

14.10.2024

ETA-POSITION ZUM DATENTREUHÄNDER

Executive Summary

Fahrzeugdaten sind Treiber für technologische Innovationen und darauf aufbauende neue Geschäftsmodelle. Sie sind zudem die Basis, um Beziehungen auszugestalten – zwischen Kundinnen und Kunden, Fahrzeugherstellern, Zulieferern und Dritten, die Services und Geschäftsmodelle rund um die Fahrzeuge anbieten. Der Europäische Data Act und eine mögliche sektorale Regulierung auf europäischer Ebene sollen die Datenverfügbarkeit und die Nutzung von Daten erhöhen. Auf nationaler Ebene nennt der Koalitionsvertrag von 2021 Datentreuhändermodelle als Möglichkeit, eine wettbewerbsneutrale Nutzung von Fahrzeugdaten zu garantieren. Gleichzeitig berücksichtigen sie die Zugriffsbedürfnisse von Nutzenden, privaten Anbietern und staatlichen Organen, aber auch die Interessen der betroffenen Unternehmen und Entwickler.

Dieses Positionspapier gibt Empfehlungen für Datentreuhändermodelle mit Bezug auf Fahrzeugdaten. Sollten für Datentreuhändermodelle für Fahrzeugdaten regulatorische Vorgaben festgelegt werden, empfiehlt der ETA diese Empfehlungen bei der Gestaltung einer möglichen Regulierung zu berücksichtigen.

Die Empfehlungen beziehen sich überwiegend auf Datentreuhändermodelle innerhalb von regulatorischen Vorgaben. Ergänzend gibt der ETA Empfehlungen, um Datentreuhändermodelle zwischen Vertragsparteien im privatwirtschaftlichen Rahmen auszugestalten. Sie bieten sich auch als Referenz für mögliche regulatorische Vorgaben für Datentreuhändermodelle in anderen Sektoren an.

Diese Position basiert auf dem ETA-Kurzpapier zur Ausgestaltung einer möglichen sektoralen Regulierung für den Zugriff auf Fahrzeugdaten, Funktionen und Ressourcen. Hier hat der ETA Empfehlungen für Aufgaben, Ziele und Umsetzungsoptionen erarbeitet.

Die Aufgaben von Datentreuhändern sollten sich nur auf das Lesen von Daten beziehen, nicht jedoch auf die Aktivierung und Nutzung von Funktionen und Ressourcen der Fahrzeuge und Dienste. Privatwirtschaftlich sind weitere Ausgestaltungen im gegenseitigen Einvernehmen der Vertragsparteien denkbar. Diese adressiert das Papier nicht. Der ETA empfiehlt allerdings, die Ausgestaltungsfreiheit für privatwirtschaftliche Datentreuhändermodelle nicht einzuschränken.

Ein Datentreuhändermodell muss den datenschutzrechtlichen Vorgaben, insbesondere der Datenschutzgrundverordnung (DSGVO), entsprechen und die Datensouveränität des Nutzers sicherstellen.

Zentrale Punkte

1. Datentreuhändermodelle sollen folgende Aufgaben erfüllen¹:
 - Absicherung Integrität: Niemand kann Daten unbemerkt manipulieren.
 - Absicherung Non-Repudiation: Ein Nachweis über den Ursprung der Daten liegt vor.
 - Absicherung Vertraulichkeit: Daten sind vor unberechtigtem Zugriff geschützt.
 - Absicherung Datenlöschung gem. DSGVO: Auditierung der Löschung

Die oben beschriebenen Aufgaben eines Datentreuhändermodells können heute bereits über vorhandene technische Lösungen erfüllt werden.

Datentreuhändermodelle sollten keine Datenspeicherung beim Treuhänder vorsehen, um Redundanzen und Vorratsdatenspeicherung zu vermeiden. Die Speicherung der Daten sollte beim Datenhalter verbleiben.

Die Aufgaben des Datentreuhänders können bei der „Absicherung Vertraulichkeit“ sowohl eine Anonymisierung des Datennachfragers als auch eine Absicherung des Non-Monitorings der Geschäftstätigkeit des Datennachfragers beinhalten.

2. Anwendungsfälle für Datentreuhändermodelle sind im Bereich hoheitlicher Aufgaben sowie im privatwirtschaftlichen Umfeld denkbar. Um die Nutzung eines Datentreuhändermodells zu begründen, könnte unter anderem eine konkrete, nicht anders adressierbare Notwendigkeit oder der explizite Wunsch der Nutzenden Grundlage sein.
3. Datentreuhändermodelle sollen für diese Anwendungsfälle als neutrale dritte Instanz agieren und dabei etablierte Datenzugriffsmöglichkeiten wie das Extended Vehicle/Backend nutzen. Voraussetzung dafür ist immer, dass der Fahrzeugnutzende seine Zustimmung zu diesem Datenzugriff gibt. Ein direkter Zugriff auf Fahrzeuge ist insbesondere aus Gründen der Cybersecurity nicht zu empfehlen.
4. Privatwirtschaftliche Unternehmen oder öffentlich-rechtliche Gesellschaften sollten diese Aufgaben im Datentreuhändermodell nur umsetzen, wenn es für diese Institutionen klare Aufgaben und Verantwortlichkeiten gibt und sie einen konkreten Mehrwert erzeugen.
5. Eine generelle Anwendung von Datentreuhändermodellen im Datenaustausch würde zu erhöhten Kosten, Ineffizienzen und aufwendigen Prozessen führen, wodurch die Datennutzung und neue datenbasierte Geschäftsmodelle erschwert würden.
6. Für Datentreuhändermodelle sollte ausgeschlossen sein, dass sie mit den Daten, die sie treuhänderisch verwalten, darüber hinaus ein Geschäftsmodell betreiben.
7. Die Umsetzung und der Betrieb von Datentreuhändermodellen sollten über den damit generierten Mehrwert finanziert werden. Dieser Mehrwert sollte sich in entsprechenden Nutzungsentgelten für die Services eines Datentreuhändermodells widerspiegeln. Eine öffentliche Finanzierung von Datentreuhändermodellen ist in Betracht zu ziehen, wenn auch der Auftraggeber öffentlich ist.
8. Datentreuhänder können als Akteure im Interesse der Nutzenden auf Datenmarktplätzen agieren: Sie können ihre Services und Daten über Datenmarktplätze anbieten.
9. Im Sinne von Qualität und Effizienz sollten mehrere Datentreuhänder im Wettbewerb anbieten können.

¹ Endkunden können Transparenz über verfügbare Daten auf zwei Wege erlangen: gem. DSGVO, die eine Auskunftspflicht für persönliche Daten absichert, und ab Umsetzung des Data Act, der Transparenz über die verfügbaren Daten einfordert.

Relevante regulatorische Vorgaben und ETA-Kurzpapiere, die den Rahmen für die ETA-Position zum Datentreuhänder bilden

Datenschutzgrundverordnung: Die DSGVO sichert den Schutz persönlicher Daten mit ihren Rechtsgrundsätzen ab (Rechtmäßigkeit der Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit der Daten, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht).

Data Governance Act: Der DGA zielt auf einen vertrauenswürdigen Datenaustausch ab, u. a. indem er neutrale Datenintermediäre etabliert, die Einzelpersonen und Unternehmen mit Datennutzenden verbinden. Diese Datenvermittler können die Daten nicht für eigene Geschäftsmodelle verwenden.

Data Act: Der DA erhöht die Datenverfügbarkeit in Europa, u. a. indem den Nutzenden und berechtigten Dritten Daten bereitgestellt werden müssen, die durch die Nutzung von vernetzten Gegenständen entstehen. Nutzende von vernetzten Gegenständen können somit am Mehrwert der erzeugten Daten partizipieren.

„Access to in-vehicle data, resources and functions“ (sektorale Regulierung): Es wird erwartet, dass dieser Regulierungsentwurf festlegen wird, wie Dritte auf Daten, Funktionen und Ressourcen von Fahrzeugen zugreifen können – in Ergänzung zum Data Act.

Das **ETA-Kurzpapier „Potenziale der Datenstrategie für die Transformation der Automobilwirtschaft nutzen“** zeigt Potentiale und Handlungsfelder auf, die Verfügbarkeit und Qualität von Daten zu erhöhen.

Das **ETA-Kurzpapier „Handlungsempfehlungen zur Erhöhung der Datennutzung und für die Umsetzung einer möglichen sektoralen Regulierung“** gibt konkrete Empfehlungen, um den Zugriff auf Daten, Funktionen und Ressourcen von Fahrzeugen auszugestalten und die Datennutzung zu erhöhen.

1 Bedarf an Datentreuhändermodellen

Der Koalitionsvertrag sieht eine wettbewerbsneutrale Nutzung von Daten vor: Entsprechende Treuhänder-Modelle sollen die Zugriffsbedürfnisse der Nutzenden, privater Anbieter und staatlicher Organe sowie die Interessen betroffener Unternehmen und Entwickler angemessen berücksichtigen.

Mit „Zugriff“ ist dabei der lesende Zugriff auf Daten gemeint, die von Fahrzeugen oder zugehörigen Diensten generiert werden, nicht die Aktivierung oder Steuerung von Funktionen oder Ressourcen.

Im automobilen Umfeld ist ein Datentreuhändermodell eine von mehreren möglichen Lösungen, um den Zugriff auf solche Daten zu regeln. In bestimmten Fällen kann der Einsatz eines Datentreuhänders die richtige Wahl sein, zum Beispiel, wenn bei der Datennutzung zwischen Original Equipment Manufacturer (OEMs), Zulieferern, Anbietern von Dienstleistungen und Nutzenden Interessenwidersprüche bestehen. Solche Anwendungsfälle sind beispielsweise im steuerrechtlichen Bereich, bei Finanzierungen, im Flottenmanagement (Dienstwagen, Carsharing, Rental Car ...) oder im Bereich des automatisierten Fahrens denkbar.

Datentreuhändermodellen sind immer dann notwendig, wenn es Interessenkonflikte der beteiligten Parteien gibt und sich diese Transparenz bei gleichzeitiger Vertraulichkeit wünschen (vergleichbar mit dem Benchmarking-Prozess unter Wettbewerbern). Im automobilen Umfeld zeichnen sich diese Parteien dadurch aus, dass auf einer Seite Daten erzeugt und gehalten werden, während auf der anderen Seite Daten benötigt werden, um ergänzend oder im Wettbewerb Produkte und Dienstleistungen anzubieten.

Zusätzlich können Anwendungsfälle auch im hoheitlichen Bereich liegen. In solchen Fällen könnte der Einsatz von Datentreuhändern regulatorisch vorgegeben sein.

Alternativ ist die optionale Nutzung von Datentreuhändermodellen denkbar, die dann aber regulatorisch eingeräumt und durchsetzbar sein sollte.

Eine grundsätzliche Anwendung von Datentreuhändermodellen für alle Datenzugriffe sollte nicht umgesetzt werden, da die Einbindung eines weiteren Akteurs zwischen Datenquelle und Datennutzenden die Prozesse komplexer und ineffizienter macht. Es würden zusätzliche Kosten entstehen und Prozesse langsamer werden, im Vergleich zu einer Datenfreigabe direkt an der Datenquelle zum Datennachfragenden.

2 Aufgaben von Datentreuhändermodellen

Um die gegenläufigen Interessen und den Wunsch nach Transparenz bei gleichzeitiger Vertraulichkeit zu adressieren, sollten Datentreuhändermodelle folgende Aufgaben adressieren:

- Absicherung Integrität: Niemand kann Daten unbemerkt manipulieren.
- Absicherung Non-Repudiation: Ein Nachweis über den Ursprung der Daten liegt vor.
- Absicherung Vertraulichkeit: Daten sind vor unberechtigtem Zugriff geschützt.
- Absicherung Datenlöschung gem. DSGVO: Auditierung der Löschung

Die Aufgaben von Datentreuhändern sollten sich nur auf das Lesen von Daten beziehen, nicht jedoch auf die Aktivierung und Nutzung von Funktionen und Ressourcen der Fahrzeuge und Dienste.

Bei der Absicherung der Vertraulichkeit ist es nicht notwendig, dass Datennachfrager ihr Geschäftsmodell offenlegen müssen, weder gegenüber dem Datentreuhänder, noch gegenüber dem Datenhalter.

Auch kann der Datentreuhänder bei der Absicherung der Vertraulichkeit bei Bedarf eine Anonymisierung des Datennachfragers gegenüber dem Datenhalter anbieten, so dass ein Non-Monitoring bezüglich der Aktivitäten des Datennachfragers durch den Datenhalter abgesichert wird.

Die oben beschriebenen Aufgaben eines Datentreuhändermodells können heute bereits über vorhandene technische Lösungen erfüllt werden.

Datentreuhändermodelle sollten keine Datenspeicherung beim Treuhänder vorsehen, um Redundanzen und Vorratsdatenspeicherung zu vermeiden. Die Speicherung der Daten sollte grundsätzlich auch bei Anwendung von Datentreuhändermodellen beim ursprünglichen Datenhalter verbleiben.

Ein Datentreuhändermodell muss den datenschutzrechtlichen Vorgaben, insbesondere der Datenschutzgrundverordnung (DSGVO), entsprechen und die Datensouveränität des Nutzers sicherstellen.

3 Umsetzung von Datentreuhändermodellen

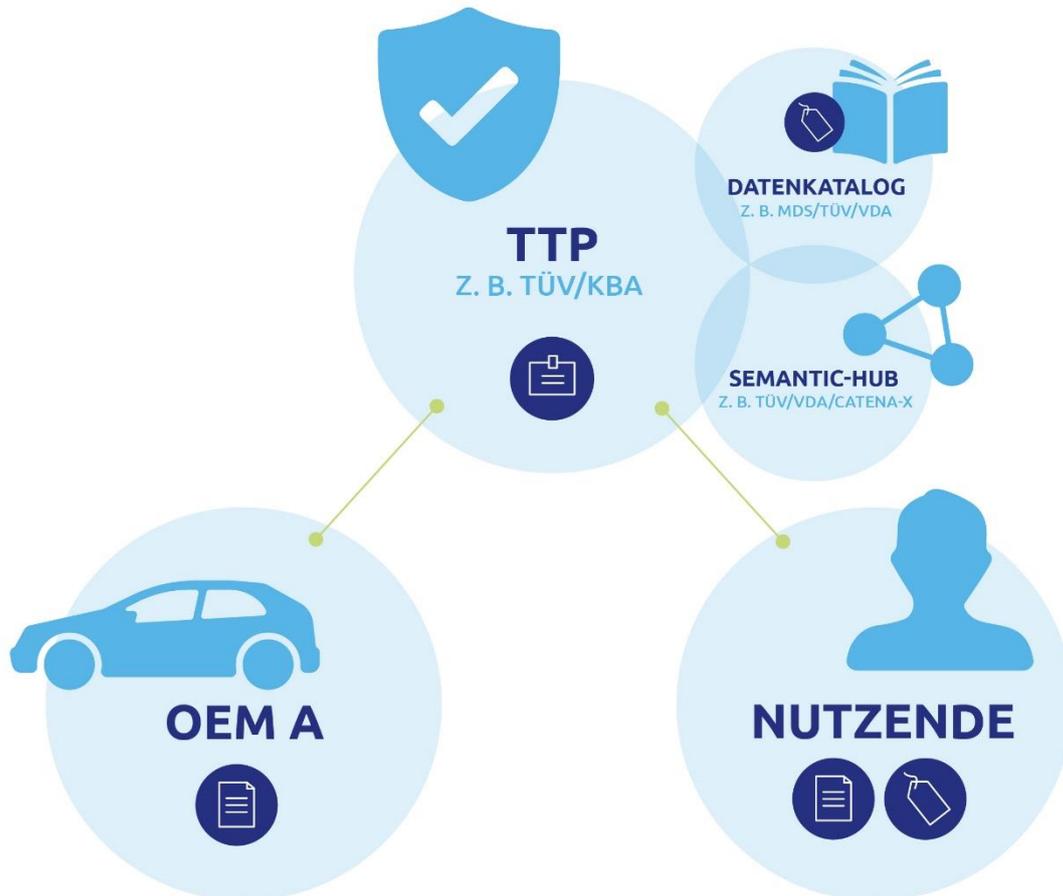
Im Koalitionsvertrag ist vorgesehen, dass ein Dateninstitut Datentreuhändermodelle etablieren soll. Es soll sich darauf fokussieren, die Anforderungen aus den Anwendungsfällen umzusetzen. Idealerweise nutzt es etablierte Lösungen und Technologien.

Der Zugriff auf die benötigten Fahrzeugdaten sollte immer über das Backend der Hersteller erfolgen, da hier bestehende Lösungen genutzt werden können, die die Systemintegrität und die Cybersecurity der Fahrzeuge nicht gefährden und nachweislich zuverlässig funktionieren.

Ein direkter Zugriff auf Fahrzeuge ist keine Option. Die Gründe sind Cybersecurity, Datenschutz, Komplexität der technischen Anforderungen und die einhergehende Systemintegrität sowie die Kosten für Datenzugriff und -übertragung.

Die genannten Anforderungen an Datentreuhändermodelle, nämlich Integrität, Non-Repudiation und Vertraulichkeit der Daten lassen sich über bestehende technische Lösungen heute bereits erfüllen: Eine verteilte Speicherung eindeutiger kryptografischer IDs (Hash) stellt sicher, dass die Daten nicht manipuliert wurden. Die Nutzenden stimmen dem Zugriff im Fahrzeug zu. Das stellt sicher, dass nur die berechtigten Nutzenden die Daten freigeben können. Dafür können die etablierten und vor Zugriff von Dritten abgesicherten Prozesse zur Freigabe von Daten im Fahrzeug genutzt werden. Konnektoren stellen sicher, dass nur die berechtigten Personen auf die Daten zugreifen. Datenverschlüsselung und Zertifikate zur Entschlüsselung erhöhen die Vertraulichkeit der Daten.

ARCHITEKTUR



OEM A kann beweisen, dass die Daten das Original sind.

Die TTP kann bestätigen, dass OEM A die Daten nicht manipuliert hat.

-  Datensatz
-  Metadaten des Datensatzes
-  eindeutige kryptografische ID (Hash)

Abbildung 1: Beispielhafte Architektur zur Umsetzung der Anforderungen (Quelle: ZF Friedrichshafen AG)
 TTP: Trusted third party (vertrauenswürdige Dritte)
 TÜV: Technischer Überwachungsverein
 KBA: Kraftfahrt-Bundesamt
 MDS: Mobility Data Space
 VDA: Verband der Automobilindustrie e. V.

Eine Alternative wäre die Nutzung von offenen, lock-in-freien Technologien. So können beispielsweise regelmäßig Kilometerstände abgespeichert werden. Berechtigte Nutzende können über geeignete für jeden zugängliche, dezentrale Marktplätze darauf zugreifen.

Datentreuhändermodelle werden durch Neutralität sowie transparente und nachvollziehbare Prozesse vertrauenswürdig. Die beschriebenen Lösungen „by technology“ erhalten ihre Vertrauenswürdigkeit durch Zertifizierung. Eine solche Zertifizierung könnte beispielsweise durch das Dateninstitut erfolgen. Das macht eine laufende Auditierung überflüssig.

4 Finanzierung des Datentreuhändermodells

Das Datentreuhändermodell adressiert konkrete Anforderungen an Daten aus Anwendungsfällen: Datennutzende erhalten einen Mehrwert durch die Umsetzung der Aufgaben eines Datentreuhändermodells. Dieser Mehrwert sollte durch ein Entgelt für die Nutzung des Datentreuhändermodells abgegolten werden.

Die Anbieter von Datentreuhändermodellen sollten in der Lage sein, die anfallenden Kosten von Beauftragenden einzufordern, zuzüglich einer angemessenen Gewinnmarge.

Eine finanzielle Absicherung des Datentreuhändermodells durch die öffentliche Hand sollte in Betracht gezogen werden, wenn ein Auftraggeber aus dem öffentlichen Bereich kommt und die Beauftragung der Erfüllung hoheitlicher Aufgaben dient.

5 Zusammenspiel mit anderen Datenmarktteilnehmern

Datentreuhändermodelle können in existierende Datenmarktplätze eingebunden werden. So wäre eine Integration in die Mobiltheke/National Access Point (NAP) oder den Mobility Data Space (MDS) vorstellbar. Der NAP bzw. MDS bietet dabei die Transparenz der verfügbaren Daten und bringt Anbieter und Nachfrager zusammen. In die existierenden technischen Lösungen zum Datenaustausch können Funktionalitäten eingebunden werden, die die Aufgaben der Datentreuhändermodelle erfüllen. Somit könnte der NAP bzw. MDS die Aufgaben als zusätzlichen Service für die Marktplatzteilnehmer anbieten. Auch über neutrale Server kann die Erfüllung der Aufgaben der Datentreuhändermodelle angeboten werden. Hier ist der zusätzliche Service möglich, dass der Datenempfänger nicht gegenüber dem Datenhalter offengelegt wird.

Die Einbindung in existierende Datenmarktplätze ist jedoch keine Voraussetzung für die Umsetzung eines Datentreuhändermodells, da OEMs heute bereits direkt in Datenmarktplätze wie MDS eingebunden sind.

6 Empfehlung

- Klare Festlegung der Funktionen von Datentreuhändermodellen, die im Rahmen der datenschutzrechtlichen-Regelungen erfüllt werden
- Umsetzung von Datentreuhändermodellen im privatwirtschaftlichen Bereich nicht flächendeckend und verpflichtend, sondern als buchbarer Mehrwertdienst für Anforderer wie Flottenmanager etc.
- Klare Vereinbarung, dass sich die Aufgaben von Datentreuhändern nur auf das Lesen von Daten beziehen sollten, nicht jedoch auf die Aktivierung und Nutzung von Funktionen und Ressourcen der Fahrzeuge und Dienste

Über den Expertenkreis

Der Expertenkreis Transformation der Automobilwirtschaft (ETA) ist ein unabhängiges Beratungsgremium des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK). Der Expertenkreis entwickelt ziel- und adressatenorientierte Handlungsempfehlungen an die Politik, die Wirtschaft und die Gesellschaft, mit deren Hilfe der langfristige Strukturwandel der Branche erfolgreich gestaltet werden kann. Übergeordnetes Ziel ist es, Klimaneutralität zu erreichen sowie Wertschöpfung, Arbeits- und Ausbildungsplätze am Automobilstandort Deutschland zu sichern.

Der ETA besteht aus 13 Personen aus Wissenschaft, Wirtschaft und Gesellschaft, die von Bundesminister Dr. Robert Habeck für die 20. Legislaturperiode berufen wurden. Über flexible und agil operierende Arbeitsformate sind weitere Sachverständige sowie relevante Institutionen und Stakeholder in die Arbeit des ETA eingebunden. Die Mitglieder erhalten keine Vergütung oder Aufwandsentschädigung für ihre Mitwirkung im ETA. Der Expertenkreis wird durch eine vom BMWK beauftragte Prozessbegleitung und wissenschaftliche Begleitung unterstützt. Der ETA hat mit dem Expertenbeirat Klimaschutz in der Mobilität (EKM) ein Schwestergremium beim Bundesministerium für Digitales und Verkehr (BMDV). Beide Gremien sind in die Strategieplattform Transformation der Automobil- und Mobilitätswirtschaft (STAM) der Bundesregierung eingebunden.

Für die Inhalte ist der ETA verantwortlich. Er entwickelt Stellungnahmen, Positionspapiere und Berichte teilweise in seinen Arbeitsgruppen, berät und beschließt sie anschließend im Plenum und veröffentlicht sie dann in eigener Verantwortung.

IMPRESSUM

VERFASSER: Expertenkreis Transformation der Automobilwirtschaft (ETA), Reinhardtstraße 58, 10117 Berlin | <https://expertenkreis-automobilwirtschaft.de/>

HERAUSGEBER: Bundesministerium für Wirtschaft und Klimaschutz (BMWK)