insbesondere unter Berücksichtigung wettbewerblicher Aspekte besteht jedoch keine Veranlassung, dem Fahrzeughersteller im Rahmen des Mobilitätsdatenwächtermodells eine Sonderstellung einzuräumen. Für den Fall, dass der Fahrzeugnutzer einem Dritten die sein Fahrzeug betreffenden Mobilitätsdaten überlassen will, muss dies dem Fahrzeugnutzer organisatorisch und technisch möglich sein. Um an dieser Stelle der faktischen Datenhoheit der Fahrzeughersteller zu begegnen, soll anstelle des Fahrzeugherstellers einem „Datentreuhänder“ technisch der unmittelbare Datenzugang gewährt werden. Der „Datentreuhänder“ empfängt die Daten aus dem Fahrzeug und kann diese weiterleiten. Über die Information, ob, inwieweit und an wen Mobilitätsdaten weitergegeben werden dürfen/sollen, verfügt nicht der „Datentreuhänder“, sondern der „Mobilitätsdatenwächter“. Dieser betreibt ein Personal Information Management

System (PIMS), in dem der Fahrzeugnutzer seine erforderlichen Erklärungen und Einstellungen zur Datenverarbeitung hinterlegen und sämtliche Datenverarbeitungsvorgänge transparent nachverfolgen kann.

- Die Hauptaufgabe des „Datentreuhänders“ besteht darin, den Zugang zu Mobilitätsdaten in technischer Hinsicht zu gewährleisten. Durch den Zugang über eine besondere treuhänderische Stelle, die alle IT-Sicherheitsanforderungen erfüllt, wird bestehenden Cyberrisiken begegnet. Neben der Ermöglichung des Datenzugangs soll der „Datentreuhänder“ – soweit datenschutzrechtlich geboten – für den ordnungsgemäßen technischen Vorgang einer nachträglichen Anonymisierung sorgen. Aus der wettbewerblichen Perspektive ist die Einbindung mehrerer „Datentreuhänder“ anzustreben. Soweit es sich um wettbewerbsrelevante Daten handelt, sollte der Fahrzeughersteller seinen exklusiven direkten Datenzugang aufgeben und Zugang zu Mobilitätsdaten, wie andere Dritte, lediglich (ggf. kostenpflichtig) über den „Datentreuhänder“ erhalten.

- In Entsprechung zur Darstellung der Aufgaben des „Datentreuhänders“ nimmt der „Mobilitätsdatenwächter“ die Funktion der Autorisierungsstelle wahr. Diese Aufgabentrennung zwischen „Datentreuhänder“ (Zugang zum Fahrzeug; Datenweiterleitung) und „Mobilitätsdatenwächter“ (Autorisierung) gewährleistet die Neutralität beim Umgang mit den Mobilitätsdaten. Der Betrieb eines Personal Information Management Systems (PIMS) soll den Nutzern dabei helfen, die Datenverarbeitungen besser anweisen, kontrollieren und steuern zu können. Zur Begegnung der mobilitätsdatenspezifischen Herausforderungen bei der Datenverarbeitung ist die Einbindung folgender PIMS-Funktionen zweckmäßig: 1. Einwilligungsmanagement, 2. Gewährleistung von Transparenz und Nachvollziehbarkeit von Verarbeitungsvorgängen, 3. Assistenz zur Durchsetzung von Datenschutzrechten. Die erfolgreiche Implementierung eines PIMS setzt, neben Organisation und Finanzierung, standardisierte technische Voraussetzungen sowie vor allem eine Kooperationspflicht der Datenverarbeiter mit dem PIMS voraus. Die nur freiwillige Nutzung eines PIMS dürfte wegen fehlender Akzeptanz auch auf Betroffenenseite zum Misserfolg führen. Soweit ein PIMS nicht eingeführt wird, kämen hilfsweise verbindliche Vorgaben für die herstellereigenen Systeme der Fahrzeughersteller und Berücksichtigung der beschriebenen PIMS-Funktionen in Betracht.

- Zur Sicherstellung von Neutralität, Qualität und Finanzierung sollten sowohl der „Datentreuhänder“ als auch der „Mobilitätsdatenwächter“ als staatliche oder zumindest beliehene Stelle ausgestaltet werden. Die Überlassung der jeweiligen Aufgaben an private Unternehmen ist zwar denkbar. Jedoch bleibt unklar, ob eine privatwirtschaftliche Finanzierung überhaupt realisiert werden kann oder ob durch (ein einzelnes) hauptsächlich wirtschaftlich handelnde Unternehmen die Ziele des „Datentreuhänders“ und des „Mobilitätsdatenwächters“, namentlich insbesondere ein diskriminierungsfreier Zugang zu Fahrzeugdaten

sowie eine selbstbestimmte Entscheidungshoheit der Fahrzeugnutzer, überhaupt gewährleistet werden können. Auf lange Sicht betrachtet sollten die staatlichen Stellen die Aufgaben des „Datentreuhänders“ und des „Mobilitätsdatenwächters“ aber nicht exklusiv wahrnehmen. Es sollte privaten Unternehmen grundsätzlich freistehen, ebenfalls im Rahmen des Mobilitätsdatenwächtermodells als Wettbewerber tätig zu werden, wobei zur Einhaltung der Qualitätsstandards ein angemessenes Zertifizierungs- und Überwachungssystem zu etablieren wäre.

- Das „Mobilitätsdatenwächtermodell“ lässt sich beliebig und flexibel auf verschiedene Use Cases anwenden. Gleichermaßen kann das Modell den Interessen der Fahrzeughersteller, der Dienstleister aus der Privatwirtschaft, des Gemeinwohls sowie hoheitlicher Stellen gerecht werden.

- Soweit der europäische Gesetzgeber Regelungen im Sinne des hier vorgestellten Mobilitätsdatenwächtermodells nicht vorantreibt, kann der deutsche Gesetzgeber auf nationaler Ebene tätig werden. Ein geeigneter Regelungsbereich wäre das von der Bundesregierung für das Jahr 2024 angekündigte „Mobilitätsdatengesetz“. Eine solche nationale Regelung müsste dabei mit europäischen Vorschriften vereinbar sein. Insoweit erscheinen jedoch die Regelungen, wie sie vorliegend für den kontrollierten, treuhänderischen Umgang mit Mobilitätsdaten vorgeschlagen werden, nur konsequent und stehen insbesondere im Einklang mit der verfolgten europäischen Datenstrategie.

***

G. Abbildungsverzeichnis

H. Quellenverzeichnis

Bönninger, zfs 2014, 184.

BfDI, Vernetzte Fahrzeuge – Datenschutz im Auto, 2020.

Datenethikkommission der Bundesregierung, Gutachten der Datenethikkommission, Oktober 2019

Denker et al., „Eigentumsordnung“ für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive, 2017

Europäischer Datenschutzbeauftrage (EDSB), Stellungnahme 9/2016, 2016

Europäische Kommission, Access to In-vehicle data and Resources, 2017

Europäische Kommission, Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie, COM/2020/66 final

FIGIEFA et al., Secure On-board Telematics Platform Approach, Januar 2021

Hoegaerts/Schönenberger, The automotive digital transformation and the economic impacts of existing data access models, 2019

Hornung/Goeble, CR 2015, 265, 268

Huerkamp/Nuys, NZKart 2021, 327

Kerber/Gill, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022.

Klink-Straub/Straub, ZD 2018, 459.

Kühling/Buchner, DS-GVO BDSG, Kommentar, 3. Auflage, 2020

Kumpf, Smart Cars – eine datenschutzrechtliche Analyse, 2017

Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302.

Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, 2018

Poikola et al., MyData – an introduction to human-centric use of personal data, 2020

Reiter, DAR, 2022, 122

Schenkel, Neuer kartellrechtlicher Datenzugangsanspruch am Beispiel von Fahrzeugdaten, Festschrift für Dr.-Ing. E.h. Jürgen Bönninger, S. 227ff.

Störing/Eilers, PinG 2015, 118,

Strech/vonKielmansegg/Zenker/Krawczak/Semler, Datenspende – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 2020.

VdTÜV e.V. et al., Position zum Zugang zu Fahrzeugdaten über die Remote-Fahrzeugschnittstelle (Over-the-Air) für hoheitliche Aufgaben, 29. März 2019

Verbraucherzentrale Bundesverband, Neue Datenintermediäre – Anforderungen des vzbv an Personal Information Management Systeme (PIMS) und Datentreuhänder, 12. September 2020

Verbraucherzentrale Bundesverband, Positionspapier, Fahrerlos alle mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht, 12. Oktober 2021

VDA, Positionspapier, ADAXO: Automotive Data Access – Extended and Open - VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten, 2021

Weber, WRP 2020, 559

Weichert, NZV 2017, 507

Wolff/Brink, BeckOK Datenschutzrecht. 37. Edition, 2021

Zdanowiecki, DSRITB, 2018, 559

ZDK/ADAC/GDV et al., Positionspapier, Gleichberechtigter Zugang zum vernetzten Fahrzeug – Mobilitätsbranche fordert sektorspezifische Regelung, 20 Januar 2022.

Rechtsanwalt Prof. Dr. Julius Reiter
Professor für Wirtschaftsrecht
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für IT-Recht

Rechtsanwalt Dr. Olaf Methner
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Arbeitsrecht
Fachanwalt für IT-Recht

Rechtsanwalt Bénédict Schenkel
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für IT-Recht

Baum Reiter & Collegen Rechtsanwaltsgesellschaft mbH

Standort Düsseldorf
Benrather Schlossallee 101
40597 Düsseldorf

Standort Berlin
Hausvogteiplatz 11a
10117 Berlin

Tel.: 0211 / 836 805-70
Fax: 0211 / 836 805-78
E-Mail: kanzlei@baum-reiter.de
www.baum-reiter.de

15. November 2022