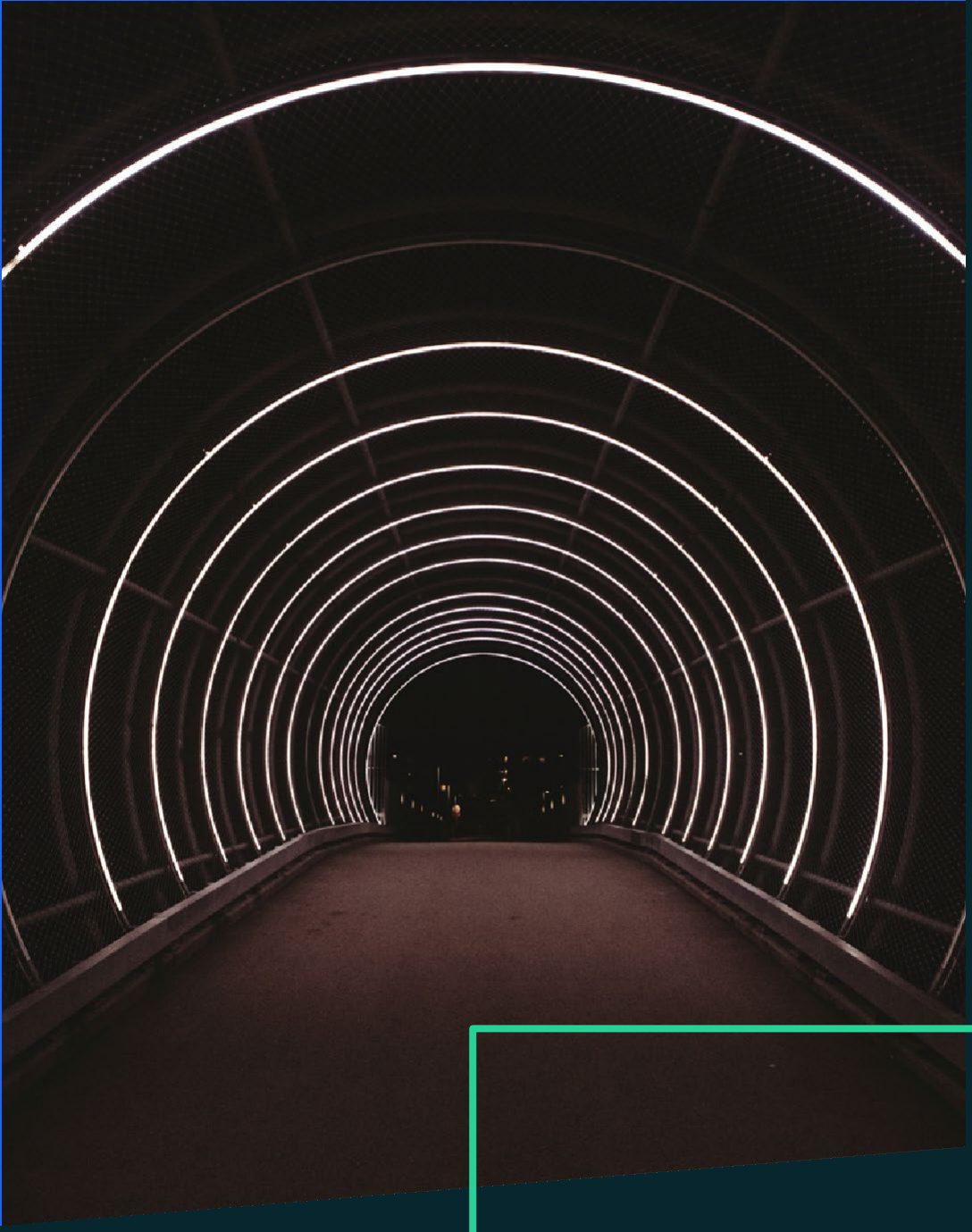

bitkom

Explainer: Datentreuhänder im Automobilbereich

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Paul Hannappel | Bereichsleiter Mobility &
Logistics | T 030 27576-130
p.hannapel@bitkom.org

David Schönwerth | Bereichsleiter Data Economy
T 030 27576-179 | d.schoenwerth@bitkom.org

Verantwortliches Bitkom-Gremium

AK Automatisiertes, vernetztes & autonomes Fahren
AK Datenpolitik & Datenräume

Inhalt

1 Einleitung & Use Cases

Der Bitkom spricht sich derzeit weder für noch gegen einen Datentreuhänder im Automobilbereich aus. In jedem Fall denken wir, dass die Diskussion zu diesem Thema, wenn dann, sachlich und entlang konkreter Szenarien geführt werden sollte.

Potenzielle Anwendungsfälle eines Datentreuhänders im Automobilbereich im Kontext des Teilens von Daten im Umfeld von **Fahrzeugherstellern, Fahrzeughaltern, Zuliefererbetrieben, Prüforganisationen, Werkstätten, Automobilclubs, Pannendiensten, Versicherungsunternehmen und bestimmten weiteren Dritten** werden im Folgenden benannt. Zu beachten ist dabei, dass die beschriebenen Aufgaben eines Datentreuhändermodells zum Teil heute bereits über vorhandene technische Lösungen erfüllt werden können. Ebenso ist zu klären, welche Aufgabe durch einen Datenvermittlungsdienst ausgeführt werden können (vgl. Kapitel 4):

Anonymisierung oder Pseudonymisierung von Daten: Ein Datentreuhänder könnte durch Pseudonymisierung oder Anonymisierung die Verarbeitung von Daten von vormals personenbezogenen Daten ermöglichen und es somit erlauben, dass wertvolle Erkenntnisse aus den gesammelten Daten gewonnen werden können (z. B. Daten zum Fahrverhalten).

Aufbereitung und Harmonisierung der Datenformate: Datentreuhänder können die unterschiedlichen Datenformate verschiedener Fahrzeughersteller vereinheitlichen, sodass Drittanbieter die Daten leichter weiterverwenden und innovative Dienste entwickeln können.

Neutrale, unabhängige Instanz für den Datenaustausch: Ein Datentreuhänder kann als neutrale Instanz für den sicheren Datenaustausch mit unterschiedlichen Akteuren dienen.

Übergreifender Datenaustausch für die Verkehrssicherheit: Ein Datentreuhänder kann den hersteller- und versicherungsübergreifenden Austausch von Daten zur Verkehrssicherheit ermöglichen (z. B. Daten zu Unfällen und gefährlichen Straßenabschnitten).

Übergreifender Datenaustausch für Nachhaltigkeitsreporting: Ein Datentreuhänder kann hersteller- und versicherungsübergreifend Daten sammeln und konsolidieren, um ein umfassendes Nachhaltigkeitsreporting (z. B. eines Fuhrparks) zu ermöglichen, das den gesetzlichen und organisatorischen Anforderungen entspricht.

Datenbörse für Fahrzeughalter: Ein Datentreuhänder könnte eine »Datenbörse« bereitstellen, die alle relevanten Fahrzeugdaten aus verschiedenen Quellen sammelt und dem Fahrzeughalter sicher und übersichtlich zur Verfügung stellt.

2 Gesetzlicher Hintergrund

2.1 Beziehung zur UN-Richtlinie Nr. 155

Die ↗ Richtlinie stellt insb. Anforderungen an die Sicherheit von Fahrzeugen gegen Cyber-Angriffe. Nach der UN-Richtlinie Nr. 155 verantwortet der Fahrzeughersteller die Cybersicherheit des Fahrzeuges – von der Konzeption bis zur Entsorgung. Die Regelung gilt unbeschadet anderer UN-Regelungen, sowie regionaler oder nationaler Rechtsvorschriften, die den Zugang zu dem Fahrzeug, seinen Daten, Funktionen und Ressourcen sowie die Bedingungen für diesen Zugang durch Berechtigte regeln. Daraus allein kann nicht abgeleitet werden, wie sich UN-Richtlinie Nr. 155 zu erwähnten Rechtsvorschriften verhält.

2.2 Beziehung zur UN-Richtlinie Nr. 156

Die ↗ Richtlinie knüpft an die UN-Richtlinie Nr. 155 an und schreibt die Entwicklung und den Betrieb eines »Software Update Management Systems« (SUMS) für Neufahrzeuge vor. Die Richtlinie fordert auch zusätzliche Maßnahmen, wenn Updates über eine Funkschnittstelle »over the air« (OTA) verteilt werden. Die Einhaltung der Richtlinie verantwortet der Fahrzeughersteller.

2.3 Beziehung zur Typgenehmigungsverordnung

Die ↗ Verordnung (EU) 2018/858, die sog. Typgenehmigungsverordnung (Typgenehmigungs-VO), regelt unter anderem die Genehmigung und Marktüberwachung von Kraftfahrzeugen sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge. Die Typgenehmigungs-VO wird zur Begriffsbestimmung (Artikel 3) einzelner Akteure herangezogen.

2.4 Beziehung zum Data Governance Act

Es wäre zu klären, ob und ggf. inwiefern zukünftige Datentreuhänder im Automobilsektor unter den ↗ Data Governance Act (DGA) fallen würden. Diese Verordnung gilt in der EU seit 24. September 2023. Die sich daraus u. a. ergebenden neuen Pflichten für Datenvermittlungsdienste hat der Bitkom ↗ hier bereits näher erläutert.

2.5 Beziehung zum Data Act

Es wäre zu klären, welche Rolle zukünftige Datentreuhänder im Automobilsektor vor dem Hintergrund der ab September 2025 geltenden Datenbereitstellungspflichten des ↗Data Act[3] (oder deren Implementierung) haben. Der Anspruch des Datenempfängers gegen den Dateninhaber auf eine Direktlieferung der Daten nach Art. 5 Abs. 1 Data Act ohne Zwischenschaltung eines Datenintermediärs, bspw. eines Datentreuhänders, bleibt jedenfalls ohne Weiteres unberührt.

2.6 Access to in-vehicle data, functions and resources

Die Europäische Kommission erarbeitet aktuell einen ↗Entwurf für eine Verordnung für den Zugriff auf Fahrzeugdaten, -funktionen und -ressourcen. Wichtig ist hierbei die Unterscheidung zwischen einerseits Daten und andererseits Ressourcen (d. h. Hardware) sowie Funktionen (d. h. Software).[4]

2.7 Koalitionsvertrag (2021 bis 2025) zwischen SPD, Bündnis 90/Die Grünen und FDP

Ferner strebt der ↗Koalitionsvertrag der Bundesregierung ein Treuhändermodell für Fahrzeugdaten an.[5]

2.8 Beziehung zum Mobilitätsdatengesetz

Der ↗Referentenentwurf für ein Mobilitätsdatengesetz des Bundesministeriums für Digitales und Verkehr (BMDV) sieht einen Datenkoordinator für Mobilitätsdaten sowie eine unabhängige Datenaufsichtsbehörde vor. Fahrzeugdaten sind jedoch vom Anwendungsbereich des Gesetzes ausgenommen.

3 Der EU-Data Act wird grundsätzlich ab dem 12. September 2025 angewendet. Mit ihm werden insbesondere Datenzugriffsrechte für Nutzende von vernetzten Geräten und verbundenen Diensten gegenüber sog. Datenhaltern eingeführt. Diese Rechte ergänzen die Portabilitätsrechte der DS-GVO um den Anwendungsbereich von Daten ohne Personenbezug und erweitern die Gruppe der Anspruchsinhaber um rechtliche Personen.

4 Im erwarteten sektoralen EU-Verordnungsentwurf für den Zugang zu Fahrzeugdaten soll es (anders als im horizontalen EU-Data Act) nicht nur um Daten, sondern ebenso um Ressourcen und Funktionen gehen. Die Formulierung »data, functions, and resources« findet sich ebenfalls in Ziff. 1.3 UN-Richtlinie Nr. 155.

5 Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, 2021, Seite 52.

3 Definitionen

3.1 Allgemein

Technisch ist die Abgrenzung zwischen **Daten, Funktionen (d. h. Software) und Ressourcen (d. h. Hardware)** nicht einfach und teils streitig, da diese Konzepte miteinander verschränkt sind und sich gegenseitig bedingen. Teilweise wird argumentiert, dass die Trennung zwischen Daten, Funktionen und Ressourcen in der Praxis unrealistisch ist. Andererseits wird argumentiert, dass dies insbesondere auf einer Governance- bzw. Berechtigungs-Ebene absolut möglich ist. Auch in UN-Richtlinie Nr. 155 wird diese Unterscheidung angestellt.

Daten: Beim Zugriff auf oder der Bearbeitung von Daten werden darunterliegend bestimmte Funktionen auf entsprechenden Ressourcen ausgeführt. Ein Zugriff auf Funktionen oder Ressourcen wird typischerweise auch Zugriff auf bestimmte Daten beinhalten. Auf der Governance-Ebene ist damit aber typischerweise der lesende Zugriff auf bereits vorhandene Daten gemeint.

Funktionen: Das Ausführen von Funktionen erzeugt Daten regelmäßig zunächst nur im Fahrzeug. Beim externen Zugriff auf Funktionen werden **Daten** an das Fahrzeug übertragen, in Funktionen verarbeitet, und häufig auch zurückgeschickt. Dies wird natürlich auf entsprechender **Hardware** ausgeführt. Ein reiner Funktionszugang beinhaltet jedoch regelmäßig nur den (schreibenden) Zugang zu einer Funktion, nicht zu einer Ressource (Hardware).

Ressourcen: Der Zugriff auf Hardware erfordert Zugriff auf bestimmte **Daten** und **Software**.

Ob sich die Rolle des Datentreuhänders auf die Vermittlung des Zugangs zu Daten, Funktionen und / oder Funktionen beschränkt, wird in diesem Dokument bewusst ausgeklammert. Auch solche könnten im Zugriffsbereich von Datentreuhändern liegen. Daraus ergäben sich unterschiedliche technische und organisatorische Aufgaben. Auch bei einem Datentreuhänder, der ausschließlich Daten weiterleitet, wird irgendjemand Zugriff auf Funktionen und Ressourcen haben müssen – dies könnte z. B. der Fahrzeughersteller sein.

Eine Ferndiagnose und das Auslesen von Daten unter Zwischenschaltung eines Datentreuhänders kann ohne Zugriff auf Ressourcen, aber mit Daten- und Funktionszugriff erfolgen. Hierbei würde natürlich ein **indirekter, mittelbarer** Zugriff -auf Ressourcen nötig sein (die Daten müssen gespeichert und verarbeitet werden – dafür benötigt es Hardware). Dabei sei darauf hingewiesen, dass ein solcher Anspruch auf Direktzugang zu den Ferndiagnosediensten, die von Herstellern sowie Vertragshändlern und -werkstätten genutzt werden, für unabhängige Wirtschaftsakteure nach Art. 61 Abs. 1 Satz 3 Typgenehmigungs-VO besteht.

Abgesehen von einem Lesezugriff auf Daten, der wohl zu großen Teilen über den Data Act abgebildet wird, ist bei anderen Interaktionen mit dem Fahrzeug stets ein Schreibzugriff in bestimm-

ten Bereichen notwendig. Auch bei einem Lesezugriff werden regelmäßig bestimmte Logfiles beschrieben. Deshalb sollte ggf. neben der Unterscheidung Daten / Funktionen / Ressourcen pro Bereich in enger Abstimmung mit dem Fahrzeughersteller die jeweilige Sicherheitsrelevanz von Schreib- und Lesezugriffen berücksichtigt werden. Hier ist das bloße Ausführen (Triggern) von herstellerseitig implementierten Funktionen vom tatsächlich schreibenden (verändernden) Zugriff zu unterscheiden. Bei beidem werden Daten in das Fahrzeug eingebracht. Nach der UN-Richtlinie Nr. 155 verantwortet der Fahrzeughersteller die Cybersicherheit des Fahrzeuges – von der Konzeption bis zur Entsorgung[7]. UN-Richtlinie Nr. 155 gilt unbeschadet von Datenzugriffsrechten berechtigter Parteien,[8] der Data Act wiederum unbeschadet u. a. anwendbarer sektoraler Regeln inkl. solcher zur Cybersicherheit.[9]

3.2 Daten

Es wäre zu klären, welche Definition von »Fahrzeugdaten« genutzt werden soll. Fahrzeugdaten könnten Informationen sein, die der Fahrzeughersteller über das Fahrzeug-Backend verfügbar macht. Fahrzeugdaten könnten aber ebenso sämtliche Informationen sein, die an der Telematiksteuereinheit (Telematik Control Unit – TCU) eines Fahrzeuges zur Verfügung stehen. Auch könnte sich etwa an der Definition von »ohne Weiteres verfügbare Daten« im Data Act orientiert werden. Ebenfalls ist zu klären, inwiefern Daten **über das Fahrzeug** und / oder Daten, die **vom Fahrzeug erzeugt** werden, Teil der Definition wären.

3.3 Funktionen

Eine Funktion könnte grundsätzlich jeder ausführbare Programmcode (Lese- und / oder Schreibzugriff) innerhalb des Fahrzeuges oder außerhalb des Fahrzeuges mit Verbindung zum Fahrzeug sein, oder eine Teilmenge davon. Funktionen, die nur lesend auf Daten zugreifen, sollten von Funktionen, die schreibend (verändernd) auf Daten zugreifen, unterschieden werden.

3.4 Ressourcen

Eine Ressource könnte prinzipiell jedes Hardwareelement sein, das direkt oder indirekt ansteuerbar ist, oder eine Teilmenge davon.

3.5 Akteure

Fahrzeughersteller

»Fahrzeughersteller« wäre wohl der Hersteller gemäß Typgenehmigungs-VO (EU) 2018/858 Artikel 3 (40).

6 Ziff. 7.2.2.1. UN-Richtlinie Nr. 155.
7 Ziff. 1.3. UN-Richtlinie Nr. 155.
8 ErwG. 115 Satz 3 Data Act

Fahrzeugnutzer

Fahrzeugnutzer könnte Fahrzeugeigentümer, Fahrzeughalter, Fahrzeugfahrer, und / oder ein Mitfahrer sein.

Fahrzeugeigentümer

»Fahrzeugeigentümer« könnte die natürliche oder juristische Person sein, in deren Eigentum das Fahrzeug steht. Es könnte zusätzlich auch noch zwischen Eigentümer, Besitzer, Mieter etc. unterschieden werden.

Fahrzeugfahrer bzw. Mitfahrer

»Fahrzeugfahrer« könnte die natürliche Person sein, die das Fahrzeug steuert oder mitfährt.

Fahrzeughalter

»Fahrzeughalter« könnte die natürliche oder juristische Person sein, auf die das Fahrzeug behördlich angemeldet ist.

Datenempfänger

»Datenempfänger« könnte jede natürliche oder juristische Person sein, die im Auftrag des Fahrzeugnutzers oder auf anderer rechtmäßiger Grundlage Daten über einen Datentreuhänder erhält oder erhalten soll (insb. die Fahrzeugnutzenden, Verbrauchende, Unternehmen, öffentliche Stellen). Datenempfänger, die auf Verlangen des Fahrzeugnutzers oder auf anderer rechtmäßiger Grundlage Daten unmittelbar aus dem vernetzten Kraftfahrzeug erhalten, sind nicht Gegenstand dieses Explainers (s. u. Ziff. 3.3).

Unabhängiger Wirtschaftsakteur

Wirtschaftsakteur im Sinne des Art. 3 Nr. 45 der Typgenehmigungs-VO (EU) 2018/858, der einen Anspruch auf Zugang zu den Reparatur- und Wartungsinformationen, sowie Ferndiagnosediensten, die von Herstellern sowie Vertragshändlern und -werkstätten genutzt werden, hat (dazu Ziff. 3.3).

Datentreuhänder

»Datentreuhänder« könnte jede juristische Person iSd Art. 10 ff. DGA (oder darüber hinaus) sein, die mit Zustimmung des Fahrzeugnutzers oder auf anderer rechtmäßiger Grundlage Daten des vernetzten Fahrzeuges erhält und Datenempfängern auf Verlangen des Datenhalters zur Verfügung stellt.

Datenbereitsteller

Je nach Berechtigung zur Datenfreigabe könnten dies Fahrzeugnutzer, Fahrzeughersteller und Anbieter von Diensten, die Daten bzw. Informationen im Zusammenhang mit der Nutzung eines Kraftfahrzeugs erheben, sein.

4 Mögliche Aufgaben von Datentreuhändern

4.1 Allgemein

Im Folgenden werden mögliche Ausgestaltungsfragen für den Einsatz von Datentreuhändern für den Zugriff auf Daten skizziert. **Dabei wird das Thema Ressourcen und Funktionen ausgeklammert. Auch solche könnten im Zugriffsbereich von Datentreuhändern liegen.** Insofern ein Datentreuhänder einen Datenvermittlungsdienst unter dem Data Governance Act dargestellt, wird dadurch sichergestellt, dass der Datentreuhänder als neutraler Administrator und unabhängige dritte Stelle agiert. Wie durch Primärrecht (AEUV 101) grundsätzlich erforderlich, muss in jedem Fall sichergestellt sein, dass Kunden- und Geschäftsdaten unabhängiger Drittanbieter nicht im Zugriff eines Wettbewerbers sind und genutzt werden können.

Betrieb der nötigen Dateninfrastruktur

Je nach Umfang und Ausgestaltung des Datentreuhänders wäre zu klären, welche technisch-organisatorische Infrastruktur notwendig ist und wer diese vorhält.

Identifikation der beteiligten Akteure und Validierung ihrer Zugangsberechtigung (IAM)

Der Datentreuhänder könnte (akkreditierte) Identitäten für die Beteiligten vergeben und validieren und den Zugang von Datenempfängern auf die dem Datentreuhänder vorliegenden Daten gegen entsprechende Zugangsregeln freigeben.

Darüber hinaus muss ein Datentreuhänder sicherstellen, dass Fahrzeugeigentümer bzw. Fahrzeugfahrer oder die vom Fahrzeugeigentümer ausgewählten Dienstleister durch den Fahrzeughersteller nicht kontrolliert werden und diesem nicht bekannt sind.

Einholung notwendiger Zustimmungen, ggf. unter Berücksichtigung DS-GVO, BDSG, TT-DSG, DGA, DA etc.

Datentreuhänder könnten Fahrzeugnutzern jederzeit und im eigenen Geschäftsgebiet die Selbstverwaltung ihrer Daten ermöglichen, und ihnen die Möglichkeit geben, zu kontrollieren, wer wann auf die über den Datentreuhänder freigeschalteten Daten zugreifen kann.

Beispielsweise könnten Datentreuhänder Fahrzeugnutzern erlauben, ihre Daten selbst zu monetarisieren und sie zum Zwecke von Angebotsanfragen, bzw. Preisvergleichen an Dritte weiterzugeben.

Zu klären wäre insbesondere:

- Handelt es sich um personenbezogene Daten oder nicht?
- Welche Verarbeitungsgrundlage ist erforderlich?
- Inwiefern ist eine Zweckbindung notwendig?
- Bei Einwilligung: darf broad consent eingeholt werden (und was heißt das konkret)?
- Für Zugriff durch Supportmitarbeitende o. Ä. des Treuhänders wäre zu klären, ob immer eine Einwilligung des Datenhalters vorliegen müsste.

Festlegung und Durchsetzung von Qualitätsanforderungen bzw. SLAs etwa zu Safety, Security, Privacy, Integrity

Es besteht Einigkeit, dass die Sicherheit von Fahrzeug, Verkehrsgeschehen und Fahrzeuginsassen an oberster Stelle steht. Hierbei sind insb. die Bereiche Safety (physische Sicherheit), Security (Daten- und Informationssicherheit), Privacy (Datenschutz) sowie die Integrität der Verarbeitungslogik und -inhalte der entsprechenden Systeme relevant. Nicht minder wichtig ist die Datensouveränität des Fahrzeugnutzers sowie der gleichberechtigte Datenzugang für alle Marktteilnehmer, wo immer rechtlich möglich.

Der Fahrzeughersteller bliebe nach UN-Richtlinie Nr. 155 für die Cybersicherheit des Fahrzeugs über den gesamten Lebenszyklus verantwortlich. Vor dem Hintergrund wäre zu klären, ob und wie ein Zugriff durch Datentreuhänder ausgestaltet werden könnte. Sollte kein bereits etablierter Zugriffsmechanismus genutzt werden, dann müssten Haftung, Absicherung etc. durch den Datentreuhänder im Rahmen des Zivilrechts für den gesamten Lebenszyklus übernommen werden.

Auch mit derartigen Anforderungen bzw. Agreements und vor dem Hintergrund der grundsätzlich anzunehmenden Vertrauenswürdigkeit von Zuliefererbetrieben, Prüforganisationen, Werkstätten, Automobilclubs, Pannendiensten, Versicherungsunternehmen und bestimmten weiteren Dritten gälte es dennoch zu klären, wie im – nie auszuschließenden – Fall eines Schadensereignisses mit Haftungsfragen umgegangen würde. Dabei ist zu beachten, dass ein Schadensfall durch Beeinträchtigung der Fahrzeugsicherheit nicht das naheliegendste Szenario ist, wenn bloß mittelbar über einen Datentreuhänder Daten über zu dem Zeitpunkt etablierte Zugriffsmechanismen gelesen werden und gar kein Funktions- oder Ressourcenzugriff stattfindet.

Wer würde das Risiko tragen, wenn ein Zugang auf das Fahrzeug dennoch zu einem Verstoß gegen Gesetze und Rechtsverordnungen führt?

Wie würde der Zustand adressiert, dass ein »Fehler« des Fahrzeugs aus Fahrzeugnutzersicht wohl typischerweise dem Fahrzeughersteller angelastet wird, selbst wenn dieser pflichtgemäß gehandelt hat (Reputationsschaden)?

Es wäre zu klären, ob bzw. inwiefern eine separate Zulassung von Datentreuhändern, Hardware oder Software über die Typgenehmigungs-VO möglich wäre, um die Haftung nicht (unverschuldeterweise) dem Fahrzeughersteller aufzutragen. Haftungsfragen zwischen Datentreuhänder und anderen Akteuren könnten im Rahmen einer Vertragsverhandlung inklusive Datenschutzkonzept und Haftungsparagrafen geklärt werden.

Es wäre zu klären, ob ein Datentreuhänder a) die vorgegebenen Datenverarbeitungsregeln wie ein Auftragsverarbeiter umsetzt, in bestimmten engen Fällen (z. B. bei der Herausgabe der Pseudonyme) dem Auftraggeber, sei es der Dateninhaber oder der Datenempfänger, gegenüber jedoch nicht weisungsgebunden ist, oder b) selbst (gemeinsamer) Verantwortlicher mit dem Dateninhaber oder der Datenempfänger für die Datenverarbeitung ist. In jedem Fall könnten Datentreuhänder zumindest eine Mitverantwortung für die ordnungsgemäße Verarbeitung und Übermittlung der Daten tragen. Dies beträfe etwa Fragen der Datensicherheit oder der rechtmäßigen Verarbeitung. Transparenz über Leistungsgegenstände und Konditionen (Stichwort Vergleichbarkeit) für Akteure sollte der Regelfall sein.

4.2 Kernumfang der Aktivitäten (Worauf wird zugegriffen?)

Es wäre zu klären, ob sich die Funktion von Datentreuhändern auf das Matchmaking zwischen Akteuren (1:1; 1:n; n:m), oder nur die Verbindung von bereits „gematchten“ Akteuren bezieht. Bei bilateralen Verbindungen könnte das Pooling unterschiedlicher Datensätze eines einzelnen Datenbereitstellers eine Rolle spielen (z. B. Verlaufsdaten). Bei multilateralen Verbindungen (1:n, n:m) könnte wiederum auch das Pooling von Datensätzen unterschiedlicher Datenbereitsteller eine Rolle spielen.

Es wäre zu klären, durch welche Akteure Auswahl und Beauftragung von Datentreuhändern erfolgt.

4.3 Zwischenspeicherung von Daten

Alleinig beim Direktzugriff auf Daten nach Etablierung eines Kommunikationskanals zwischen Fahrzeughersteller bzw. Fahrzeugnutzer und Datenempfänger (in-situ data access oder Transfer) könnte auf eine Zwischenspeicherung der Daten beim Datentreuhänder verzichtet werden (»dezentraler Aufbau«). Einen solchen Anspruch auf Direktzugang zu den Ferndiagnosediensten, die von Herstellern sowie Vertragshändlern und -werkstätten genutzt werden, haben aktuell unabhängige Wirtschaftsakteure nach Art. 61 Abs. 1 Satz 3 Typgenehmigungs-VO.

Das Transferieren von Daten könnte u. a. sog. compute-to-data-Ansätze (»in-situ data access«) umfassen. Dabei würde, vereinfacht gesagt, ein Algorithmus unter Kontrolle des Datentreuhänders ausgeführt. Dabei hätte der Datenempfänger keinen Zugriff auf die Daten, sondern nur auf die Ergebnisse der Ausführung des Algorithmus. Eine Zwischenspeicherung wäre je nach Speicherort der Daten (Datenbereitsteller, Datentreuhänder) optional.

Neben dem »reinen« Transferieren von Daten wären unterschiedliche weitere Verarbeitungsmöglichkeiten denkbar, insb. Filterung, Aggregation, Sortierung, Gruppierung, Konvertierung / Formatierung von Daten. Dabei wäre regelmäßig eine Zwischenspeicherung der Daten durch den Datentreuhänder notwendig (»zentraler Aufbau«):

- Zusammenführung unterschiedlicher Datensätze ggf. unterschiedlicher Herkunft, ggf. Reduktion / Zusammenführung von Schnittstellen,
- Überwachung und Sicherstellung der Einhaltung von Qualitätsanforderungen
- Treffen von Aussagen über Datenqualität
- Bearbeitung, Formatierung und Harmonisierung von Daten
- Pseudonymisierung und / oder Anonymisierung von Daten, und / oder
- Anbietung von compute-to-data Verfahren

Bei der Anonymisierung von Daten kann es zu einem Zielkonflikt kommen, wenn anonymisierte Daten ex-post nicht mehr miteinander verknüpfbar wären (Daten im Zeitverlauf könnten nicht mehr einem einzelnen Fahrzeugnutzer zugeordnet werden).

4.4 Bezug zu anderen Konzepten

Dieses Dokument unternimmt nicht den Versuch, das Konzept eines Datentreuhänders abschließend zu definieren, sondern höchstens, sich einer Definition sehr grob anzunähern. Hierbei sind Zweck und Funktionalität viel wichtiger als die scharfe Abgrenzung von anderen Konzepten. Dennoch muss das Konzept eines Datentreuhänders – das Gegenstand dieses Papers ist – so gut wie möglich zu den Konzepten **Datenraum** und **Datenvermittlungsdienst** in Bezug gesetzt werden. Im Kontext unterschiedlicher Begriffsverständnisse[10] scheint es am sinnvollsten, auf die europarechtliche Definition Bezug zu nehmen. Demnach handelt es sich bei:

Datenräumen »um zweck- oder sektorspezifische oder sektorübergreifende interoperable Rahmen für gemeinsame Normen und Verfahren für die Weitergabe oder die gemeinsame Verarbeitung von Daten – unter anderem für die Entwicklung neuer Produkte und Dienste, wissenschaftliche Forschung oder Initiativen der Zivilgesellschaft«[11] und bei einem

9 Für Kritik zur Definitionsvielfalt des Konzepts **Datenraum** siehe Bitkom, 2022, Datenräume und Datenökosysteme – Erste Einordnung und aktueller Stand, 2022, S. 5.
Der Begriff **Datenvermittlungsdienst** wurde unserem Vernehmen nach vor dem Gesetzgebungsverfahren zum Data Governance Act nicht (mit breiter Zustimmung) definiert.

10 Art. 33 (1) S. 1 Data Act

Datenvermittlungsdienst um »einen Dienst, mit dem 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 [abzüglich bestimmter Ausnahmen]«[12]

Wie in Bezug auf Datenvermittlungsdienste schon in 1.4 angesprochen, ist es denkbar, dass ein Datentreuhänder gleichzeitig einen Datenvermittlungsdienst nach DGA darstellt. Ebenso ist es denkbar, dass ein Datentreuhänder einen Datenraum nach Data Act darstellt.

11 Art. 2 (11) Data Governance Act

5 Struktur und Organisation von Datentreuhändern

Datentreuhänder müssen u. a. die Anforderungen an die rechtliche, organisatorische und finanzielle Unabhängigkeit nach Art. 12 Data Governance Act erfüllen, falls sie Datenvermittlungsdienste im Sinne des DGA[13] erbringen. Ebenso müssen Lock-in-Effekte vermieden werden – dies adressiert der DGA teilweise durch seine Neutralitätspflichten für Betreiber von Datenvermittlungsdiensten. Um die Wahlfreiheit aller Parteien nicht einzuschränken, darf keine Monopolstellung eines einzelnen Datentreuhänders entstehen. Demnach wären mehrere private, beliehene und / oder staatliche Stellen wichtig.

Es wäre zu klären, ob sich Datentreuhänder durch ihre Tätigkeit und die daraus resultierenden Geschäftsmodelle selbst tragen sollten und nicht (dauerhaft) durch staatliche Investitionen gefördert werden sollten.

12 Art. 2 (11) i.V.m. Art. 10 Data Governance Act

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org