Gesamtverband Autoteile-Handel

Fragenkatalog im Nachgang zum Stakeholderdialog am 17.10.2024

I. Datenerfassung und -speicherung

1. Welche Arten von Daten werden von Fahrzeugen erfasst? (Kategorisieren nach Diagnosedaten, Nutzerdaten, originären Fahrzeugdaten etc.)

Nach unserem Verständnis richtet sich der gesamte Abschnitt I an die Fahrzeughersteller. Unserer Auffassung nach können diese Fragen auch nur von diesem vollständig und abschließend beantwortet werden. Als Interessenvertreter des freien Fahrzeugteile-Handels sehen wir daher von einer Beantwortung ab.

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?

Zur Formulierung der Fragestellung „Daten …erhalten" möchten wir anmerken, dass eine Diskussion zu kurz greift, die nur auf einen „Lesezugriff" gerichtet ist, sofern dies gemeint sein sollte. Unabhängig davon, ob eine Unterscheidung nach Lese- und Schreibzugriff überhaupt sachgerecht ist, dürften die für den Kfz-Teilehandel überragend wichtigen Vorgänge des Anmeldens, Anlernens und Decodierens neu in das Fahrzeug eingebauter Ersatzteile in jedem Falle einen Schreibzugriff darstellen.

Im Übrigen erwartet der Kunde die Lösung eines bestehenden Problems rund um das Fahrzeug, nicht nur dessen bloße Beschreibung („System Crash Report"). Er erwartet – ganz allgemein gesprochen - eine Verbesserung des bestehenden Zustands. Eine Verbesserung stellt eine Veränderung dar, weswegen bei Services im Kfz-Bereich ein schreibender Zugriff den Normalfall darstellen dürfte.

Wir sind auch der Meinung, dass die Fragestellung das Kriterium „Qualität" enthalten muss, um ein „level playing field" zur Entwicklung digitaler Dienste im und rund um das Fahrzeug zu schaffen.

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?

Die Formulierung „Direkter Zugriff" ist missverständlich und wurde in der Form auch nicht vom Kfz-IAM gefordert. Sinnvoller erscheint die Unterscheidung zwischen Onboard- und Offboard-Zugriffen.

Derzeit ist ein Onboard-Zugriff in der Regel über den OBD-Port möglich. Einschränkungen der Zugangsmöglichkeiten über den OBD-Port waren uns sind jüngst Gegenstand gerichtlicher Verfahren.

Denn, obwohl von den einschlägigen Verordnungen nicht zugelassen, kommt es seitens der OEMs immer wieder zu Einschränkungen, Behinderungen und Diskriminierungen von Dritten beim Thema Zugriff über den OBD-Port.

Gesamtverband Autoteile-Handel

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?

Im Zusammenhang mit dieser Frage legen wir großen Wert auf die nochmalige Feststellung, dass der Kfz-IAM KEIN neues Zugriffssystem für sich selbst von den Fahrzeugherstellern fordert. *Gleiches gilt für Sicherheitsvorschriften, Entwicklungs- und Betriebsprozesse.*

Der Kfz-IAM fordert lediglich Gleichbehandlung in Bezug auf die Zugangskanäle, die auch der Fahrzeughersteller für dessen Aftermarket-Angebote nutzt.

Die dem Fahrzeughersteller obliegenden Schutzmaßnahmen ziehen wir im Grundsatz nicht in Zweifel. Der Kfz-IAM akzeptiert Sicherheitskonzepte, sofern es sich dabei um die gleichen handelt, die der Fahrzeughersteller für sich oder seine Zulieferer anwendet.

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?

An dieser Stelle erlauben wir uns den Hinweis, dass die DSGVO schon seit Jahren unmittelbar und abschließend gilt und ein entsprechendes Nutzer-Consent-Management-System für alle Akteure selbstverständlich ist. Darüber hinausgehende Vorschriften zum Schutz von Nutzerdaten sind nicht erforderlich.

Auf der anderen Seite gelten aber auch Typgenehmigungsverordnung und Kfz-GVO. Diese Vorschriften dürfen nicht gegeneinander ausgespielt werden.

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?

In Anknüpfung an die Typgenehmigungsverordnung und die Kfz-GVO muss eine SSL zukunftssicher dem technischen Fortschritt entsprechend Wettbewerb für Angebote im (Apps; Kfz-Teile) und am Fahrzeug (Wartung, Reparatur, Pannenhilfe usw.) festschreiben. Dies bedeutet, dass IAM-Akteure diesbezügliche Ansprüche unmittelbar gegen Fahrzeughersteller geltend machen können müssen.

Jeder Datenzugriff muss nach den gleichen Standards auf die gleichen Systeme gewährt werden, wie sie der Fahrzeughersteller für dessen Angebote nutzt.

Im Rahmen einer SSL wird dagegen NICHT gefordert, neue Systeme oder Prozesse für den IAM zu entwickeln oder zu implementieren. Es soll lediglich das bereits Bestehende genutzt bzw. „geöffnet" werden.

Letztlich ist im Ergebnis nicht entscheidend, ob man Handlungsbedarf begrifflich aus einer Regelungslücke oder aus Marktversagen herleitet. Aus unserer Sicht ist der Zugang zu Fahrzeugdaten, Funktionen und Ressourcen bisher nicht grundsätzlich geregelt. Eine Regelungslücke besteht in der Regel dort, wo der Gesetzgeber seinen Willen zur Regelung durch bereits bestehende konkrete gesetzliche Vorschriften zum Ausdruck gebracht hat, dabei aber bestimmte Fälle von diesem unabsichtlich übersehen wurden. Der Zugang zu Fahrzeugdaten etc. ist aber mit 858, Gruppenfreistellungsverordnung und Data Act nur fragmentarisch, nicht grundsätzlich geregelt.

Wir halten daher "Regelungsbedarf durch Marktversagen" für begrifflich zutreffender. Wettbewerb im Kfz-Aftermarket ist vom Gesetzgeber im Sinne bezahlbarer Mobilität gewollt.

Unabgängig davon, wofür man sich hier begrifflich entscheidet, reicht das bisherige Regelwerk nicht aus. Es besteht dringender gesetzgeberischer Handlungsbedarf.

2. Welchen Anwendungsumfang sollte eine mögliche SSL haben? Welche Zugänge zu DFR werden konkret benötigt und von wem?

In Ergänzung zu der zuvor beantworteten Frage muss eine SSL die Entwicklung innovativer Services mit direkter Kommunikationsmöglichkeit mit dem Fahrzeugnutzer durch den Kfz-IAM ermöglichen.

3. Welche dieser zusätzlichen Daten könnten sicherheitskritisch sein und warum? Wie kann sichergestellt werden, dass nur zugriffsberichtigten Dritten der Zugang zu DFR gewährt wird?

Selbstverständlich muss der Fahrzeughersteller „fremde" Software, die Zugriff auf eines der auch von ihm genutzten Systeme erhält, vorab prüfen und freigeben können. Dies darf aber nicht dazu führen, dass Dritten der Zugriff auf ein System mit dem Verweis darauf, dieses sei grundsätzlich sicherheitskritisch, generell verweigert wird.

Es spricht ohnehin einiges dafür, bei einem modernen vernetzten Fahrzeug davon auszugehen, dass sich eine kategorische Unterteilung in „sicherheitsunkritisch" und „-kritisch" gar nicht vornehmen lässt.

Dafür, Dritte als weniger kompetent oder vertrauenswürdig einzustufen, gibt es keine sachliche Grundlage. So werden On-Board-Diagnose-Systeme meist nicht von den Fahrzeugherstellern selbst, sondern von Zulieferern entwickelt.

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?

Für faire Wettbewerbsbedingungen benötigt der Kfz-IAM alles das, was auch den Fahrzeughersteller-Netzen zur Verfügung steht. Das bedeutet: Gleicher Zugriff auf die gleichen Systeme nach gleichen Prozessen.

Gesamtverband Autoteile-Handel

Für den Kfz-Teilehandel sind wichtige Anwendungsfälle insbesondere die Ersatzteileidentifikation sowie das Anmelden, Anlernen und Decodieren von neu eingebauten bzw. neu einzubauenden Kfz-Ersatzteilen.

Funktioniert dies nicht, wird daraus zunächst ein aufwändiger Warenretouren- bzw. Reklamationsfall (ggfs. Sachmängelgewährleistung). Kurzfristig wirkt sich dies negativ auf die Nachhaltigkeitsbilanz auf (Transport). Langfristig werden diese Ersatzteile nicht wieder bestellt und drohen vom Markt zu verschwinden. Dies hat wettbewerbsschädigende Wirkung, da das Angebot schrumpft, Teilemonopole entstehen und die Preise für diese Teile nicht mehr vom Markt bestimmt werden. Reparatur und Wartung verteuern sich, Mobilität wird für viele nicht mehr bezahlbar.

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?

Wir verweisen hier auf unsere Beantwortung von Frage I. 4. Schon das Anmelden, Anlernen, Decodieren eines neu eingebauten Ersatzteils am Fahrzeug stellt einen Schreibzugriff dar. Der Wettbewerb bei Reparatur und Wartung ist auch in Bezug auf die Typgenehmigungsverordnung relevant.

6. Wie hoch wäre der Aufwand für die Bereitstellung dieser zusätzlichen Daten?

Der Kfz-IAM fordert für sich keine Sonderlösung! Es geht um bereits bestehende Fahrzeuge und deren existierende Struktur. Daten etc. stehen den Vertragsbetrieben bereits zur Verfügung.

7. Welche Standards oder Schnittstellen sollte die SSL definieren (z.B. Mindestdatensatz, Formate etc.)? Wie könnte die Definition ausgestaltet werden?

Mit einer SSL müssen ein einheitliche Standards zum Zugang zu Fahrzeugdaten, -funktionen und -ressourcen definiert werden. Man wird davon ausgehen müssen, dass diese Standards der fortwährenden Weiterentwicklung bedürfen.

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?

Jedes aktuelle und künftige vom Fahrzeughersteller für dessen Services genutzte System in Bereichen, für die vom Gesetzgeber Wettbewerb vorgesehen ist, muss nach den gleichen (Zugangs-)Regeln für Wettbewerber nutzbar sein.

ExVe und ADAXO erfüllen die Anforderungen als Offboard-Modelle eines Gatekeepers und gleichzeitig Wettbewerbers am Markt nicht.

9. Gibt es weitere wichtige Punkte, die eine SSL regeln sollte?

Gesamtverband Autoteile-Handel

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?

Da der Data Act von vornherein auf Daten beschränkt ist und der Weg über den Gerätebenutzer führt, sehen wir in dem Data Act keine Grundlage für eine SSL. Der Anwendungsbereich einer SSL muss materiellrechtlich umfangreicher sein (auch Funktionen, Ressourcen; Schreibzugriff; originär eigene Anspruchsgrundlagen für IAM-Akteure gegen „Dateninhaber"), daher müssen diese beiden Vorschriften aus unserer Sicht in der Systematik der Gesetzgebung gleichberechtigt nebeneinander und nicht „übereinander" stehen.

2. Sehen Sie weitere mögliche Synergien oder Widersprüche zu bestehender Regulierung oder Regulierungsvorhaben (z.B. Anh. X der Typgenehmigungs-Verordnung)?

Die Kfz-GVO und ihre Leitlinien sowie Art. 64 ff. der Typgenehmigungsverordnung 2018/858 wurden hier bereits angesprochen. Diese wettbewerblichen Zielsetzungen sollten mit einer SSL weiterentwickelt werden.

Eine bloße „Legalisierung" der Secure Gateways für die Zukunft im Rahmen eines Delegated Act zum Anhang X der Typgenehmigungsverordnung stünde im Widerspruch zu den Zielsetzungen einer SSL.