wdk
POSITION

Antworten der Kautschukindustrie zum *„Fragenkatalog im Nachgang zum Stakeholderdialog am 17.10.2024“*

Datenerfassung und -speicherung

1. Welche Arten von Daten werden von Fahrzeugen erfasst? (Kategorisieren nach Diagnosedaten, Nutzerdaten, originären Fahrzeugdaten etc.)
2. Wie und wo werden diese Daten gespeichert?
3. Wie wird mit aggregierten Daten verfahren? Werden Dritten aggregierte Daten zur Verfügung gestellt?
4. Haben Dritte die Möglichkeit, Daten im gleichen Umfang wie der Fahrzeughersteller zu erhalten? Welche Unterschiede zeichnen sich ab?
5. Unter welchen Voraussetzungen und in welchem Umfang wird aktuell Dritten ein direkter Zugriff auf im Fahrzeug verarbeitete oder gespeicherte Daten sowie auf Funktionen und Ressourcen (DFR) des Fahrzeugs gewährt? Welche konkreten Hürden und Anforderungen gibt es?
6. Welche Datenübertragungstechnologien werden genutzt und welche Standards bzw. Schnittstellen existieren für die Datenübertragung vom Fahrzeug in das OEM-Backend sowie für den Datenaustausch zwischen Fahrzeugen verschiedener Hersteller und Modelle?
7. Mit welchen Technologien und sonstigen Verfahren oder Anforderungen werden Fahrzeugdaten geschützt, auf die Dritten ein direkter Zugriff gewährt wird? In welcher Hinsicht unterscheiden sich diese Technologien, Verfahren und Anforderungen vom direkten Zugriff der OEM auf Fahrzeugdaten?
8. Wie wird aktuell sichergestellt, dass Fahrzeugdaten nur für legitime Zwecke verwendet werden? Welche Maßnahmen werden ergriffen, um die Privatsphäre bzw. den Datenschutz der Fahrzeugnutzer zu gewährleisten?

wdk
Wirtschaftsverband der deutschen Kautschukindustrie e. V.
Zeppelinallee 69 • 60487 Frankfurt am Main
Tel. +49 69 7936-0 • Fax +49 69 7936-140
info@wdk.de • www.wdk.de

wdk:

Diese Fragen müssen von der Fahrzeugindustrie, den OEM, beantwortet werden. Die Antworten sollten aber allen Stakeholdern zu Verfügung stehen, da nur so eine lösungsorientierte Diskussion stattfinden kann.

II. Anforderungen an eine potenzielle EU-Sektor-Regulierung (SSL)

1. Welchen Anwendungsbereich sollte eine mögliche SSL haben? Wo besteht ein Regelungsbedarf bzw. existiert eine Regelungslücke?
2. Welchen Anwendungsumfang sollte eine mögliche SSL haben? Welche Zugänge zu DFR werden konkret benötigt und von wem?
3. Welche dieser zusätzlichen Daten könnten sicherheitskritisch sein und warum? Wie kann sichergestellt werden, dass nur zugriffsberechtigten Dritten der Zugang zu DFR gewährt wird?
4. Können Sie konkrete use-cases benennen, für die ein direkter Zugriff auf Fahrzeugdaten, Funktionen oder Ressourcen für erforderlich erachtet wird? Falls möglich, wie müsste ein alternativer Zugang zu Fahrzeugdaten ausgestaltet sein, um die genannten use-cases unter gleichen Wettbewerbsbedingungen zu ermöglichen?
5. In welchen use-cases wird auch ein schreibender Zugriff auf Fahrzeugdaten für notwendig erachtet? Wenn ja, in Bezug auf welche Daten? Welche Daten davon sind sicherheits- bzw. typgenehmigungsrelevant?
6. Wie hoch wäre der Aufwand für die Bereitstellung dieser zusätzlichen Daten?
7. Welche Standards oder Schnittstellen sollte die SSL definieren (z.B. Mindestdatensatz, Formate etc.)? Wie könnte die Definition ausgestaltet werden?
8. Welche Rahmenbedingungen sollten für den Zugang gelten? Welche bestehenden Konzepte des Datenzugangs könnten auch im Rahmen der SSL relevant sein? Wie können bestehende Konzepte mit einer SSL verbunden werden?
9. Gibt es weitere wichtige Punkte, die eine SSL regeln sollte?

wdk:

Wie im Papier vom 15. Oktober 2024 erläutert, reicht der Data Act nicht aus und der Sektor benötigt eine SSL.

Die sektorspezifische Regulierung (SSL) auf EU-Ebene adressierte in den letzten bekannten Diskussionsständen exakt diejenigen Lücken, die der allgemeine Data Act für die Arbeit im digitalen und digitalisierten Automotivsektor aufwies:

1.) Die SSL definierte in Ergänzung des „Lesen von Daten“ aus dem Fahrzeug nach dem Data Act, wie die eigentliche digitale Leistungserbringung am und im Kfz erfolgen sollte. Dies geschieht im Software Defined und Controlled Vehicle immer durch das Aufrufen von Funktionen unter Nutzung von Ressourcen wie Speicherplatz und Bandbreite. So werden neue Apps im Fahrzeug installiert, neue Ersatzteile angelernt und neue Updates eingespielt.

2.) In Bezug auf Sicherheit und Verantwortung forderte die SSL konsequent ein einheitliches Cyber Security Management System, ein Produktüberwachungssystem nach höchsten Sicherheitsstandards für alle „intelligenten Services“, die am oder im Kfz eingesetzt werden. […]

[…] die SSL forderte daher, dass für jede Serviceart und für jede Software,

gleich, auf welche Daten, Funktionen und Ressourcen sie im Fahrzeug an bestimmten Integrationspunkten (ExVe-Backend, OBD-Port, Kfz-Infotainment, On-Board-Zentralcomputer wie ICAS) Zugriff hatte, ein einheitlicher Satz an Testprozessen und Testkriterien anzuwenden war.

Auch hier wurde nur nach Bestehen der Tests das Zugangszertifikat erteilt und erst dann Service und Serviceanbieter in das Cyber Security Management System und Produktmanagementsystem des Herstellers integriert.

Damit beantwortet die SSL für den Kfz-Sektor exakt die kritischen Fragen nach Sicherheit und Verantwortung, die im Data Act unbeantwortet blieben. […]

III. Verhältnis zu anderen Regulierungen

1. Der Data Act stellt die Grundlage für eine mögliche SSL dar. An welchen Stellen gibt es Ergänzungsbedarf? An welcher Stelle sollte es vom Data Act abweichende Regelungen geben? An welcher Stelle sollte an gesetzgeberischen Entscheidungen des Data Act festgehalten werden? An welcher Stelle könnten sich potenzielle Kollisionen oder Widersprüche ergeben?
2. Sehen Sie weitere mögliche Synergien oder Widersprüche zu bestehender Regulierung oder Regulierungsvorhaben (z.B. Anh. X der Typgenehmigungs-Verordnung)?

wdk:

Der Data Act beschreibt […] lediglich eine Einbahnstraße, nämlich das Bereitstellen und Lesen von der Datenquelle Kfz durch den Hersteller zum Kunden und von dort hin zum Dienstanbieter. Weiter eingeschränkt wird die Menge an Daten, die über diese Einbahnstraße transportiert werden dürfen/müssen, durch Vorbehaltsrechte am geistigen Eigentum und etwaige Verbote, auf Basis dieser Daten gleichwertige Produkte zu entwickeln.

Im Ergebnis sichert ein ideal umgesetzter Data Act demnach maximal einen eingeschränkten Lesezugriff auf ein Kundenfahrzeug. […]

[…] Über [einen] Rückweg im Rahmen einer digitalen Serviceerbringung im Software Defined Vehicle sagt der Data Act leider an keiner Stelle etwas aus.

Frankfurt, Januar 2025