Der Automotivesektor braucht eine sektorspezifische Regulierung

Managementzusammenfassung

Die unterzeichnenden Verbände fordern die deutschen Ministerien dringend dazu auf, die vorbereitete sektorspezifische Regulierung für den Zugang zu Daten, Funktionen und Ressourcen (SSL) zügig auf europäischer Ebene umzusetzen. Eine Umsetzung ist für den Erhalt der Wettbewerbsfähigkeit des europäischen Automotivesektors gegenüber den Herausforderern aus USA und China essenziell. Nur hierdurch wird ein innovativer europäischer Digitalmarkt im Bereich Automotive für komplexe digitale Services im Kfz geschaffen. Der Data Act reicht wegen seines begrenzten Fokus auf das reine Datenlesen und Datenverteilen hierzu nicht aus. Erfolgt keine sektorspezifische Regelung, ist bereits heute absehbar, dass die isolierten Bemühungen einzelner OEMs aufgrund der Gesetze der Plattformökonomie of Scale weiter in der Bedeutung hinter die Angebote der deutlich größeren Player aus China und den USA zurückfallen werden.

Einleitung

Der Automotivesektor wird im Zuge des technischen Fortschrittes zunehmend digitalisiert. Diese Digitalisierung läuft allerdings in diesem typischen Industriesektor deutlich anders ab, als es zum Beispiel der Verbraucher in seinen Erfahrungen aus dem Bereich Social Media, Internetsuche oder Online-Shopping gewohnt ist.

Im Automotivesektor ist derzeit noch keine Online-Transaktionsplattform wie Amazon existent, auf der Endkunden zum Bestpreis jedes Modell jeder Marke erwerben können. Niemand im Sektor hat derzeit einen so tiefen Kundeneinblick wie zum Beispiel Meta (Facebook, Instagram) oder Google (Suchmaschine), welche täglich genutzt werden, Unmengen von Daten generieren und über datenbasierte Geschäftsmodelle wie beispielsweise individuelles Marketing-Milliardenumsätze für diese sehr wenigen Marktteilnehmer generieren.

Der letztgenannte Fakt ist kritisch. Beim Blick auf die Milliardenumsätze von Meta wird oft vergessen, wie viele tatsächliche Nutzer hierzu notwendig sind und wie gering der Umsatz pro Nutzer im Jahr ausfällt. Instagram erzielte 2023 etwa 60 Mrd. Umsatz, benötigte dafür aber auch 2.1 Milliarden Nutzer, was etwa einem Umsatz von 30 Euro pro Nutzer und Jahr entspricht. Selbst diese Umsatzgröße wurde nur deswegen erreicht, weil die Relevanz von Instagram weltweit so bedeutend ist. Hieraus kann schlussgefolgert werden, dass das reine Geschäft mit „datenbasierten Geschäftsmodellen“ deutlich kleiner ist und deutlich weniger Akteure zulässt als oft angenommen.

Ein Vergleich der Umsatzstruktur im Kfz-Sektor zeigt hierzu deutliche Unterschiede, da der Sektor ganz anders aufgestellt ist. Eine einzelne Inspektion eines Autos unterschreitet selten den Wert von 300 Euro (und liegt damit um den Faktor 10 oder eine Größenordnung über den Instagram-Jahresumsätzen pro Kunde), ein Neuwagen kostete im Durchschnitt 2023 den Rekordpreis von 44.630 Euro, also mehr als das 1000-fache des Instagram Jahresumsatzes pro Kunde. Im Ergebnis führt dies dazu, dass sich von der Produktion (Zulieferer, OEMs) bis zu Vertrieb, Betrieb und Wartung deutlich mehr Unternehmen unabhängig am Markt etablieren konnten.

Zwei weitere Unterschiede zwischen den Märkten für Social Media und dem Automotive-Sektor zeigen sich im Systemdesign und in der Kritikalität. Für die „kundenindividuelle Werbung“ als wichtigste Einnahmequelle für Meta oder auch Google reicht ein nur lesender Zugriff auf die Kundendaten völlig aus:

Was hat der Kunde bisher auf Google gesucht, welchen Kanälen folgte er auf Instagram? Mit diesen Informationen können sodann Werbeanzeigen versteigert werden (Microbidding auf Google), die dem suchenden Kunden vor seinen Suchergebnissen präsentiert wurden. Die Risiken sind hier hochgradig überschaubar. Im schlimmsten Fall wird aus Sicht des Werbetreibenden die Werbeanzeige ignoriert, im schlimmsten Fall aus Sicht der Plattform Google ist der Kunde von der Werbung derart genervt, dass er auf eine andere Suchmaschine wechselt.

Deutlich anders sind die Herausforderungen im Automotivesektor. Hier müssen die Softwareapplikationen als App im Infotainmentsystem, als Diagnosesoftware auf externen Testgeräten oder als Steuersoftware auf komplexen Ersatzteilen (wie Xenon-Scheinwerfern mit intelligentem Kurvenlicht) nicht nur in sich stabil und sicher sein, sondern auch über die Lebenszeit des Kfz mit der Softwareumgebung im Kfz, die ebenfalls Patches und Updates unterworfen ist, interagieren. Da die Integration im Software Defined Vehicle ebenfalls ständig steigt, werden deutlich mehr Verbundprobleme und Quereffekte durch die Kunden berichtet, mit deren Behebung Hersteller und Werkstätten zunehmend überfordert sind. Ebenso wirft dies auch noch nicht geklärte rechtliche Fragen zur Haftung auf, beispielsweise wenn Updates an Komponente X durch den Anbieter Y zu Ausfällen des gesamten Fahrzeuges und zu Schäden an ganz anderen Komponenten geführt haben. Ungewollte Beeinträchtigungen des Verhaltens für autonome Fahrfunktionen sind hier sicherlich das kritischste Szenario.

Zusammengefasst lässt sich feststellen, dass sich der Sektor Automotive in Bezug auf Systemdesign, Kritikalität, aber auch in den Größen Umsatzstruktur und Geschäftsmodelle deutlich anders darstellt als beispielsweise der Sektor Social Media. Wir sind uns dieser Unterschiede bewusst und gehen nachfolgend konkreter darauf ein, wie wir vor allem das unterschiedliche Systemdesign und die höhere Kritikalität von Komponenten im Automotivbereich adressieren.

Warum der Data Act nicht ausreicht

Der Fokus des Data Acts liegt laut dessen Artikel 1 im Bereitstellen von Daten durch den Dateninhaber für den Nutzer, der diese dann auch an Dritte weiterleiten darf. Für den Bereich Kfz bedeutet dies, dass Daten aus dem Produkt Kfz, die dem faktischen Dateninhaber (dem OEM) vorliegen, dem Nutzer des Produktes (Fahrer/Eigentümer) zur Verfügung gestellt werden müssen, welcher sie dann an berechtigte dritte Parteien weiterleiten darf.

Etwas vereinfacht beschreibt der Data Act daher 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.

In Analogie zu den Geschäftsmodellen der verhaltensbasierten Werbung könnte – in idealer Kenntnis aller Vorgänge im Kfz – dem Kunden auf der Datenbasis des Data Acts bisher neben Empfehlungen zu Tank- und Ladestopps höchstens eine nächste Wartung angeraten werden (Predictive Maintenance). Viel mehr ist aus Sicht eines dritten Diensteanbieters aus dem Sektor nicht möglich.

Die Probleme mit den Ansprüchen aus dem Data Act zeigen sich dann beim „Rückweg“.

Kunden bezahlen einen Dienstanbieter nicht allein wegen der Empfehlung, einen Ladestopp einzulegen oder wegen einer Fehlerdiagnose, nach der eine Komponente im Kfz defekt ist. Sie bezahlen dann, wenn sich durch die Handlung eines Dienstanbieters ihr Fahrzeugzustand verbessert hat, mithin das E-Auto geladen oder das Ersatzteil eingebaut worden ist.

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

Dies fällt umso mehr ins Gewicht, als dass durch die schweren Bedrohungen durch Cyberkriminalität eine dringende Notwendigkeit entstanden ist, grundsätzlich jeden (!) Zugriff auf das Fahrzeug nach sorgfältiger Risikobewertung mehrstufig abzusichern.

Die gesetzliche Grundlage hierfür sind die UNECE-Regulierungen 155/156, in deren Folge bereits Maßnahmen wie beispielsweise die Verschlüsselung des OBD-Ports als zentralem Zugang in der Werkstatt oder die Codierung von Ersatzteilen umgesetzt worden sind.

Für einen Serviceanbieter stellt die aktuelle Situation daher als äußerst unbefriedigend dar: Ein „Ansehen“ ist nach Maßgabe des Data Acts erlaubt, ein „Anfassen“ im Sinne eines gewünschten Zugriffs durch den Kunden wird vom OEM unter Hinweis auf das aus Sicherheitsgründen „abgeschlossene“ Kfz jedoch verwehrt.

Als zentrale Argumente von Gesetzgeber und OEM werden hierbei Sicherheit und die Zuweisung von Verantwortung angeführt. Diese sind valide und sollen daher auch nicht angezweifelt werden.

Zur Sicherstellung von Sicherheit und Verantwortung kommen in allen Prozessphasen und auf allen Ebenen der digitalen Leistungserbringung stets zwei zentrale Konzepte zum Einsatz:

- Authentifizierung
- Autorisierung

Authentifizierung klärt die Frage: „Wer bist Du?“ und dient vorrangig der Zuweisung von Verantwortung. Jeder Mitarbeiter in der Werkstatt, jedes intelligente Ersatzteil und jede Software am und im Auto muss in ihrer jeweiligen Version zunächst eindeutig identifiziert sein.

Autorisierung klärt die Frage: „Was darfst Du?“ und fördert die Sicherheit im Auto. Nur nachdem ein Mitarbeiter, ein Ersatzteil oder eine App eine Vielzahl von Sicherheits-, Qualitäts- und Funktionstests durchlaufen hat, die ein Hersteller auf der Basis von gesetzlichen Vorgaben und/oder eigenen Qualitäts- und Sicherheitsstandards für diese Serviceart vorgeschrieben hat, erhält der Mitarbeiter, die App oder das Ersatzteil die Zugangsberechtigung zur Arbeit am Kfz, bzw. zur Verwendung am oder im Kfz.

Überspitzt ausgedrückt existiert exakt ein relevanter Datenpunkt: Die elektronische Zugangsberechtigung zur Verwendung eines Services (App, Ersatzteil etc.) am Kfz, die im Cyber Security Management System und im Produktverfolgungssystem eines Herstellers eingetragen wird.

Offensichtlich ist jedoch, dass diese „Zugangskarten“ nicht ohne Weiteres in großer Zahl an beliebige Kunden und Drittanbieter bereitgestellt werden können, wie in Artikel 1 des Data Acts beschrieben ist.

Stattdessen werden Sie als zeitlich begrenzte Zugangskarte im Ergebnis einer aufwändigen und sich im Fallen von Updates ständig wiederholenden Prüfung auf Betriebssicherheit vom OEM vergeben und können bei Nichtbestehen einer Prüfung auch wieder jederzeit widerrufen werden.

Warum der Sektor eine SSL braucht

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.

Zur Begründung des einheitlichen Sicherheits- und Zugangssystems

Im Software Defined Vehicle mit seinen permanent der Veränderung durch Updates bestimmten Lebenszyklus existieren keine technischen Grenzen zwischen Primär- und Aftermarket mehr. Wie bei Mobiltelefonen oder Laptops werden die gleichen Modelle (iPhone 15) schon über die Produktionszeit hinweg mit unterschiedlichen Softwareständen der einzelnen Zulieferer ausgeliefert. Nach erfolgtem Verkauf spielen sowohl Hersteller und Zulieferer als auch die App-Anbieter ständig neue Versionen/Updates „Over the Air“ ein. Die Marktsegmente wachsen technisch zusammen. Deshalb kann und darf es auch keine zwei unterschiedlichen Sicherheitsstufen geben.

Exakt, wie weiter oben beschrieben, forderte die SSL 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 Testprozesse und Testkriterien anzuwenden waren.

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.

Was die SSL nicht ist

Da die SSL oft als ein „Sektorspezifischer Data Act“ missverstanden wird, wird in diesem Zuge die Befürchtung geäußert, in der SSL würde die Offenlegung weiterer Datenpunkte vom OEM gefordert und ginge damit über die Anforderung des Data Acts hinaus.

Dies ist ausweislich der letzten Diskussionsstände nicht der Fall und würde – wie oben dargelegt – auch keinen erkennbaren Sinn ergeben. Das Problem im digitalen Sektor Automotive ist nicht die Bereitstellung von zu wenigen Daten, sondern die unklare Regelung bezüglich digitaler und digitalisierter Produkte, die auf Basis dieser Daten zum Einsatz kommen und wie der Zugang dieser Produkte, also ihre Integration in und am Kfz stattfinden sollen.

Heruntergebrochen beschreibt der „Data Act“ den Zugang zu Daten aus einem System (z.B. Kfz), während die SSL den Zugang, der gegenüber Daten deutlich komplexeren Produkte und Services auf Basis dieser Daten in das System Kfz regelt.

Warum die Zeit für eine SSL drängt

Aus Sicht der Unterzeichner ist die SSL die einzige Möglichkeit und Chance, die dem europäischen Gesetzgeber noch bleibt, um einen konkurrenzfähigen Digital Single Market im Bereich Automotive zu etablieren. Die Europäische Kommission hat bereits einen Rechtsvorschlag erarbeitet. Das dazugehörige Impact Assessment wurde vom EU-Ausschuss für Regulierungskontrolle bereits im November 2023 genehmigt.

Wird die SSL nicht zügig auf europäischer Ebene umgesetzt, erscheint uns ein weiterer Bedeutungsverlust unserer Player gegenüber den größeren Playern aus USA und China als unvermeidlich.

Seit mindestens zehn Jahren (Start Android Auto und Apple CarPlay 2014) versuchen die europäischen Autobauer im neuen Sektor IT weitgehend vergeblich, eigene digitale Ökosysteme pro OEM aufzubauen:

Eigene Infotainmentlösungen wie MBUX, MB.OS (Mercedes), R-Link (Renault), SDL (Ford et al), GM NGI (General Motors) sollten fremde App-Entwickler anlocken, um den Erfolg von Apple und Google mit ihren App Stores zu wiederholen und „das nächste Google" im Automotivesektor zu werden. Parallel wurden für die „datenbasierten Geschäftsmodelle" nach dem Mantra „Daten sind das neue Öl", Herstellerbackends und Datenmarktplätze kreiert, aus denen neue, zusätzliche Einnahmequellen resultieren sollten. Schließlich nutzte man die durch die Technik mögliche Kontrolle über intelligente Ersatzteile, um mehr und mehr Ersatzteile zu höheren Preisen bei niedrigerem Innovationsdruck exklusiv anbieten zu können.

Heute kann zu diesen Punkten wie folgt konstatiert werden: Die eigenen Infotainmentlösungen der Hersteller sind entweder ganz vom Markt verschwunden (SDL, NGI, R-Link) oder basieren in den aktuellen Versionen unter der Haube auf dem Google-Angebot „Android Automotive". Ein zentraler Grund war jedes Mal die aus Sicht der App-Entwickler zu geringe Kundenzahl. Bei mehr als einer Milliarde Android-Usern entwickelt, kaum ein Entwickler etwas für die knappe Million von Mercedes-Fahrern, die eine neue Version von MB.OS einsetzen.

Bei den großen Datenmarktplätzen ist Wejo in die Insolvenz gerutscht (2023), Otonomo war 2021 mit 1,4 Milliarden Dollar bewertet und wurde 2023 für einen Wert von 70 Millionen in einem Asset Deal übernommen. Ausweislich der bei Northdata einsehbaren Zahlen sind auch Deutsche Pendants wie Caruso und High Mobility seit Jahren noch nicht profitabel. Der Hauptgrund neben uneinheitlichen Datenstandards und Dataverfügbarkeit der OEMs sowie unterschiedlichsten Preismodellen dürfte auch hier der zunehmend verschlossene Weg zurück ins Kfz gewesen sein.

OEM-Vertreter selbst bezeichneten den Erfolg des „Datenverkaufs über ExVE" als „Underwhelming", was nach den Ausführungen zu Beginn des Papers nicht überrascht. Daten sind eben keine Ressource neben dem Portfolio an digitalen und digitalisierten Services, sondern ein integraler Teil der digitalen Serviceerbringung über den kompletten Lebenszyklus des Services und des Kfz hinweg.

Am dramatischsten wird jedoch die Entwicklung im Ersatzteilemarkt verlaufen, die wegen der langen Lebenszykluszeit eines Kfz sich erst langsam bemerkbar machen wird. In Zeiten sinkender Neuwagenmargen haben alle Player versucht, die Margen im Aftermarketgeschäft zu erhöhen. Seit Jahren steigen die Ersatzteilpreise laut Studien des Gesamtverbandes der Versicherer deutlich über der Inflationsrate. Unter diesen stechen mit besonders drastischen Erhöhungen die Teile heraus, die ein Hersteller exklusiv anbieten kann. Exklusivität wird in Europa durch den Designschutz auf sichtbare Teile und technisch durch die beschriebene Kontrolle des OEM auf intelligente Ersatzteile garantiert.

Wenn also bereits jetzt europäische Kunden vor den hohen Neuwagenpreisen heimischer Anbieter zurückschrecken und beginnen, in China einzukaufen, wird sich dieser Trend noch einmal dramatisch verschärfen, wenn in den Vollkostenrechnungen von Verbraucherorganisationen demnächst ausgewiesen werden sollte, wieviel teurer typische Reparaturen bei heimischen Anbietern geworden sind im Vergleich zur Konkurrenz aus USA und Fernost.

Hier kann nach den Regeln der Marktwirtschaft nur eine SSL diejenige Konkurrenz und Innovation hervorbringen, die der europäische Automotivesektor heute benötigt.

Das Zulassen von alternativen Anbietern für Ersatzteile und Services heißt im Übrigen nicht, dass ein OEM dann an den Ersatzteilen und Services nichts mehr verdient. Ähnlich wie bei den

Plattformanbietern wie Amazon (Marketplace) und Apple/Google (AppStore) ist davon auszugehen, dass für den Vertriebsaufwand der Plattform Kfz und für den hohen Testaufwand der Services Vergütungen an den OEM zurückfließen, ggf. in der typischen Form einer Umsatzbeteiligung.

Wenn durch eine SSL eine grundsätzliche Zugangsberechtigung gegeben ist und die digitalen Geschäftsmodelle sich eingespielt haben, werden auch zwangsläufig die Standards entstehen und eingesetzt werden (wie z.B. der Vehicle Signal Standard des World Wide Web Councils), auf deren Basis sich dann preiswerter von allen Playern im Ökosystem entwickeln lässt. Dies kommt sodann auch dem Kunden/Verbraucher zugute.

Nur durch diese Öffnung (durch SSL) und eine folgende Standardisierung in wichtigen Teilbereichen kann ein Digital Single Market in Europa entstehen.

Passiert dies nicht, steht eine Uberisierung von Europa nach dem Vorbild des Smartphone-Marktes zu befürchten. Bei iPhones z.B. verkaufen deutsche Händler nur noch die Geräte und reparieren diese im Design aus den USA mit den Teilen, die in China gefertigt werden.

Eine überschaubare Wertschöpfung, der es durch eine SSL gegenzusteuern gilt.

ASA Bundesverband der Hersteller und Importeure von Automobil-Service-Ausrüstungen e.V.

Gesamtverband der Versicherer e.V.

Gesamtverband Autoteile-Handel e.V.

Verband der Internationalen Autovermieter e.V.

Wirtschaftsverband der deutschen Kautschukindustrie e.V.

Zentralverband Deutsches Kraftfahrzeuggewerbe e.V.

Zentralverband Karosserie- und Fahrzeugtechnik e.V.