Policy Sheet Europawahl 2019

VERNETZTE MOBILITÄT

Standards im Umgang mit Fahrzeugdaten für die Mobilität des 21. Jahrhunderts setzen!

Das Internet der Dinge (IoT) führt in allen Bereichen unserer Gesellschaft zu umwälzenden Veränderungen. Alle heute entstehenden Ökosysteme führen zu verstärkter digitaler Interaktion, einer tiefer reichenden Integration der Wertschöpfungsketten und einer zunehmenden Abhängigkeit der Marktteilnehmer untereinander. Datenverfügbarkeit, Wahlfreiheit der Kunden und Vertrauen in die Sicherheit der Nutzung von Daten sind unabdingbar für die Funktionsfähigkeit sowie die Innovationsfähigkeit und das Wachstum dieser neuen digitalen Wirtschaft.

Neue Entwicklungen wie das vernetzte Fahren sowie multimodale Nutzungsmodelle in der Mobilität gehen mit einer erhöhten Konnektivität und somit auch Datenkommunikation einher. Ein wichtiges Element des digitalen Wandels in der Mobilität ist, dass die Sicherheit von Daten und vernetzten Fahrzeugen und Systemen gewährleistet wird und die diesbezügliche Glaubwürdigkeit vorhanden ist. Cybersicherheit und Datenschutz werden zum Dreh- und Angelpunkt einer zuverlässigen, nachhaltigen und sicheren Wirtschaft, vor allem im Mobilitätssektor.

DIE AKTUELLE LAGE

Digitale Trends in der Mobilität bergen Chancen und Risiken

- Moderne Fahrzeuge produzieren bereits heute eine große Menge an Daten, die in der Regel immer personenbezogen sind, soweit diese mit der Fahrzeugidentifikationsnummer („FIN“) verbunden sind. Hieraus ergeben sich besondere rechtliche Anforderungen für die Nutzung und das Management dieser Daten hinsichtlich Datenschutz und Security, welche wiederum Auswirkungen auf die Betriebs- und Verkehrssicherheit der Fahrzeuge haben.
- Im Rahmen der Car2Car- und Car2Infrastructure-Kommunikation ist die Bereitstellung von Verkehrs- und Fahrzeugdaten von Bedeutung, die allen Verkehrsteilnehmern zugutekommt sowie den Betrieb sicherheitsrelevanter Dienste gewährleistet. Fahrer können damit eine aktuelle Übersicht der Verkehrslage oder frühzeitige Warnungen vor Gefahrenstellen erhalten.
- Mobilität wird heute verkehrsträgerübergreifend verstanden. Es gibt viele Situationen, in denen Straßenbahnen, Züge, Schiffe und Flugzeuge (auf der Rollbahn) die Verkehrswege von Fahrzeugen kreuzen. IoT-Visionen zukünftiger Mobilität beinhalten die Kommunikation und Bereitstellung von Daten zwischen allen Verkehrsträgern (Car2X, V2X, Rail2X, Ship2X, Airplane2X etc.)
- Im Regelfall werden Daten von Sensoren und Fahrzeugkomponenten heute direkt über eine Mobilfunkschnittstelle zum Server eines Fahrzeugherstellers übertragen, wo sie nur eingeschränkt von Drittanbietern genutzt werden können. Der Hersteller verfügt heutzutage somit über einen privilegierten Zugang und Einblick in die Daten und Datenströme anderer Marktteilnehmer. Dies birgt nicht nur das Risiko einer unzulässigen Datengenerierung und -speicherung durch diesen Informationsaustausch, sondern vor allem das einer Wettbewerbsverzerrung.

- Die zunehmende Vernetzung von Fahrzeugen birgt neben Potenzialen grundsätzlich auch neue Risiken im Bereich der IT- und Datensicherheit. Die Kommunikationsstellen einzelner Fahrzeugmodelle sind Zielscheiben für Cyberangriffe, da in die sensibel sicherheitsrelevante Steuerung der Fahrzeuge eingegriffen werden kann.

UNSERE POSITIONEN

Zugang und Bereitstellung von Mobilitätsdaten ermöglichen – sicher, neutral und standardisiert

- Technische Überwachung der TÜV im Zeitalter der digitalen vernetzten Mobilität heißt konkret: Daten von Einzelnen und Unternehmen zu schützen, das Recht auf sichere Übertragbarkeit von Daten technisch zu realisieren, Schaden von Personen, Unternehmen und Infrastrukturen abzuwenden und ein zuverlässiges Fundament durch unabhängige Prüfungen und Zertifizierungen zu schaffen, in dem das Vertrauen in eine vernetzte digitale Welt verankert und fairer Wettbewerb ermöglicht werden kann.
- Hinsichtlich der notwendigen Security-Absicherung müssen Fahrzeughersteller eine einheitliche, in ihrem Ansatz generische und hochsichere Sicherheitsarchitektur in neuen Fahrzeugen vorsehen, um den Manipulationsschutz der elektronischen Steuergeräte, Komponenten und Systeme zu verbessern.
- Entscheidend bleibt, dass die Fahrzeugnutzer (Betroffene im Sinne von Art. 4 Nr. 1 EU-DSGVO) selbst die Wahl haben, wie sie mit ihren Daten umgehen möchten, sofern es sich nicht um gesetzlich geregelte Daten handelt. Darum müssen die Kunden cloudbasierter Dienstleistungen ganz bewusst entscheiden können, welche Daten sie preisgeben und was mit ihren Daten passiert.
- Vorbehaltlich der vorherigen Zustimmung der Fahrzeugnutzer sollten alle Dienstleister im Mobilitätssektor in gleicher, fairer, angemessener und diskriminierungsfreier Position sein, um Dienstleistungen für die Fahrzeugnutzer anzubieten.
- Zur Wahrnehmung speziell hoheitlicher bzw. öffentlicher Aufgaben im Rahmen der technischen Überwachung durch die TÜV muss ein vollumfänglicher, diskriminierungsfreier Zugriff auf originäre Fahrzeugdaten *over-the-air* gewährleistet sein. Hoheitliche Aufgaben umfassen den Ereignisdatenspeicher („Fehlerspeicher“) im Fahrzeug, die technische Fahrzeugprüfung und die Überwachung des Abgasverhaltens des Fahrzeugs.
- Der Zugang zu Fahrzeugdaten sowie deren Speicherung und Verwaltung sollte über herstellerunabhängige cloudbasierte neutrale Datentreuhänder, genannt TrustCenter, erfolgen. Ein neutrales TrustCenter für Fahrzeugdaten sorgt für einen hochsicheren, authentischen Zugang zum vernetzten Fahrzeug. Dazu gehören ein Identitäts- und Autorisierungsmanagement für den Zugriff auf Daten aus vernetzten Fahrzeugen aller Verkehrsträger, damit nur autorisierte Berechtigte Zugriff auf sensible Daten haben.
- Die EU-Kommission ist gefordert, rechtliche Grundlagen für ein faires und sicheres Mobilitätsdatenmanagement im Europäischen Binnenmarkt zu etablieren. Ziel muss es sein, das europäische Wettbewerbsrecht zu modernisieren sowie dessen rechtliche Grundlagen im Digitalbereich zu harmonisieren und zusammenzuführen.

Kontaktdaten

Ansprechpartner: Richard Goebelt
E-Mail: richard.goebelt@vdtuev.de
Tel.: +49 151 120 396 90
www.vdtuev.de/europawahl-2019/