Position

VDA | Verband der Automobilindustrie

Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten

Fachlicher Ansprechpartner

Geschäftsführung

Klaus Bräunig
Dr.-Ing. Damasky
Dr. Kay Lindemann

Abteilungsleiter

Graham Smethurst
Tel.:+49 (0) 30 897842-426

E-Mail: smethurst@vda.de

Der Handlungsbedarf:

Moderne Fahrzeuge besitzen bereits heute bis zu einhundert fortwährend miteinander kommunizierende On Board Control Units zur Gewährleistung richtigen Fahrens und Kundenfunktionalität. Mit steigender Konnektivität und Digitalisierung kann der Zugriff auf Fahrzeuge und Fahrzeugdaten theoretisch von jeder auch noch so entlegenen Ecke der Welt aus möglich sein. Diese Möglichkeit legt viele bisher ungenutzte Potentiale frei, die beispielsweise zur Unfallvermeidung, höherer Energieeffizienz oder Reduzierung von CO2-Ausstößen beitragen und dabei den Fahrkomfort erhöhen. Datenaustausch schafft das Fundament für die Verbindung von Verkehrsträgern und realisiert das volle Potential einer nahtlosen Intermodalität. Daten bilden die Intelligenz des gesamten Verkehrssystems, indem sie hochautomatisierten und autonomen Fahrzeugen ermöglichen, ihr volles Potential auszuschöpfen. Fahrzeuge werden zu Datenerzeugern. Der sichere Austausch von Daten bildet die Grundlage für neue Geschäftsaktivitäten und -anwendungen

Allerdings bestehen bezüglich Sicherheit und Datenschutz signifikante Risiken und Herausforderungen. Dies unterscheidet die Automobilindustrie von anderen bereits etablierten Plattformen. Denn das Auto ist kein Smartphone: Im Gegensatz zu Handys oder anderen Geräten dieser Art, benötigt ein Fahrzeug wesentlich höhere Standards im Bezug auf Sicherheit und Datenschutz.

- Fahrzeugsicherheit: Das Ziel ist die Vermeidung von inakzeptablen Risiken physischer Verletzungen oder direkter bzw. indirekter Gesundheitsschäden.
- Automobilsicherheit: Das Ziel ist der Schutz von Integrität und Verfügbarkeit von Fahrzeugfunktionen, elektronischen Komponenten und Daten sowohl gegen Cyber-Angriffe als auch Manipulation.
- Datenschutz: Das Ziel des Datenschutzes ist der Schutz von Einzelpersonen und die Gewährleistung, dass diese über die Nutzung sämtlicher persönlicher Daten informiert werden (Transparenz) und sie die Wahl haben, welche Daten zu welchem Zweck an wen weitergegeben werden.

Auf der einen Seite werden durch die voranschreitende Konnektivität von Fahrzeugen neue Anwendungen für den Kunden oder innovative Businessmodelle ermöglicht, auf der anderen Seite macht diese Entwicklung das Fahrzeug allerdings auch verwundbar gegenüber Cyberattacken. Anders als das Smartphone ist das Fahrzeug jedoch für seine/n Nutzer von hoher Sicherheitsrelevanz. Somit haben die Integrität und Sicherheit des Fahrzeugs und Fahrers oberste Priorität und müssen jederzeit garantiert sein.In Abwesenheit eines weitläufig akzeptierten Konzepts, das die Erfüllung der Anforderungen sicherstellt, werden die Vorteile der Konnektivität und Automatisierung nicht verwirklicht und das

Kundenvertrauen leidet darunter.

Zusammenfassung

Der VDA vertritt eine Position, die die Anforderungen an Safety und Security, Datenschutz sowie diskriminierungsfreie Innovation erfüllt.

Konzept für die Datenübertragung

Diese Position stützt sich auf eine Zwei-Wege-Architektur:

1. Jeder OEM nimmt die Rolle eines Systemadministrators ein und übernimmt die Verantwortung für einen sicheren Transfer von den im Fahrzeug generierten Daten zu einem standardisierten und gewarteten Business-to-Business-OEM-Interface (B2B).
2. Dritte können direkt über dieses B2B-OEM-Interface oder über Neutrale Server, die die Daten des OEM-Servers zusammentragen, auf Fahrzeugdaten zugreifen. Dem Neutralen Server können verschiedene Services unterschiedlicher Anbieter nachgeschaltet sein.

Der Zugriff auf Fahrzeugdaten über den OEM-Server unterliegt B2B-Vereinbarungen.

Um Risiken für den Kunden und die öffentliche Sicherheit zu vermeiden, wird kein direkter Zugriff auf das Fahrzeug durch Dritte zugelassen. Das beschriebene zweistufige Konzept für den Transfer von im Fahrzeug generierten Daten ermöglicht aber einen völlig diskriminierungsfreien Zugriff und damit sowohl neue Innovationen als auch offenen und fairen Wettbewerb, ohne dabei Marktmachtmissbrauch und Monopoletablierung in digitalen Märkten zuzulassen. Der gesetzlich regulierte Status Quo und Weiterentwicklungen der OBD-I-/ OBD-II-Schnittstelle werden für Diagnose- und Wartungszwecke erhalten. Die OEMs behalten sich das Recht vor, spezifische Maßnahmen zum Schutz der Fahrzeugintegrität während des Normalbetriebs durchzuführen.

Konzept für Datennutzungskategorien

Zur Regulierung der Datenverfügbarkeit befinden sich weltweite Regulierungsinitiativen in Planung. Alle Entscheidungen in Bezug auf die Datenteilung beeinflussen Wettbewerb, Sicherheit und Produkthaftung. Für eine faire Debatte ist ein breites und weitgehend akzeptiertes Verständnis von Daten und deren Nutzung eine wichtige Vorraussetzung.

Der Position des VDA liegen vier Datenkategorien zugrunde:

Kategorie 1 – Daten für die Verbesserung der Straßenverkehrssicherheit: Hier liegt der Fokus auf dem gesellschaftlichen Nutzen. Die anonymisierten Daten werden zur signifikanten Steigerung der Verkehrssicherheit zwischen den beitragsleistenden Vertragsparteien (inklusive der öffentlichen Hand) ausgetauscht.

Kategorie 2 – Daten für markenübergreifende Services: ein definiertes OEM-übergreifendes Datenset, das aus nicht differenzierenden anonymisierten Fahrzeugdaten besteht.

Kategorie 3a – Daten für markenspezifische Services: Daten eines differenzierenden OEM-spezifischen Datensets, das aus OEM-spezifischen anonymisierten Daten und Daten mit spezieller IP-Relevanz besteht.

Kategorie 3b – Daten für die Komponentenanalyse und Produktoptimierung: ein differenzierendes komponentenspezifisches und anonymisiertes Datenset, das der OEM ausschließlich dem relevanten Komponentenentwickler zu Produktverbesserungszwecken zur Verfügung stellt.

Kategorie 4 – Persönliche Daten: ein definiertes OEM-übergreifendes und OEM-spezifisches Datenset, das nur denjenigen Parteien zugänglich gemacht wird, die hierfür die Zustimmung des Kunden erhalten haben. Dies kann auf Grundlage von geltendem Recht, Verträgen oder Einwilligung geschehen. Die Daten dieser Kategorie unterstützen Services, die eine Identifikation des Kunden oder des Fahrzeugs erfordern, oder aber, die die Nutzung personenbezogener Daten einschließen. Dies inkludiert ebenfalls die Fahrzeug-Identifikationsnummer (FIN), beschränkt sich aber nicht auf diese. Die Daten der vierten Kategorie werden ausschließlich unter Berücksichtig der Persönlichkeitsrechte des Kunden zur Verfügung gestellt.

Daten für die Verbesserung der Straßenverkehrssicherheit (Kategorie 1) werden von der deutschen Automobilindustrie der öffentlichen Hand speziell zur Erhöhung der Straßenverkehrssicherheit zur Verfügung gestellt. Dies wird in einer diskriminierungsfreien Art und Weise über die OEM-Backend-Server basierend auf individuellen Vereinbarungen geschehen und sollte auf Gegenseitigkeit beruhen.All diejenigen, die Daten mit der geforderten Qualität beisteuern, sind zur Nutzung der geteilten Daten berechtigt.

Die Daten der Kategorien zwei bis vier sind durch ihre unterschiedlichen Nutzungen und Anforderungen an den Datenschutz charakterisiert. Die Daten werden diskriminierungsfrei basierend auf individuellen Vereinbarungen (sofern nicht gesetzlich geregelt) zwischen dem Kunden und dritten Marktteilnehmern über ein B2B-Interface zur Verfügung gestellt. Die Lieferung der Daten geschieht in Bezug auf beispielsweise Preisgestaltung, die Menge und Art der zur Verfügung gestellten Daten, Rechtzeitigkeit der Übertragung und allen anderen relevanten Qualitätskriterien auf diskriminierungsfreie Art und Weise.Die Zwei-Wege-Architektur trifft auf den Umgang mit allen vier Datenkategorien zu und beinhaltet die verschiedenen Datenschutz- und Datennutzungsanforderungen jeder Kategorie. Ziel ist es, Plattformen zum Austausch von Mobilitäts-, Aftermarket- und im Fahrzeug generierten Daten zu schaffen, die dem Kunden analog zu den bereits existierenden Plattformen zum Datenaustausch für Geräte wie Tablets und Smartphones eine Wahlmöglichkeit anbieten und den freien Wettbewerb fördern.

Politischer Dialog

Die Digitalisierung wird Mobilität und die Automobilindustrie fundamental verändern. Die durch diese technologische Innovation geschaffenen Möglichkeiten werden in den nächsten zehn Jahren einen größeren Einfluss auf diesen Industriezweig haben, als alles andere in den letzten 30 Jahren.

Aufgrund der sehr hohen ökonomischen und gesellschaftlichen Relevanz von Regeln für die Datennutzung, strebt der VDA eine aktive Rolle in dieser Diskussion auf nationaler und EU-weiter Ebene an. Die Europäische Kommission hat eine Reihe von Initiativen ins Leben gerufen, die sich auf dieses von Fahrzeugherstellern und -zulieferern gemeinsam erstellte Konzept beziehen. Besonders die von DG-Connect begonnene Debatte zum Thema "C-ITS" und der "Initiative für freien Datenfluss" ("Free flow data initiative") betrifft die Frage, wie Fahrzeugdaten an Dritte übertragen werden können, direkt. Gleichzeitig beeinflussen die Debatten und Entscheidungen rund um die Fahrzeugdaten die Interessen verschiedener anderer Unternehmen, beispielsweise aus der Versicherungsbranche, mit denen der VDA gleichermaßen in Dialog treten möchte.

Dieses Positionspapier konzentriert sich auf die ursprünglich im Fahrzeug generierten Daten für B2B- sowie auf die B2C-Nutzung und schlägt ein

Konzept für eine sichere und diskriminierungsfreie Möglichkeit der Datenfreigabe vor. Aus datenschutzrechtlicher Sicht werden nur diejenigen Services berücksichtigt, die den Endverbraucher betreffen. Die Datenschutzaspekte für Berufskraftfahrer fallen beispielsweise nicht darunter. So wie bei allen Konzepten müssen auch hier die Datenschutzrechte des Kunden sowie bestehende und geplante Gesetzgebung zum Datenschutz berücksichtigt werden.

Dieses Positionspapier folgt den Datenschutzprinzipien des VDA aus dem Jahr 2014 und der vom VDA und der deutschen Datenschutzbehörde im Januar 2016 zum Thema Datenschutz gemeinsam veröffentlichten Erklärung.

Das digitale Fahrzeug

Das Fahrzeug ist bereits seit geraumer Zeit digital. Fahrzeuge beinhalten eine Vielzahl elektronischer und durch Software gesteuerte Systeme, die Daten erzeugen und für Funktionen im Fahrzeug nutzen. Diese Daten tragen bereits jetzt schon zu effizienteren Motoren und verbesserter Fahrzeugsicherheit bei. Eine relativ neue Entwicklung ist das vernetzte Fahrzeug. Eine Vielzahl von Konnektivitätsarten ermöglicht den Austausch von Daten mit dem Fahrzeug.

Vernetzt für Komfort und Entertainment – Gegenwärtig sind viele Fahrzeuge für die Nutzung von Komfort- und Entertainment-Services vernetzt. Das Fahrzeug kann Zugriff auf das Smartphone des Kunden erhalten und so eine sichere Nutzung von auf dem Handy befindlichen Apps und Daten im Fahrzeug ermöglichen. Das Fahrzeug ist mit dem Backend verbunden und ermöglicht damit den Datenaustausch für noch bessere Komfort- und Entertainment-Angebote.

Vernetzt für E-Call – E-Call führt erstmalig ein Sicherheitselement in die Fahrzeugkonnektivität ein. Die Zuverlässigkeit von E-Call und die Übertragung zugehöriger Daten hängt von der Verbindung des Fahrzeugs zum Mobilfunknetz ab. Daher ist eine umfassende Netzabdeckung unverzichtbar.

Vernetzt für Fahrfunktionen – Die nächste Stufe der Sicherheitsrelevanz wird erreicht, wenn Konnektivität dabei hilft, Daten zur direkten Beeinflussung des Fahrzeugverhaltens bereitzustellen. Diese Art der Konnektivität wird die Fähigkeiten von On-Board-Systemen verbessern und ermöglicht den automatisierten und autonomen Systemen dadurch, ihr volles Potential für eine ausgefeilte Nutzererfahrung zu entfalten. Durch die Einführung von automatisierten und autonomen Fahrlösungen wird die Notwendigkeit für starke Sicherheitsvorkehrungen immer immanenter, da mögliche Konsequenzen eines Angriffs auf diese Systeme völlig neue Dimensionen annehmen können.

Obwohl die Fahrzeugkonnektivität neue Funktionen für den Kunden sowie neue Geschäftsmöglichkeiten realisiert, wird die Anfälligkeit des Fahrzeugs für mögliche Cyber-Angriffe dadurch in jeder Form erhöht. Im Gegensatz zu einem Smartphone ist ein Fahrzeug ein sicherheitsrelevantes Gerät. Die Integrität und Sicherheit des Fahrzeugs ist von äußerster Wichtigkeit und muss zur Gewährleistung eines vorhersehbaren Fahrzeugverhaltens und der Insassensicherheit zu jeder Zeit geschützt werden.

Leitprinzipien

Der Schlussbericht der EU-Kommission des C-ITS-Plattform-Projekts vom Januar 2016 identifizierte die folgenden "fünf Leitprinzipien, die angewendet werden sollten, wenn Zugriff auf Fahrzeugdaten und -ressourcen gewährt wird."

a) Bedingungen für die Datenbereitstellung: Einwilligung

Der Dateneigner (Besitzer und/oder Nutzer des Fahrzeugs oder mobiler Geräte) entscheidet, ob Daten bereitgestellt werden dürfen und wer Zugriff auf diese erhält. Dies schließt ebenfalls den konkreten Zweck für die Nutzung der Daten ein (und damit für den ausgewiesenen Service). Für Endverbraucher und Dateneigner gilt immer eine Ausstiegsoption. Dies steht jedoch ohne Verbindlichkeit zu den Anforderungen behördlicher Verwendung.

b) Fairer und unverfälschter Wettbewerb
Vorbehaltlich der Einwilligung des Dateneigners sollten alle Dienstleister in einer gleichwertigen, fairen, angemessenen und diskriminierungsfreien Position sein, ihre Dienste dem Dateneigner anzubieten.

c) Datenschutz und Datensicherheit
Der Bedarf nach Datenschutz für Fahrzeug- und Bewegungsdaten für Dateneigner ist eindeutig gegeben. Selbiges gilt auch für Unternehmen im Bezug auf Wettbewerbs- und/oder Sicherheitsgründe.

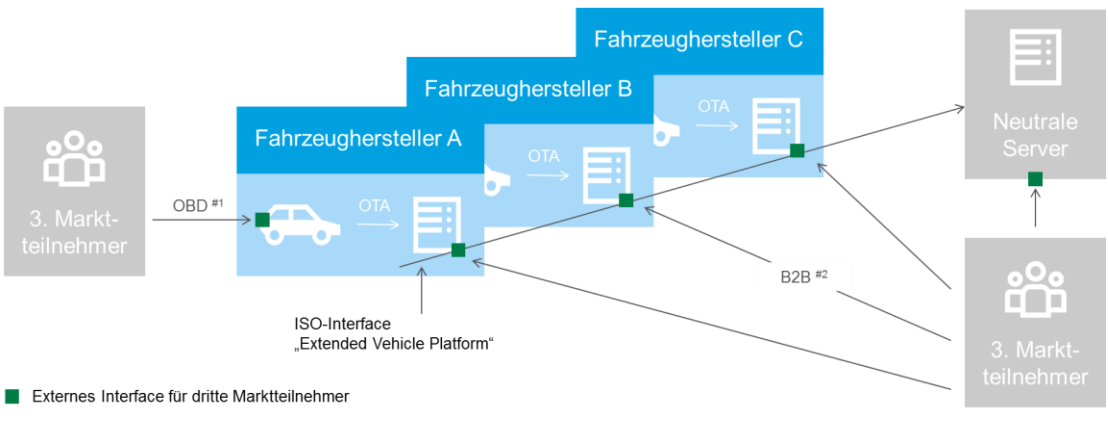
d) Manipulationssicherer Zugriff und Haftung
Dienstleistungen, die Fahrzeugdaten und -ressourcen verwenden, dürfen die ordnungsgemäße und sichere Funktion des Fahrzeugs nicht gefährden. Außerdem darf der Zugriff auf Fahrzeugdaten und -ressourcen keinen Einfluss auf die Haftung des Fahrzeugherstellers im Bezug auf die Nutzung des Fahrzeugs haben.

e) Datensparsamkeit
Unter Vorbehalt, dass Datenschutzbestimmungen oder spezifische technologische Vorschriften eingehalten werden, unterstützt ein standardisierter Zugriff die Kompatibilität verschiedener Anwendungen, besonders der regulierenden Schlüsselanwendungen, und ermöglicht somit die gemeinsame Nutzung derselben Fahrzeugdaten und -ressourcen.

Der Vorschlag des VDA wurde im Einklang mit diesen Leitprinzipien entwickelt. Dieses Konzept behandelt sowohl die Zugriffsmethode auf das Fahrzeug sowie auf die im Fahrzeug generierten Daten, die zur Verfügung gestellt werden sollen.

Zugriff auf das Fahrzeug

Direktverbindungen zum Fahrzeug stellen ein potentielles Sicherheitsrisiko dar, allerdings ist eine Vernetzung für den Zugriff auf die im Fahrzeug generierten Daten notwendig. Der Zugriff auf das Fahrzeug muss zur Risikominimierung auf verwaltete Schnittstellen beschränkt sein.



#1 Diagnose und Reparatur
#2 B2B-Vereinbarung unter Berücksichtigung der Anforderungen an Fahrzeugsicherheit (Safety/Security) und Datenschutz

Aus Gründen der Safety und Security sowie des Datenschutzes erfolgt der Datentransfer in jedem Fall über das OEM-Backend als sog. Last-mile unter Berücksichtigung der Safety-, Security- und Privacy-Anforderungen. Hinter dem OEM-Backend können ein oder mehrere neutrale Server liegen, an welchem die Dienstleister ihre beliebigen Services andocken können Diese neutralen Server werden weder vom OEM betrieben noch finanziert.

Zur Gewährleistung der Safety sind keine direkten „triggerbaren“ Aktionen auf Steuergeräte durch Dritte über eine Online-Schnittstelle zulässig. Ausnahmen, die die Sicherheit und Sicherheitsbeschränkungen berücksichtigen, müssen in bilateralen Vereinbarungen festgelegt werden.

Der Status Quo der OBD-II-Schnittstelle wird beibehalten, d.h. Zugriff für Tier 1, freie Werkstätten und rechtlich zulässige Services auf Diagnosedaten (Level 1, Level 2) inkl. zukünftiger Erweiterungen wird gewährt. Die OEMs behalten sich das Recht vor, spezifische Maßnahmen zum Schutz der Fahrzeugintegrität während des Normalbetriebs durchzuführen. Aufgrund dieser wachsenden Bedrohung könnten OEMs zur Ergreifung von Maßnahmen zur Sicherstellung der gesetzlichen Vorgaben gegenüber Datenschutz, Produkthaftung, Produkt- und Verkehrssicherheit gezwungen sein.

Fahrzeugdaten ohne Schwerpunkt auf Diagnose- and Reparatur, auf die derzeit über die OBD-I-/OBD-II-Schnittstelle zugegriffen wird und über Drittanbieterprodukte übertragen werden, werden soweit wie möglich und gemäß der bilateralen B2B-Vereinbarungen auf die OEM-Backend-Server migriert und stehen daher auf neutralen Downstream-Servern zur Verfügung.

Schreibende Diagnosezugriffe über eine Onlineschnittstelle sind nicht verfügbar - vorbehaltlich bilateraler Vereinbarungen zwischen den beteiligten Marktteilnehmern, diese müssen über die OBD-I- und OBD-II-Schnittstelle gemäß GVO erfolgen, damit Fahrzeuge bei Stillstand auch von Dritten im Aftersales diagnostizier- und reparierbar sind.

Der Datentransfer zwischen Fahrzeug und Backend liegt in der Gesamtverantwortung des OEMs als „Administrator“ (Aggregationsgateway im Fahrzeug, Funkstrecke, Backend). Der Hersteller ist in der Verantwortung, dass diese Strecke funktioniert und die Privacy-, Safety- und Security- Anforderungen zu jederzeit erfüllt werden.Die durch den OEM über die B2B-Schnittstelle zur Verfügung gestellten Daten müssen von gleicher Qualität sein, wie die Daten auf dem OEM-Backend.

Die vom Fahrzeug an das OEM-Backend übertragenden Daten erscheinen ohne übermäßige Verzögerung auf der externen ISO 20078 B2B-OEM-Schnittstelle.

Kategorien der Datennutzung

Die überwiegende Mehrheit der im Fahrzeug generierten Daten sind rein technisch. Diese bestehen nur temporär, werden lokal in den Fahrzeugsystemen verwendet und somit niemals gespeichert. Die übrigen der im Fahrzeug generierten Daten können für verschiedene Zwecke verwendet werden. Der VDA hat vier Nutzungskategorien für im Fahrzeug generierte Daten definiert, die mit den Kategorien in den Datenschutzprinzipien des VDA aus dem Jahr 2014 in Korrelation stehen.

Kategorie 1 – Daten für die Verbesserung der Straßenverkehrssicherheit: Hier liegt der Fokus auf dem gesellschaftlichen Nutzen. Die anonymisierten Daten werden zur signifikanten Steigerung der Verkehrssicherheit zwischen den mitwirkenden Vertragsparteien (inklusive der öffentlichen Hand) ausgetauscht[#1], z. B.

Fahrzeugdaten: Aktivierung der Warnblinkanlage

Infrastrukturdaten: Position von Einsatzfahrzeugen

Kategorie 2 – Daten für markenübergreifende Services: ein definiertes OEM-übergreifendes Datenset, das aus nicht differenzierenden anonymisierten Fahrzeugdaten besteht, z. B. Umgebungstemperatur, Verkehrsfluss.

Kategorie 3a – Daten für markenspezifische Services: Daten eines differenzierenden OEM-spezifischen Datensets, das aus OEM-spezifischen anonymisierten Daten und Daten mit spezieller IP-Relevanz besteht, z. B. Fahrbahnmarkierung, Fahrgestellsensordaten für die Feststellung des Straßenzustands.

Kategorie 3b – Daten für die Komponentenanalyse und Produktoptimierung: ein differenzierendes komponentenspezifisches und anonymisiertes Datenset, das der OEM dem relevanten Komponentenentwickler ausschließlich zu Produktverbesserungszwecken zur Verfügung stellt[#1], z. B. Leistungsdaten der Kraftstoffpumpe.

Kategorie 4 – Persönliche Daten: ein definiertes OEM-übergreifendes und OEM-spezifisches Datenset, das nur durch den Kunden autorisierten Drittanbietern zur Verarbeitung von Daten nach Gesetz, Vertrag oder Einwilligung zur Verfügung gestellt wird[#1]. Die Daten in dieser Kategorie unterstützen Services, die eine Identifikation des Kunden oder des Fahrzeugs erfordern**,** oder aber**,** die die Nutzung personenbezogener Daten einschließen. Dies inkludiert ebenfalls die Fahrzeug-Identifikationsnummer (FIN), beschränkt sich aber nicht auf diese. Die Daten werden nur mit Einwilligung des individuellen Anwenders oder auf Basis eines Vertrags mit einem individuellen Anwender zur Verfügung gestellt und dürfen nur durch den ausgewählten spezifischen Partner des individuellen Anwenders genutzt werden, z. B. Fahrzeugposition (in Verbindung mit der FIN).

#1 Daten werden Dritten vom OEM im Rahmen einer B2B-Vereinbarung zur Verfügung gestellt.

Kategorie 1	Kategorie 2	Kategorie 3a	Kategorie 3b	Kategorie 4
Daten zur Verbesserung der Straßenverkehrs-sicherheit	Daten für marken-übergreifende Services	Daten für marken-spezifische Services	Daten für die Komponen-tenanalyse und Produkt-optimierung	Personenbezogene Daten
Verkehrssicherheitsrele-vante Daten	Nicht differenzierende Fahrzeugdaten	Differenzierende und für den OEM IP-relevante Fahrzeugdaten	Differenzierende und für den OEM sowie Zulieferer IP-relevante Fahrzeug-daten	„Recht auf Zugriff" nur für zur Datenverarbeitung durch Gesetz, Vertrag oder Einwilligung befugte Parteien
Daten z.B. für: öffentliche Verkehrsleitzentralen	Diskriminierungsfreier Datenzugriff für Dritte[#2] [#3]	OEM oder vom OEM beauftragter Partner	OEM oder vom OEM beauftragter Partner	Vom Kunden ausgewählte(r) Partner
Feuerwehr, Polizei, …	Produkt	Händler, Tochterges.	Produkt	Kunde

Der Kunde[#1] wird über die Nutzung der Daten informiert. Die OEMs werden dem Kunden Entscheidungsmöglichkeiten, die er jederzeit widerrufen kann, zur Verfügung stellen, es sei denn, die betreffende Funktion ist gesetzlich angeordnet.

Kategorien der Datennutzung

Zugriff auf im Fahrzeug generierte Daten

Daten der Datenkategorie 1 (anonyme Daten zur Steigerung der Verkehrssicherheit) werden einer hoheitlichen Stelle vom Backend-Server des OEM diskriminierungsfrei basierend auf individuellen Vereinbarungen mit dem OEM zur Verfügung gestellt. Die Daten sind nur dann obligatorisch zur Verfügung zu stellen, sofern sie in standardisierter Form im Fahrzeug vorgehalten werden. Es gibt keine Verpflichtung, diese Daten im Fahrzeug zu erheben. Sofern Daten übermittelt werden, partizipieren jedoch alle an diesen Daten, die am Informationsaustausch teilnehmen (Reziprozität).

Daten der Kategorien 2 bis 4 sind nicht-differenzierende anonymisierte Daten, konkurrierende differenzierende anonymisierte Daten und personenbezogene Daten, die von OEM-Backend-Servern bereitgestellt werden. Die Daten werden diskriminierungsfrei basierend auf individuellen Vereinbarungen (sofern nicht gesetzlich geregelt) zwischen dem Kunden und dritten Marktteilnehmern über ein B2B-Interface zur Verfügung gestellt. Die Lieferung der Daten geschieht in Bezug auf beispielsweise Preisgestaltung, die Menge und Art der zur Verfügung gestellten Daten, Rechtzeitigkeit der Übertragung und allen anderen relevanten Qualitätskriterien auf diskriminierungsfreie Art und Weise.Der Datenzugriff erfolgt über eine für den OEM-Backend-Server festgelegte und zertifizierte Schnittstelle. Der Datenzugriff und die Bereitstellung von Funktionen durch Verwendung der Daten innerhalb des Fahrzeugs erfordert eine Vereinbarung zwischen dem Lösungsanbieter (Dritter oder Betreiber des unabhängigen Servers) und dem OEM (B2B-Vereinbarung). Der Datenzugriff findet trusted und zertifiziert statt. Eine Überwachung durch den OEM wird nur zum Schutz gegen unautorisierten Zugriff und Systemangriffe sowie im datenschutzrechtlich nötigem Ausmaß durchgeführt. Beim Datenzugriff müssen besonders die im Bezug auf Sicherheit und Haftung relevanten Leitprinzipien berücksichtigt werden.
Der Betreiber der neutralen Server kann mit den jeweiligen OEMs weitere Datenfelder zur Aufnahme in den neutralen Server verhandeln, ohne dabei die Nutzung oder den Anbieter offenzulegen (B2B-Vereinbarung), und damit neue Geschäftsmodelle ermöglichen. Der neutrale Server wird nicht durch einen OEM betrieben und finanziert (Unabhängigkeit).Die Anonymität der auf die Daten zugreifenden Partei wird im Rahmen der Datenschutzvorschriften gewährleistet. Für die Einholung und Verwaltung der Kundeneinwilligung bezüglich des Zugriffs von Dritten auf personenbezogene Daten über die B2B-OEM-Schnittstelle ist der OEM verantwortlich. Außerdem muss er sicherstellen, dass der Kunde der Übertragung spezifischer Fahrzeugdaten an den spezifischen Empfänger für spezifische Zwecke zugestimmt hat. Für persönliche Daten, auf die eine dritte Partei über einen neutralen Server zugreift, muss der OEM sicherstellen, dass der Kunde der Übertragung spezifischer Fahrzeugdaten, z. B. über den Betreiber des neutralen Servers, zugestimmt hat. In diesem Falle muss der Betreiber des neutralen Servers gewährleisten, dass der Kunde der Übertragung spezifischer Daten vom Fahrzeug zum spezifischen Empfänger für spezifische Zwecke zugestimmt hat.

#1 Der Begriff „Kunde“ wird hier einheitlich verwendet und ist weit zu verstehen. Je nach Kontext sind hiermit Fahrer, Halter oder Nutzer gemeint.

#2 Beteiligung an diesem Konzept und die technische Umrüstung des Fahrzeugs können vom OEM nicht verlangt werden.

#3 Die Leitprinzipien sind bei der Nutzung des definierten Dateninterfaces zu beachten. Die Nutzung des Interfaces schließt Rechte und Pflichten mit ein.

Das technische Design und die Ausgestaltung seines Produktportfolios liegen in der Verantwortung des OEM. Im Rahmen bilateraler Geschäftsbeziehungen können individuelle Vereinbarungen unter Berücksichtigung der technischen Möglichkeiten und der Anforderungen an Safety, Security und Privacy geschlossen werden.

Es bestehen keinerlei Einwände gegen die Schaffung von Serviceleistungen Dritter, die auf den von der standardisierten B2B-Schnittstelle an den OEM-Backend-Server gelieferten Daten basieren, sofern Datenschutz- und Sicherheitsanforderungen berücksichtigt werden und eine Vereinbarung zwischen Serviceanbieter und dem OEM besteht.

Zur Förderung von Innovationen und Unterstützung von Forschungs- und Entwicklungsaktivitäten ist eine bilaterale Vertragsgestaltung des Datentransfers von anonymen, pseudonymen Daten denkbar. Rahmenbedingungen für die Datenübertragung zu Entwicklungszwecken gilt es zu definieren.

Für die Bereitstellung von Daten im Rahmen der kommerziellen Nutzung ist die Generierung eines funktionsfähigen Datenmarktplatzes zielführend. Für die Generierung und Aufbereitung der Daten zu kommerziellen Diensten entsteht ein Aufwand, welcher beim Abruf der Daten kommerzieller Vertragsbestandteil sein muss. Zu definierende Rahmenbedingungen: Businessmodell, Nutzungsrechte, Marktplatz, etc. unter Berücksichtigung der Trennung von Bezahlung der Daten und Bezahlung der Services (Schaffung fairer Wettbewerbsbedingungen).

VDA
Verband der Automobilindustrie e. V.
Behrenstr. 35
10117 Berlin
Telefon: +49 (0) 30 897842 - 0
Fax: +49 (0) 30 897842 - 600
info@vda.de
www.vda.de

Freigegeben 19.09.2016