Verband der TÜV e.V.

TÜV®

Datum
17. Nov. 2017

Datenschutz, IT-Security & Compliance als Basis für neue Geschäftsmodelle in der digital vernetzten Mobilität

Stellungnahme zur Fachkonsultation des BMVI ‚Eigentumsordnung' für Mobilitätsdaten

Zusammenfassung

Mit der im August 2017 veröffentlichten Studie „Eigentumsordnung für Mobilitätsdaten?" hat das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) einen wichtigen industriepolitischen Diskussionsbeitrag geleistet. Daten stellen ein Wirtschaftsgut dar, für deren Nutzung rechtliche und ökonomische Rahmenbedingungen geschaffen werden müssen.

Das moderne Automobil ist nicht länger nur Hardware, sondern vielmehr eine Komponente eines digital vernetzten Systems. Die Frage nach der besten und aktuellsten Software für die jeweiligen Fahrzeugkomponenten über den gesamten Fahrzeuglebenszyklus wird eine entscheidende Rolle für die Sicherheit des Automobils und die Gestaltung des Mobilitätsmarkts spielen. Durch die Vernetzung von Fahrzeugen und Fahrzeugen mit der Infrastruktur sind neue Dienstleistungen möglich, die das Potential haben, den Dienstleistungsmarkt im Bereich Automotive weitreichend zu verändern. Hierauf richtet die vorliegende Studie ihr primäres Augenmerk.

Aus Sicht des Verbands der TÜV e.V. erfordert der Schutz der persönlichen Daten sowie der Schutz vor Cyberattacken besondere Security-Anforderungen für Fahrzeuge, die bereits während der Entwicklung sowohl im Auto auch als in dem damit verbundenen System betrachtet und realisiert werden müssen (Security & Privacy by Design). Die Studie berücksichtigt nur ansatzweise, dass erst eine umfassende sicherheitsrelevante Betrachtung und Bewertung datenbasierter Mobilitätsdienste und digitale Funktionalitäten im Fahrzeug, das notwendige Vertrauen und die Akzeptanz in der Automobilbranche zwischen Hersteller, Zulieferer und Aftermarket sowie in der Bevölkerung schaffen.

Ziel politischen Handelns sollte es sein, Lösungen zu forcieren, die einen möglichst großen und wettbewerbsoffenen Mobilitätmarkt etablieren, in dem alle Dienstleister und Drittanbieter eine gleichwertige, angemessene und diskriminierungsfreie Ausgangslage haben. Erstens können sie so den jeweiligen Anwendern ihre digitalen Dienste im Fahrzeug sicher und datenschutzkonform anbieten. Zweitens kann sich so eine hohe Innovationskraft entfalten und Verbraucherschutz in den Bereichen Automotive und Mobility gewährleistet werden.

Datenschutz, IT-Sicherheit, Nutzerkomfort und Wettbewerbsrecht können in Einklang gebracht werden. Hierfür sind aber aus unserer Sicht eine regulative Begleitung der Entwicklung durch rechtliche Maßnahmen des Gesetzgebers in Abstimmung mit den EU-Institutionen (gezielte Schließung von Schutzlücken bis hin zu einem „Datengesetz") und außerrechtlichen Maßnah-

men (Förderung eines einheitlichen Marktes durch Standardisierung, Förderung des Bewusstseins etc.) kurz- und mittelfristig notwendig.
Die Frage der „Eigentumsordnung für Mobilitätsdaten“ spielt hierbei eine grundlegende Rolle.

Alle Anwendungsszenarien in der Studie gehen von der Grundannahme aus, dass die relevanten Fahrzeugdaten zunächst an einen Server im Verfügungsbereich des Fahrzeugherstellers (Back-End) gesendet und verarbeitet werden. Produktsicherheit und Produkthaftung, wie von den Fahrzeugherstellern angeführt, begründen jedoch weder ein ausschließliches Datenverarbeitungsrecht in Backend-Servern einzelner Hersteller (vgl. „CarData-Programm“ von BMW), noch kann damit allein begründet werden, dass Dritte nicht direkt auf die Fahrzeugdaten zugreifen dürfen. Hier hätte die Studie offener argumentieren müssen, ohne bereits einer technologischen Ausrichtung Vorrang einzuräumen. Entscheidend bleibt, dass der Fahrer selbst die Wahl hat, wie er mit seinen Daten umgehen möchte. Darum müssen die Kunden Cloud-basierter Dienstleistungen in der Mobilität souverän entscheiden können, welche Daten sie preisgeben und was mit ihren Daten passiert. Ihnen muss es möglich sein, die Datenübermittlung zu erkennen, zu kontrollieren und gegebenenfalls auch zu stoppen.

Mit dem nachfolgend erläuterten Konzept des TrustCenters möchte der Verband der TÜV e.V. einen eigenen Diskussionsbeitrag leisten und die bestehenden Ansätze zur Datennutzung um die Idee einer sicheren und datenschutzkonformen Cloud-basierten Lösung ergänzen. Der Fahrzeughalter und –fahrer soll von der Verwendung der eigenen Daten durch Cloud-basierte Dienste auch finanziell profitieren, und insbesondere – in Abgrenzung zu anderen Konzepten – auch die vollständige Transparenz und Datensouveränität erhalten, die das TrustCenter in Kombination mit einer IT-Sicherheit-Architektur in einem digital vernetzten Fahrzeug (Automotive Platform) realisiert. Er kann entscheiden, welchem Dienstleister er wann und unter welchen Konditionen die Daten freigibt. Das TrustCenter schafft entsprechend der Compliance by Design Grundsätze technische Vorkehrungen, die Wettbewerbsbeschränkungen vorbeugt. Automobilhersteller und andere Dienstleister können mit den Bedingungen des TrustCenter ihre Dienstleistungsangebote an den Eigentümer bzw. Halter des Fahrzeugs unterbreiten, ohne die Daten und Datenströme des Wettbewerbs permanent auslesen zu können.

Für die IT-Sicherheit und die Berücksichtigung der gesetzlichen Datenschutzanforderungen (Security & Privacy by Design) empfiehlt der VdTÜV zudem die Verwendung einer neuen, hochsicheren Automotive Platform, die mit einem entsprechenden Interface im Fahrzeug die Kommunikation innerhalb des Systems und nach außen absichert. Diese Komponente ist dringend notwendig, um u. a. Car 2 X Funktionalitäten zukünftig sicher anbieten zu können. Entsprechend des Automotive Platform Konzepts werden die verschiedenen IT-Systeme im Auto logisch voneinander getrennt. Entertainment und Komfortsysteme sind nur über die Sicherheitsarchitektur mit safety- und emissionsrelevanten Systemen verbunden. Der Zugang über einen On-Board-Diagnose (OBD)-Stecker oder eine Telematikschnittstelle (TCU) auf die elektronischen Systeme des Fahrzeugs bleibt somit auch in Zukunft mit einer hochsicheren IT-Sicherheitsarchitektur im Fahrzeug möglich.

Die Konzepte des TrustCenter und der Automotive Platform ermöglichen in ihrer Kombination einen direkten, sicheren und datenschutzkonformen Zugriff auf das Fahrzeug. Im Fahrzeug erzeugte Daten werden über die Automotive Platform sicher und transparent an ein TrustCenter

zur Bereitstellung weiterer Funktionalitäten durch Partner und Dienstleister übermittelt. Auch im Hinblick auf den in der Studie empfohlenen Open-Data Ansatz kann ein unabhängiger, neutraler und sicherer TrustCenter zu einer wesentlichen Verbesserung bei der Nutzung erhobener Daten bspw. im Bereich car-2-infrastructure führen.

1. Leitbilder für den Zugang zu Fahrzeugdaten und deren Verarbeitung

Unter Würdigung der vom BMVI vorgestellten Studie „Eigentumsordnung für Mobilitätsdaten?“ hat der VdTÜV aus Sicht der unabhängigen Prüf- und Zertifizierungsdienstleistungsbranche folgende Leitbilder für den Zugang zu Fahrzeugdaten und deren Verarbeitung aufgestellt.

- Bedingung für die Datenbeschaffung: Einverständnis und Vertrauen

Entscheidend bleibt, dass der Nutzer selbst die Wahl hat, wie er mit seinen Daten umgehen möchte. Darum müssen die Kunden Cloud-basierter Dienstleistungen ganz bewusst entscheiden können, welche Daten sie preisgeben und was mit ihren Daten passiert. Ihnen muss es möglich sein, die Datenübermittlung zu erkennen, zu kontrollieren und ggf. auch zu stoppen.

- Fairer und ungestörter Wettbewerb

Vorbehaltlich der vorherigen Zustimmung der betroffenen Person sollten alle Dienstleister in gleicher, angemessener und diskriminierungsfreier Position sein, um Dienstleistungen für die betroffene Person anzubieten. Die Monopolisierung von Kundendaten kann zu Lock-In-Effekten führen, die den Kunden daran hindern, frei über seine Daten zu verfügen. Häufig behindert sie auch den fairen Wettbewerb sowie die wirtschaftliche und technische Entwicklung.

- Anforderungen an Datenschutz und Security

Das Automobil als IoT-Produkt macht den Schutz gegen Cyberangriffe von außen notwendig. Angriffspunkte sind beispielsweise die Car-Backend-Kommunikation, die Car-to-Car-Kommunikation oder die Car-to-X-Kommunikation. Die Motivation, sich in eine dieser Verbindungswege zu hacken, ist groß, denn die Fahrzeuge können so nicht nur gestohlen, abgehört, per Tracking verfolgt oder manipuliert werden. Es ist auch möglich, Dienste im Auto zu blockieren oder umzuleiten.
Als Schutz vor diesen Bedrohungen kommt beispielsweise in Frage, die Verbindungen der CAN-Busse physikalisch zu trennen, die Kommunikation zwischen den Systemen über ein Gateway oder eine fahrzeuginterne Plattform zu kontrollieren oder die interne Kommunikation mindestens der kritischen Informationen zu verschlüsseln. Wichtige Maßnahmen stellen auch regelmäßige mehrstufige Updates sowie das permanente Monitoring des Fahrzeugnetzwerkes auf Cyberangriffe dar.
Die Daten in vernetzten Fahrzeugen sind als personenbezogene Daten einzustufen, wenn sie ohne besonderen Aufwand einer bestimmten Person zugeordnet werden können. Bereits bei Konstruktion und Herstellung müssen die Grundsätze Privacy-by-Design und Privacy-by-Default für die zukünftige Datenverarbeitung im Fahrzeug berücksichtigt werden. So sollten personenbe-

zogene Daten prinzipiell im Auto selbst verbleiben und nur anonymisiert oder pseudonymisiert in einem externen Server der Hersteller oder Dienstanbieter verarbeitet werden.

- Manipulationsschutz und Haftung

Auch Produktsicherheit und Produkthaftung sind im Zusammenhang mit der Handhabung von Daten aus vernetzten Fahrzeugen relevant, da sie den Interessen und dem Schutz von Kunden dienen. Trotzdem werden grundlegende Datenschutzprinzipien durch Haftungspflichten weder aufgehoben noch eingeschränkt. Insbesondere sind Hersteller nicht aufgrund von Verpflichtungen im Zusammenhang mit Produktsicherheit und -haftung berechtigt, fortlaufend und umfassend Daten aus vernetzten Fahrzeugen zu erheben und auszuwerten. Produktsicherheit und Produkthaftung begründen ferner weder ein ausschließliches Datenverarbeitungsrecht der Hersteller, noch kann damit allein begründet werden, dass Dritte nicht auf diese Daten zugreifen dürfen.

- Datenwirtschaft

Mit der Einschränkung, dass Datenschutzbestimmungen oder spezifische technologische Vorschriften eingehalten werden, begünstigt ein direkter standardisierter Zugang zum Fahrzeug die Interoperabilität zwischen verschiedenen Anwendungen und erleichtert die gemeinsame Nutzung der gleichen Fahrzeugdaten und Ressourcen. Nicht das Sammeln von Daten verspricht Erfolg, sondern deren strategische Auswertung.

Exkurs: Grundlegende Datenschutz-Prinzipien im vernetzten Automobil

Oberstes Gebot einer modernen Datenpolitik muss der Schutz des Rechts auf Privatsphäre, des Grundrechts auf informationelle Selbstbestimmung und der Wahlfreiheit des Verbrauchers bleiben. Die angemessene Information und die Ausgestaltung der Entscheidungsmöglichkeiten des Fahrzeughalters/Nutzer sind von zentraler Bedeutung. Entsprechend der Empfehlungen des 52. Deutschen Verkehrsgerichtstages sollte der „Austausch von Daten und Informationen aus dem Fahrzeug Regeln [unterworfen werden] [...], die das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit der Betroffenen (zum Beispiel Fahrzeughalter und Fahrer) sichern“. Alle Automobil-Daten sind rechtlich relevant. Entsprechend §3 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind personengebundene Daten solche, die Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person sind. Die Fahrzeugsystem-, -Betriebs-, Standort- und Kommunikationsdaten beinhalten immer Informationen, die zumindest dem Halter zugeordnet werden können, da sie sich auf sein Fahrzeug beziehen.

Moderne Fahrzeuge sind mit zahlreichen Sensoren ausgestattet, die technische Parameter und Umweltbedingungen messen. Sie zeichnen permanent Daten wie z. B. die Stellung der Pedale oder der Lenkwinkel, Drehzahlen der Räder, Motorleistung, Bremsdruck etc. über die standardisierte OBD-Schnittstelle oder eine Telematikschnittstelle auf. Mehrere Automobilhersteller in Europa bemühen sich eine Kategorisierung zwischen personenbezogenen und nicht-personenbezogenen Daten mit unterschiedlichen rechtlichen Konsequenzen vorzunehmen. Daten, die von digital vernetzten Fahrzeugen erzeugt werden, gelten nicht automatisch für jeder-

mann als personenbezogene Daten. Entscheidend ist die Frage, ob ein bestimmtes Unternehmen in der Lage ist, eine natürliche Person hinter den Daten zu identifizieren oder nicht.[1] Im Fahrzeug ist dies bereits durch den Umstand einer Zuordnung der Daten zu einer Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen gegeben. Fahrzeughersteller verfügen über diese Informationen in der Regel über den Kaufvertrag oder über das Händlernetzwerk. Gleiches gilt auch für Drittanbieter die beispielsweise Vereinbarungen über Ferndiagnose oder vorausschauende Wartung mit Fahrzeugnutzern haben.

Grundsätzlich gilt die Rechtslage entsprechend der ab 20. Mai 2018 EU-weit unmittelbar anzuwendenden Datenschutz-Grundverordnung (VO (EU) 2016/679): Wenn maschinell erzeugte Daten in Zusammenhang mit einer natürlichen Person gebracht werden können, gelten sie als personenbezogene Daten. Folglich legt Artikel 6, Abs.9, lit (i) der eCall-Richtlinie fest, dass die persönlichen Daten nur mit der „ausdrücklichen Einwilligung" des Fahrzeughalters verarbeitet werden dürfen. Auch für die Informierung des Fahrzeughalters bzw. Fahrzeugnutzer setzt die Richtlinie Maßstäbe. So wird in Artikel 6, Abs.9 festgeschrieben, dass die Hersteller „in der Betriebsanleitung klare und umfassende Informationen über die Verarbeitung von Daten" angeben müssen. Daten aus vernetzten Fahrzeugen können also auch dann als personenbezogene Daten gelten, wenn sie technische Aspekte beschreiben.

Entsprechend des Erwägungsgrunds 26 der Datenschutz-Grundverordnung könnten Daten nicht mehr als personenbezogen gelten, wenn sie „in einer Weise anonymisiert worden sind, dass [der Kunde als] die betroffene Person nicht oder nicht mehr identifiziert werden kann." Auch hier greift wieder das o.a. EuGH-Urteil, nach dem Hersteller die Daten auf eine eindeutige Kennung beziehen können, auch diese für den Hersteller als personenbezogene Daten einzustufen sind. Dies ist vor allem bei den bisher vorgestellten Extended Vehicle/Neutral Server Konzepten namhafter deutscher Automobilhersteller der Fall, die darüber hinaus sich zumindest einen permanenten Lesezugriff auf die Daten im Fahrzeug vorbehalten. Dadurch verlieren die Fahrzeugnutzer die Kontrolle und Souveränität über ihre Daten, sodass ihre Persönlichkeitsrechte gefährdet werden.

Die Herausforderung liegt also darin, eine datenschutzkonforme digitale Datenökonomie zu etablieren, den Verbraucher angemessen über seine „Datenwirtschaft" zu informieren, so dass dieser in der Lage ist, den Datenfluss nachvollziehen zu können bzw. eine bewusste Entscheidung darüber zu treffen, welche Daten er wann, zu welchem Zweck, zu welchen Bedingungen und für welches Unternehmen zur Nutzung und Verarbeitung zugänglich machen möchte.

2. Direkter Zugriff auf Fahrzeugdaten durch die Automotive Platform

Security und Safety sind die Hauptherausforderungen für jeden Lösungsansatz für Telematikarchitekturen. OEMs äußern regelmäßig Bedenken, dass Dritte einen Schreib-Zugriff auf elektrischen Steuergeräte (engl. „Electric control units", ECU) des Fahrzeugs haben – insbesondere auf sicherheitskritischen ECUs. Sowohl der Betrieb der einzelnen Fahrzeugsysteme als auch die Ge-

[1] Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, Patrick Breyer ./. Bundesrepublik Deutschland – C-582/14

samtfunktionalität des Fahrzeugs dürfen nicht beeinträchtigt werden. Bedenken bestehen jedenfalls gegenüber Dritten, die Software im Fahrzeug austauschen könnten.

Das VdTÜV-Konzept der Automotive Platform begegnet diesen Bedenken, indem eine hochsichere und in den Fahrzeugen einheitlich verbaute Kommunikationsplattform (Automotive Platform) vorgeschlagen wird, die den Anforderungen an Datenschutz und Security der neuen Technologien und der möglichen Geschäftsmodelle gerecht wird. Diese technische Konzeption soll Vertrauenswürdigkeit und beweisbare Sicherheit für alle beteiligten Akteure im vernetzten Fahrzeug erlauben.

Das VdTÜV-Konzept der Automotive Platform ist eine technologische Alternative zu proprietären Lösungen der Fahrzeughersteller mit einer passenden Sicherheitsarchitektur für das digital vernetzte Fahrzeug. Diese kann auf bestehende Datenzugangs-Architekturen aufsetzen und Security direkt in das Fahrzeug, u.a. durch hochsichere Separierung und authentifizierten Zugriff, bringen.

Die Automotive Platform ermöglicht das Abrufen von Echtzeitdaten auch im Fahrmodus, geringe Latenzzeiten, Zugang zu Updates über die Mobilfunknetze, sie verhindert Monitoring-by-design der Daten durch Server-Betreiber und sie erfüllt die Anforderungen an die Zukunftsbeständigkeit des digital vernetzten Fahrzeugs auch nach Ende des Service-Angebots des OEMs. Die Bereitstellung dieser Funktionalitäten bildet die Grundlage für das Betreiben einer cloud-basierten Mobilitätsdienstleistung.
Die Plattform als zentrale Sicherheitsarchitektur im Fahrzeug kann alle elektrischen Steuergeräte der verschiedenen Fahrzeugdomänen verbinden. Zudem ist die Plattform der zentrale Zugang für ein TrustCenter, um Software-Updates, Diagnose- und Wartungs-aufgaben via OBD- und/oder Telematikschnittstelle (TCU) durchzuführen. Gleichzeitig nimmt die Plattform eine hochsichere Separierung zwischen Service-diensten (externe Telematikschnittstellen des Fahrzeuges), Informationssystemen (Comfort Domain) und den Safety-relevanten Komponenten (Safety Domain) vor. Informationen, die innerhalb des Fahrzeugs, in das Fahrzeug herein oder aus dem Fahrzeug heraus übertragen werden, werden hierbei vorab von der zentralen Plattform nach bestimmten Nutzungsprofilen aufbereitet.

Die vorgesehenen Security-Funktionalitäten (Security-by-Design) sind unter anderen:

- Informationsflusskontrolle (Firewall)
- Fahrzeug-Domain-Separierung
- sichere M2M Identifizierung / Authentisierung
- Zugangskontrolle zu Fahrzeugschnittstellen und Einbruchserkennung (IDS)
- Auditierung
- Zufallsgenerator
- Verschlüsselung (Kryptoverfahren zu Signierung)

Ein Secure Element am zentralen Motorsteuergateway und anderen sicherheitsrelevanten Steuereinheiten des Fahrzeugs könnte eine hochsichere Ende-zu-Ende Datenübertragung im Internet über ein hybrides Verschlüsselungsprotokoll schaffen und als hochsicherer Tresor für notwendige

Sicherheitsschlüssel und Zertifikate sowohl für die ECUs im Fahrzeug als auch für externe Kommunikationspartner wie etwa Lichtsignalanlagen oder Drittanbietern dienen.

Die Automotive Platform bereitet vorausschauend zu kommunizierende Dateninhalte gemäß vorab definierter Fahrzeugprofile und Datenkategorien auf und versendet diese signiert und verschlüsselt zu TrustCentern oder direkt angeschlossenen Serviceanbietern (OEMs, Zulieferer, Versicherung, Halter, Flottenmanagement, Notdienst, Smart City Services, Parkhäuser, Warndienste, Überwachungsinstitutionen...) über eine Telematikschnittstelle. Diese Profile können im Betrieb durch einen Administrator geändert werden, der aber selbst weder Schreib- noch Lese-Zugriff auf die Fahrzeugdaten hat. Hierbei wird ein Privacy-by-Design Ansatz verfolgt: Nur Daten, die im Sinne des Datenschutzgesetzes zu einem bestimmten Zweck versendet werden dürfen, werden versendet. Im Auslieferungszustand des Fahrzeuges ist die Plattform in der „höchsten Datenschutzstufe“ konfiguriert (Privacy-by-Default). Falls Nutzer/Halter des Fahrzeugs zustimmen, können deren personenbezogene Daten für weitere Verwendungszwecke versendet werden; dies wird dann in den Nutzerprofilen abgebildet. Ein vertrauenswürdiger Zugriff auf die Fahrzeugdaten für Servicedienstleister in der Automotive-Branche muss somit weder aus Security- noch aus Privacy-Gesichtspunkten über die IT-Zentralen der Hersteller (Backend-Server) erfolgen. Bereits von der Automobilindustrie definierte Kommunikationsprotokolle und Dienste werden weiterhin berücksichtigt und genutzt, sofern sie nicht im Widerspruch zu dieser Security/Privacy-Architektur stehen.

Entsprechende Service-Anbieter erhalten somit die Möglichkeit, unter gleichen Bedingungen wie die Automobilindustrie intelligente datenbasierte Geschäftsmodelle für die Fahrzeugnutzer anzubieten. Die Automotive-Platform schafft einen transparenten Wettbewerb, in dem die Verbraucher die Wahl zwischen mehreren Anbietern haben und bequem wechseln können. Die Automotive Platform wäre die Grundlage für einen hochsicheren Datenverkehr zwischen dem Fahrzeug und einem TrustCenter zur Datenverarbeitung und Bereitstellung, entsprechend der o.g. Leitbilder.

3. Transparente und sichere Datenverarbeitung durch das TrustCenter

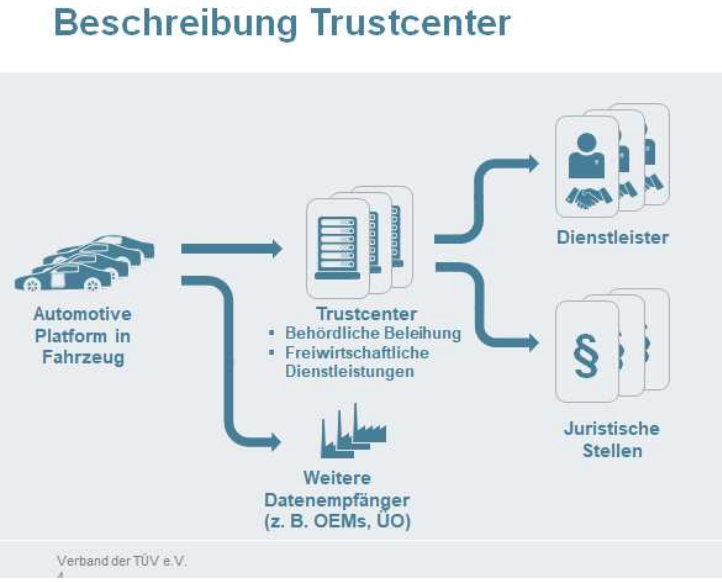
Die zunehmende Vernetzung der Fahrzeuge hat in Verbindung mit der wachsenden Bedeutung von Software im Fahrzeug zur Folge, dass jedes Fahrzeug individuell zu betrachten ist. Fahrzeuge generieren zunehmend Daten, die für Sicherheitsfunktionen genauso wie für die Weiterentwicklung von Fahrzeugen, für innovative Geschäftsmöglichkeiten oder zur Verkehrsüberwachung genutzt werden können. Durch die Vernetzung der Fahrzeuge werden die Daten zugänglich und wertvoll. Die Kontrolle über die Daten ist die Basis und Voraussetzung für erfolgreiche Geschäftsmodelle der Zukunft.

Der VdTÜV hat unter Berücksichtigung der o.g. grundlegenden Datenschutzüberlegungen und den Security-Anforderungen der Automotive Platform das sogenannte TrustCenter Konzept entwickelt, das verschiedenen Dienstleistern diskriminierungsfrei Zugriff auf Daten ihrer Vertragspartner (der Halter, Fahrer und Besitzer der Fahrzeuge – kurz, der Fahrzeugnutzer) ermöglicht. Ein Trustcenter als Teil der Kommunikationsinfrastruktur für die Fahrzeugflotte ist die Komponente

für die sichere, datenschutzkonforme, neutrale Speicherung von Daten, die in Fahrzeugen generiert wurden und für verschiedene Zwecke verwendet werden sollen. Für TrustCenter ist keine Monopolstellung vorgesehen. Interessierte und entsprechend überprüfte und ggf. überwachte Organisationen dürfen im Wettbewerb zueinander TrustCenter betreiben. Der TrustCenter schafft nach den Compliance by Design Grundsätzen technische Vorkehrungen, die es verhindern, dass der Betreiber des TrustCenters permanent und vollständig Einblick in wettbewerblich sensible Informationen anderer Marktteilnehmer zu gewinnen. Er begegnet somit auch kartellrechtlichen Bedenken, die vermehrt in der Automobilbranche gegenüber bisherigen Konzepten geäußert wurden.

Das Trustcenter-Konzept vereint die folgenden Eigenschaften:

- Modul zwischen vernetztem Fahrzeug und Dienstleister
- Herstellerübergreifende Speicherung von Daten aus vernetzten Fahrzeugen
- Neutrale und gleichberechtigte Bereitstellung dieser Daten für Dienstleistungen
- Dadurch Ermöglichen eines fahrzeugzentrierten Dienstleistungsmarkts
- Direkter Zugriff auf Fahrzeug über Automotive Platform



Es zeichnet sich gleichzeitig durch folgende Prinzipien aus:

- Security & Privacy by Design nach Stand der Technik
- Compliance by Design durch hinreichende technische Vorkehrungen
- Angepasst an internationale Standards
- Angemessene Regulierung
- Vertrauen in Unabhängigkeit
- Attraktivität und Akzeptanz am Markt
- Offenes Ökosystem

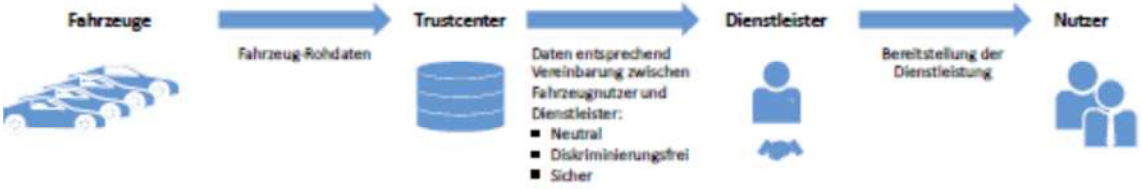
Die Implementierung des Trustcenters muss offen und transparent gestaltet werden, d.h. das Trustcenter muss für Partner und Dienstleister im Markt zugänglich sein. Ein offenes und international verfügbares Trustcenter und Ökosystem erfordert standardisierte und leistungsfähige Schnittstellen (API) zwischen allen Komponenten und Beteiligten. Dabei können mehrere TrustCenter in einer dezentralen Architektur im Verbund und konkurrierend fungieren. Fahrzeughalter

können ein TrustCenter wählen und zwischen verschiedenen TrustCenter wechseln. Eine dezentrale und integrierte Architektur begünstigt Ausfallsicherheit und Skalierbarkeit. Eine integrierte Architektur ist für übergreifende Anwendungsfälle wie z.B. die Erkennung von Cyberangriffen über einzelne TrustCenter hinweg unabdingbar.

Aufgrund der Tatsache, dass die Daten personenbezogen und sicherheitsrelevant (sowohl bezüglich funktionaler Sicherheit (Safety) als auch bezüglich Informationssicherheit (Security)) sind, müssen Datenschutz und Sicherheit während der Erfassung, des Transports, der Speicherung und der Verarbeitung sichergestellt werden. Die Umsetzung muss zukunfts- und kundenorientiert erfolgen und soll dabei innovative Ansätze wie z.B. Blockhain zur sicheren und transparenten Datenverarbeitung unterstützen.

Das TrustCenter ermöglicht transparente, neutrale und sichere Datenverarbeitung, die Verwendung der Daten über das Fahrzeug hinaus zum Nutzen und mit Einverständnis des Fahrzeugnutzers (z.B. Parkleitsystem in Städte).

Ein TrustCenter, als Teil der Kommunikationsinfrastruktur für die Fahrzeugflotte, ist die Komponente für die sichere, datenschutzkonforme, neutrale Speicherung von Daten, die in Fahrzeugen generiert wurden und für verschiedene Zwecke verwendet werden sollen.



Aus unserer Sicht sollten bei den weiteren Überlegungen im BMVI unsere Empfehlungen Berücksichtigung finden. Weitere Konzepte und Analysen bisheriger „in-vehicle data“ - Nutzungskonzepte werden in der sogenannten TRL-Studie der Europäischen Kommission beschrieben, auf die wir abschließend gern noch verweisen möchten. (Europäische Kommission, Access to in-vehicle data and resources, Final Report 2017).