VDA Verband der Automobilindustrie

Position

Entwurf EU-Verordnung Data Act vom 23.02.2022

Regulierung und Privatautonomie für die Datenwirtschaft

Berlin, Mai 2022

1. Executive Summary

- Der VDA unterstützt den datenwirtschaftsrechtlichen Ansatz des von der EU-Kommission vorgelegten Data Acts (DA), wonach für Verbraucher und sonstige dritte Unternehmen die Möglichkeit zum Datenzugang und zur Datennutzung gegeben sein soll.

- Die Automobilindustrie hat das Konzept „Extended Vehicle“ bereits erfolgreich eingeführt und stellt so auf elektronischem Wege fahrzeuggenerierte Daten in Kraftfahrzeugen Dritten (Kunden und Drittparteien) zur Verfügung.

- Die Regelungen des DA müssen allerdings angepasst werden, um für die Automobilindustrie mit ihren tiefen Lieferketten und ihren komplexen Produkten sowie für die Nutzer den größtmöglichen Mehrwert zu erzeugen.

- Der prinzipiell unbeschränkte Anwendungsbereich des DA führt zu Rechtsunsicherheit und damit zu Nachteilen für alle Beteiligten. Erforderlich ist daher, den Begriff „generated data“ so zu definieren, dass es sich um verfügbare Daten handelt, die an für die Kommunikation nach außen vorgesehenen Schnittstellen anliegen.

- Das europäische Datenwirtschaftsrecht muss weitestgehend vom Prinzip der Vertragsfreiheit als Grundvoraussetzung für die digitale Innovationsfähigkeit geprägt sein.

- Doch nun sollen den Herstellern vertragliche Bedingungen auferlegt werden, unter denen sie die Daten weitergeben müssen. Die Verwendung der Daten lässt sich faktisch nicht nachverfolgen (z.B. in daraus abgeleiteten Produkten). Es besteht somit das Risiko, dass Fahrzeughersteller auf relevante Investitionen, welche eine weitere Datenerzeugung, -sammlung und -verarbeitung bedingen, verzichten.

- Mit seinem weiten Verständnis von „Daten“ erfasst der DA personenbezogene Daten gleichermaßen. Notwendige Klarstellungen und Harmonisierungen mit der DSGVO fehlen mit der Folge datenschutzrechtlicher Unsicherheit.

- Der Zugriff für Regierungen auf Daten in einem öffentlichen Notstand ist zu weit gefasst. Es ist weder klar, unter welchen Umständen ein solcher Notstand greift, noch wer Daten dann anfordern kann, oder über welche Wege Daten abgefragt werden könnten.

2. Einleitung

Der VDA unterstützt den datenwirtschaftsrechtlichen Ansatz des Data Acts (DA), dass für Verbraucher und sonstige dritte Unternehmen die Möglichkeit zum Datenzugang und zur Datennutzung bestehen muss. Es ist sinnvoll, ein level playing field zu schaffen und die Rolle des Nutzers zu stärken. Die Mitgliedsunternehmen des VDA haben in den vergangenen Jahren bereits Systeme und Mechanismen eingeführt, welche diese grundlegenden Ziele der EU Strategy for Data – das Teilen von verfügbaren Daten an den Kunden und bei Kundenwunsch und Zustimmung an Dritte – umsetzen.

So hat die Automobilindustrie (Hersteller und Zulieferer) bereits seit langem Maßnahmen über den Rahmen ihres ADAXO-Konzepts (vormals NEVADA-Konzept) implementiert und teilt heute schon, auf Wunsch ihrer Kunden, umfassend Daten mit Dritten.

Deswegen entspricht zwar der Ansatz der EU-Kommission, mittels des DA ein „level playing field“ (FRAND-Konditionen für Datenzugriff Dritter, Ausschluss Gatekeeper nach Definition DMA) zwischen sämtlichen Akteuren der Datenwirtschaft zu schaffen, dem grundlegenden Interesse der Automobilindustrie, muss aber im Detail der Regulierung einer Prüfung hinsichtlich Systematik und Zweckmäßigkeit unterzogen werden. Die Regelungen des DA sollten angepasst werden, um für die Nutzer ebenso wie für die Automobilindustrie mit ihren tiefen Lieferketten ebenso wie für die Nutzer den größtmöglichen Mehrwert zu erzeugen. Die Produkte der Automobilindustrie sind aufgrund ihres Einsatzzweckes und des damit verbundenen potentiellen Schadensrisikos nur bedingt mit anderen Geräteklassen vergleichbar. Entsprechend müssen sie über ein hohes Maß an Integrität und Sicherheit verfügen. Zudem weisen sie eine enorme Anzahl von Sensoren und Steuergeräten auf, die kontinuierlich große Mengen an Daten erzeugen. Die überwiegende Anzahl dieser Daten ist lediglich für die unmittelbare Funktionserfüllung innerhalb des Fahrzeugs relevant.

Die EU-Kommission sieht bei Daten ein Wachstums- und Innovationspotential. Der DA soll das Ausschöpfen dieser Potentiale unterstützen. Der DA könnte in seiner jetzigen Ausgestaltung den technischen Fortschritt in Europa aber eher behindern. Die Vorgaben sind sehr weit gefasst: die Pflicht, technische Voraussetzungen zu schaffen, um Daten zur Verfügung zu stellen, ist im Entwurf im Prinzip unbegrenzt. Die Unternehmen werden gezwungen, auch für die Bereitstellung wenig relevanter Daten einen sehr hohen Aufwand zu betreiben. Dieser Ansatz wird in der Praxis an Grenzen stoßen. Es ist daher Aufgabe des Gesetzgebers, die Pflicht zur Nutzbarmachung von Daten sinnvoll zu konturieren.

Fahrzeughersteller und Zulieferer schaffen mittels signifikanter Investitionen in innovative Technologien die Möglichkeit der Datenerzeugung, -sammlung und -verarbeitung. Laut DA soll der User, sobald er die vom Produkt erzeugten Daten erhalten hat, diese kostenlos an andere Unternehmen zur freien Verfügung übermitteln können – die Geschäftsgeheimnisse des Herstellers eingeschlossen. Gleichzeitig werden dem Hersteller vertragliche Bedingungen auferlegt, unter denen er die Daten weitergeben muss. Die Verwendung der Daten lässt sich faktisch nicht nachverfolgen (z.B. in daraus abgeleiteten Produkten). Es besteht somit das Risiko, dass Fahrzeughersteller auf relevante Investitionen, welche eine weitere Datenerzeugung, -sammlung und -verarbeitung bedingen, verzichten, da die Kosten für die Datenerzeugung und -ausleitung de facto höher sind als etwaige Umsätze, die sich mit den Daten erzielen lassen. Völlig offen lässt der Entwurf zudem, wie diese Kosten zugeordnet werden können, insbesondere dann, wenn es für diese Daten keinen wirtschaftlichen Bedarf gibt.

In diesem Zusammenhang ist es besonders nachteilig, dass der sui generis Schutz für Datenbanken in Art. 35 unnötig weitgehend beschränkt wird. Der Investitionsschutz nach der Datenbankrichtline könnte es dem Hersteller, der die zur Datenerzeugung, -sammlung und -verarbeitung nötigen Investitionen selbst getätigt hat, zumindest in manchen Konstellationen die Möglichkeit eröffnen, gegen unzulässige und vom DA gerade nicht gedeckte Datennutzungen (siehe Art. 6 DA) vorzugehen.

Der Zugriff für Regierungen auf Daten in einem öffentlichen Notstand ist zu weit und unspezifisch gefasst. Es ist weder klar, unter welchen Umständen ein solcher Notstand greift, noch wer Daten dann anfordern kann, oder über welche Wege Daten abgefragt werden könnten.

3. Anwendungsbereich des DA anpassen

Aus VDA-Sicht führt dieser prinzipiell unbeschränkte Anwendungsbereich des DA zu Rechtsunsicherheit und damit zu Nachteilen für alle Beteiligten. Erforderlich ist daher, den Begriff „generated data“ so zu definieren, dass es sich um verfügbare Daten handelt, die an für die Kommunikation nach außen vorgesehenen Schnittstellen, die das extended vehicle bereitstellt, anliegen (vgl. ADAXO – s.u. Ziff.3). Funktionale Daten, die ausschließlich den Betrieb sicherstellen, sollten nicht darunterfallen. Entsprechend wird in dem Entwurf zum DA die Tatsache nicht berücksichtigt, dass den Unternehmen nicht immer alle Daten (sei es in verarbeitbarer Form oder grundsätzlich) vorliegen. Fahrzeuge generieren mittels einer Vielzahl von separaten Rechnern, Steuergeräten und Sensoren eine unheimlich große Menge an Daten, die zu einem Großteil direkt nach Verarbeitung im Fahrzeug bzw. im Sensor selbst verworfen werden. Für die Industrie ist davon auszugehen, dass solche Daten nicht erfasst sind; andernfalls wären ungeheure Datentransport-, Speicher- und Verarbeitungskapazitäten im Fahrzeug sowie in der dahinterliegenden Infrastruktur erforderlich. Dies hätte einen massiven Eingriff in das Produktdesign zur Folge - zudem resultieren durch die additive Datenspeicherung signifikant negative Kosten und Umwelteffekte. Auf diese Sensor-, aber auch eine Reihe weiterer Daten hat der Hersteller oftmals auch keinen Zugriff, da sie nicht ausleitbar sind bzw. er sie nicht ausleitet oder weiterverarbeitet.

Um die grundsätzlichen Ziele des DA zu erreichen, müssen Lücken / Umgehungsmöglichkeiten geschlossen werden, damit gerade die europäische Industrie profitiert und nicht verliert: Durch die Ausnahme in Art.2 Abs.2 und in Erwägungsgrund 15 werden im Wesentlichen Hersteller von Computern, Tablets und Smartphones privilegiert, während die oft europäischen Hersteller von Fahrzeugen, medizinischen Geräten, Agrar- und Industrietechnik benachteiligt

werden. Durch die Anforderung, dass als Datenlieferanten nur gegenständliche Produkte in Frage kommen und nicht Software, treffen die jetzt schon dominanten Anbieter von Software keine vergleichbaren Pflichten wie die Hersteller aus dem IoT-Bereich einschließlich der Automobilindustrie. Umgekehrt stärkt die Regelung, dass gegenständliche Konkurrenzprodukte verboten sind, aber konkurrierende Software erlaubt wird, die schon jetzt dominanten Anbieter von Software. Softwareunternehmen werden aus den Daten Programme erstellen (z.B. FAS/HAF), die sie den Produktherstellern unter typischen Softwareverträgen (inkl. weitgehenden Haftungsausschlüssen) anbieten werden. Die Umgehungsmöglichkeit durch eine Datenlieferung vom User an den Dritten schafft Gatekeepern mit ihrer sehr breiten Kundenbasis hervorragende Chancen, sich nahezu kostenlos die Daten zu sichern, die ihnen bislang im Portfolio noch fehlen. Europäische Mittelständler, die eigentlich vom DA profitieren sollen, werden ein solch breites Portfolio nicht annähernd erreichen können und geraten so noch mehr ins wettbewerbliche Abseits.

Der Entwurf gefährdet den Schutz von Know-How und die Vertraulichkeit von Geschäftsgeheimnissen der Industrie (bei der Automobilindustrie sowohl der Hersteller, der Zulieferer und der Hersteller von Anhängern und Aufbauten/KMUs); eine entsprechende Schutzklausel ist nicht vorgesehen. Zwar liegt laut DA die Verantwortung beim gewerblichen Kunden, dass die Daten nicht gegen die Inhaber der Rechte verwendet werden. Ein Nachweis eines Datenlecks ist jedoch schwierig. Zudem kann der potenzielle, dann bereits erfolgte Schaden existenzgefährdend sein, insbesondere für KMUs. Auch die Quantität und Qualität der gesammelten Daten durch die Unternehmen droht zu leiden und damit auch der Rückstand Europas gegenüber den USA und China weiter zuzunehmen, wenn der Zugriff Dritter auch auf vertrauliche Daten ermöglicht wird. Es muss daher im DA sichergestellt werden, dass Daten, die Geschäftsgeheimnisse betreffen, nicht herausgegeben werden müssen.

Weiterhin bringt der DA umfangreiche neue Pflichten für Hersteller von Produkten mit sich. Unternehmen der Automobilindustrie wären mit ihren vernetzten Fahrzeugen in besonderer Weise betroffen und würden mit einem erheblichen technischen Umsetzungsaufwand belastet. Allein die Anforderung des DA, dass Daten den Nutzern nach Möglichkeit fortwährend und in Echtzeit zur Verfügung gestellt werden sollen, würde die Industrie als Dateninhaber in der Praxis vor ganz erhebliche Herausforderungen stellen. Darüber hinaus bedürfen auch viele Aspekte des DA selbst größerer Klarheit, da sie derzeit zu viel Raum für Interpretationen lassen, was zu Rechtsunsicherheit und einem hohen Risiko von Rechtsstreitigkeiten führt.

Der VDA setzt auf marktgetriebene Innovationen, gerade auf dem Feld der Datennutzung. Der DA sollte auf bereits etablierte Konzepte wie ADAXO setzen, und - dem Grundsatz der Verhältnismäßigkeit folgend - den marktorientierten Ansatz fördern. Es muss das marktwirtschaftliche Prinzip der Vertragsfreiheit gewahrt bleiben, sodass die Unternehmen und Verbraucher im Innovationswettbewerb die Nutzung von Daten weiterhin gestalten können.

4. VDA-Konzept ADAXO in der Praxis umgesetzt

Die Automobilindustrie hat das Konzept „Extended Vehicle“ bereits erfolgreich eingeführt und stellt so auf elektronischem Wege fahrzeuggenerierte Daten an Dritte (Kunden und Drittparteien) zur Verfügung. Es handelt sich dabei um einen sicheren Server, über den Dritte Zugriff auf Fahrzeugdaten erhalten können, anstatt in unkontrollierter Weise direkt auf die Fahrzeuge zuzugreifen. Die Absicherung sämtlicher Schnittstellen im Fahrzeug, die eine Verbindung zur Außenwelt haben, kann am besten durch die Fahrzeughersteller erfolgen, da diese die nötigen Eingriffe in die Fahrzeugarchitektur sicher und effizient vornehmen können. Über das Extended Vehicle wird der Datenzugriff unter Gewährleistung klar definierter technischer Standards sowie produktsicherheits-, datenschutz- und wettbewerbsrechtlicher Regeln ermöglicht. Das Konzept hat den Vorteil, dass es von allen Fahrzeugherstellern über alle Modelle hinweg unterstützt wird und bezüglich Art und Menge der zu übertragenden Daten offen ist. Dies ermöglicht Fahrzeugnutzern, Service-Anbietern, Dienstleistern und Herstellern vielfältige innovative Nutzungsmöglichkeiten und eine gleichberechtigte Teilnahme am Wettbewerb.

Das neue ADAXO-Konzept des VDA stellt bereits eine Weiterentwicklung des Extended Vehicle Konzepts des VDA dar. Der VDA hat mit dem ADAXO-Papier einen Vorschlag gemacht, der Sicherheit und die transparente Nutzung der im Fahrzeug generierten Daten sehr gut miteinander verbindet. Danach stellt die Automobilindustrie freiwillig und wettbewerbsneutral Daten über eine sichere Dateninfrastruktur datenschutzkonform auch interessierten Dritten zur Verfügung. Damit wurde ein modernes und zukunftsorientiertes Konzept für den Austausch von Fahrzeugdaten zwischen allen Stakeholdern sowie für Anforderungen an Drittsoftware im Fahrzeug vorgelegt.

5. Verfügbarkeit von Reparatur- und Wartungsinformationen nach EU VO 2018/858

Außerdem sind die Fahrzeughersteller bereits seit Jahren gesetzlich verpflichtet (aktuell über die EU-Verordnung 2018/858 – Typgenehmigung-Rahmenverordnung), Reparatur- und Wartungsinformationen (RMI) aus Fahrzeugen mit „unabhängigen Wirtschaftsakteuren“ zu teilen. Damit werden insbesondere unabhängige Werkstätten und Diagnosedienstleister in die Lage versetzt, unter gleichberechtigten Bedingungen mit den Vertragshändlern und Vertragswerkstätten zu konkurrieren. Auch Pannenhilfsdienste und Anbieter von Inspektions- und Prüfdienstleistungen sind berechtigt, (technische) Fahrzeugdaten anzufordern. Die Daten werden grundsätzlich über Webseiten der Hersteller in einem standardisierten Format, in leicht zugänglicher Form und in diskriminierungsfreier Weise zur Verfügung gestellt. Zur Erfüllung dieser Vorgaben haben die Hersteller bereits erhebliche Anstrengungen unternommen, um die Daten in einer sicheren und rechtskonformen Weise zur Verfügung zu stellen.

6. Definition „generated data“ unklar

Die Definition des Begriffs „data“ in den Art.3 und 4 des DA ist unscharf. Der Anwendungsbereich des DA sollte konkreter beschrieben werden, damit er für alle Beteiligten handhabbar wird. Die gegenwärtige Formulierung mit ihrem allumfassenden Ansatz lässt jede Konturierung im Hinblick auf den Charakter der erfassten Daten und den erforderlichen Aufwand vermissen. Es muss deswegen klargestellt werden, dass

- es sich um “accessible data” handelt: Daten, die (1) das Produkt generiert während es vom Benutzer genutzt wird, (2) die angefordert werden in einem digital lesbaren Format (3) die erhalten werden können und die (4) an existierenden Schnittstellen dem data holder vorliegen,

- funktionsinterne Daten nicht von der Definition umfasst sein sollten und

- sich für den Bereitsteller der Daten keinerlei (Gewährleistungs- und/oder Haftungs-) Ansprüche aufgrund der Beschaffenheit ergeben (wie sie an der existierenden Schnittstellte vorliegen = „data as is“).

7. Definition „product“ unklar

Durch die Beschränkung aus der Produktdefinition in Art. 2 (2) auf körperliche Gegenstände werden die Anbieter von Services (insb. Software) bevorzugt. Die Ungleichbehandlung von Services, die Produkten zugeordnet werden können, im Verhältnis zu Produkten sollte explizit und unzweideutig aufgehoben werden. Eine klare Definition ist notwendig: Dienste, die tangible products zugeordnet wurden, müssen auch geschützt werden. Beispiel: Nachladbarer Navi-Service, der auf dem tangible product ausgeführt wird. Dieser Navi-Service kann ggf. durch eine Drittpartei verantwortet sein.

Ein umgekehrter Datenfluss von Serviceanbietern zu Produktherstellern ist im DA nicht vorgesehen. Im Ergebnis werden Daten aus typisch europäischen Produkten (z.B. Fahrzeugen, medizinischen Geräten, Agrar- und Industrietechnik) an Unternehmen zur Verfügung gestellt, die Services anbieten. Diese Beschränkung wird europäische Unternehmen massiv benachteiligen, welches der Zielsetzung des DA - Innovationsförderung und Cross-Sektoraler Datenaustausch in Europäischen Unternehmen – maßgeblich widerspricht. Außerdem ergeben sich Abgrenzungsschwierigkeiten, wenn die Daten beispielsweise in einem Fahrzeug, aber durch eine nicht vom Hersteller programmierte App erzeugt werden.

8. Definition „user“ unklar

Ein „User“ ist gem. Art. 2 Nr.5 DA Eigentümer, Mieter oder Leasingnehmer des Produktes oder hat einen Service erworben. Er ist also Vertragspartner hinsichtlich des Produkts oder des Services. Diese Person trägt die Risiken, soll im Umkehrschluss die Vorteile der Nutzung des vernetzten Produkts genießen und entsprechend auch Zugang zu den von ihm erzeugten Daten haben (ErwG 18). Präzisierungsbedarf besteht daher dahingehend, dass der „Nutzer“ in Anlehnung an Erwägungsgrund 18 über ein entsprechendes Vertragsverhältnis

definiert wird. Dies kommt in der Formulierung gem. Art. 2 Nr. 5 DA durch die Formulierung „oder eine Dienstleistung in Anspruch nimmt“ nicht deutlich genug zum Ausdruck, sondern sollte eher durch „oder eine vertragliche Dienstleistung in Anspruch nimmt“ ersetzt werden. Um Rechtssicherheit zu gewährleisten, sollte zudem klargestellt werden, dass es mehrere „Nutzer“ geben kann, sofern Vertragsverhältnisse zu mehreren Nutzern bestehen.

Es ist für den Hersteller auch schwer vorherzusehen, wie viele Personen seine Fahrzeuge gemeinsam kaufen, mieten oder leasen und damit nutzen; er weiß daher nicht, wie viele „Accounts“ er vorhalten muss. Damit sind auch die Anforderungen aus der EU-DSGVO bezüglich der „Data Subjects“, also der Betroffenen der Datenverarbeitung, schwer umsetzbar, da sich ein Nutzer eines Fahrzeugs nicht identifizieren muss.

9. Definition „data holder“ unklar

Der Begriff ist ungenau. Es muss zunächst klar bestimmt sein, ob lediglich vom „Data holder“ tatsächlich für seine eigenen Geschäftsvorfälle verwendete Daten betroffen und ob keine flüchtigen Daten von der Definition umfasst sind. Ist es weiterhin die „Person“, die das Fahrzeug herstellt oder der, der die „Daten hält“? Wer soll beispielsweise bei Third Party Apps, die im Produkt „Fahrzeug“ angeboten werden und Daten erzeugen, „data holder“ sein? In mehrstufigen Bereichen wie z.B. bei Mobilitätsservices sind regelmäßig mehrere Akteure beteiligt (OEM, Leasinggeber, Vermieter, Flottenbetreiber etc.). Diese Akteure haben unterschiedliche Zugriffsmöglichkeiten (technisch und rechtlich) auf die im Fahrzeug generierten Daten.

Darüber hinaus sollte die Definition an den Umstand der tatsächlichen Einwirkungsmöglichkeit auf die Daten anknüpfen (data holder). So bleibt derzeit unklar, ob der „Dateninhaber “ derjenige ist, der das IoT-Produkt herstellt oder vielmehr derjenige, der die Kontrolle über die Daten – und somit die tatsächlichen Einwirkungsmöglichkeiten – hält. Mit Blick auf den Fahrzeugmarkt stellt sich etwa die Frage, wer bei sog. „Third Party Apps“, die im Produkt „Fahrzeug“ angeboten werden und Daten erzeugen, als „Dateninhaber“ anzusehen ist. Es sollte vor diesem Hintergrund klargestellt werden, dass Dateninhaber immer nur der unmittelbare Vertragspartner des Nutzers ist und tatsächlich über seine Daten verfügt, sie also gerade nicht erst über Dritte beschaffen muss, um sie dem Nutzer zugänglich zu machen. Dadurch wird gleichzeitig sichergestellt, dass Auftragsverarbeiter entgegen vertraglicher Verpflichtungen gegenüber dem Auftraggeber zur Herausgabe veranlasst werden können. Weiterhin sollte das Verhältnis „Controller“ i.S.d DSGVO zu „Data Holder“ i.S.d DA klargestellt werden. Insbesondere die begriffliche Abgrenzung des Data Holder zum „Data Processor“ i.S.d DSGVO wird in der Praxis eine wichtige Rolle spielen.

Aus dem Online-Bereich sollte zudem bekannt sein, dass der Hersteller des Endgeräts nicht immer „data holder“ ist; z.B. beim Einsatz von Cookies. Soweit es sich um personenbezogene/-beziehbare Daten handelt, wäre eine Abgrenzung zum Begriff „Data Controller“ aus der EU-DSGVO sinnvoll.

10. Datenzugang und -nutzung nach Art. 3 Abs.1 Data Act

Auch hier sind die vom DA vorgenommenen Definitionen unzureichend/unklar:

- Die in Art. 3 Abs. 1 beschriebene Designanforderungen/-änderungen würden, sofern der Datenbegriff wie in Ziff. 5 (s.o.) nicht präziser definiert wird, erhebliche Vorlaufzeiten für die Produktion und Entwicklung innerhalb der Automobil- und Zuliefererindustrie erfordern. Insofern sehen wir die geplante Umsetzung des DA mit lediglich 2-3 Jahren als nicht oder nur bedingt umsetzbar für die Automobilindustrie an.

- Die entsprechende Bereitstellung von derzeit nicht verfügbaren Daten, würde zu einem Anstieg der Datenübertragung führen, welche zum einen unverhältnismäßige Kosten generieren würde und zum anderen zu einer erheblichen Belastung im Rahmen der zu speichernden (und nicht genutzten) Daten führen würde. Zudem sind die derzeit nicht verfügbaren Daten in vielen Fällen nicht ohne additiven Aufwand Interpretierbar und damit nutzbar.

- Sollte der Datenbegriff nicht wie kommentiert eingeschränkt werden, würde die Menge der auszuleitenden Daten massiv ansteigen und könnte nicht mehr durch die bestehende Infrastruktur in IoT-Produkten (u.a. Kraftfahrzeugen) hinsichtlich Datentransferfähigkeit, Energiebedarf und Komplexität abgedeckt werden.

- Zusätzlich ist es bei einem Fahrzeug mit einer angenommenen Lebensdauer von 15 Jahren unmöglich, schon beim Kauf die im Laufe der 15 Jahre vorkommende Datennutzung vorauszusehen bzw. unveränderlich zu lassen. Fraglich ist auch, ob auch beim Weiterverkauf eine entsprechende Information (von wem?) bereitzustellen ist.

11. Mehrpersonenverhältnisse und Datenschutz (Art. 4 des Data Act)

Eine konkrete Frage wirft Artikel 4 des geplanten DA in Bezug auf den Begriff des „Nutzers“ in Mehrpersonenverhältnissen auf. Der DA will dem Nutzer einen Anspruch auf Datenherausgabe gegen den Dateninhaber, d. h. Hersteller, einräumen. In Mehrpersonenverhältnissen, die im Nutzfahrzeuggeschäft typischerweise der Fall sind, entstehen dadurch erhebliche Abgrenzungsschwierigkeiten. Es stellt sich die Frage, wie die Datenherausgabe konkret abgewickelt werden soll, wenn der Nutzer ein Unternehmen ist (z. B. ein Flottenbetreiber als Eigentümer/Halter des Fahrzeugs), die Daten aber von den Fahrern als Betroffene im datenschutzrechtlichen Sinne generiert werden. In solchen Konstellationen kann die Herausgabe von personenbezogenen Daten nur auf Basis einer tauglichen Rechtsgrundlage (z. B. Einwilligung des Betroffenen) erfolgen. Daraus ergibt sich die Folgefrage, wie solche Einwilligungen nachgewiesen und verwaltet werden sollen.

Es sollte klargestellt werden, dass der DA den Nutzern keinen Anspruch auf Herausgabe personenbezogener Daten anderer Betroffener gibt. Der derzeitige Wortlaut legt nahe, dass ein solcher Anspruch besteht, und es an dem für die Verarbeitung Verantwortlichen (Dateninhaber) liegt zu prüfen, ob es i. S. d. DSGVO eine angemessene Rechtsgrundlage gibt, um dem Nutzer Zugang zu den personenbezogenen Daten anderer Betroffener zu gewähren. Dies stellt eine unangemessene Belastung für die Datennutzer dar. Ein Anspruch auf Herausgabe personenbezogener Daten anderer betroffener Personen würde möglicherweise auch im Widerspruch zu den Zielen der DSGVO gemäß Artikel 1 DSGVO stehen.

Die Rahmenbedingungen der vertragliche Ausgestaltung nach Art. 4 Abs.6 für nicht-personenbezogene Daten sind unklar. Welche Auswirkungen zieht etwa eine Beendigung eines solchen Vertrages zwischen data holder und user nach sich? Die einmal dem data holder überlassenen Daten müssen bei diesem verbleiben.

Aus datenschutzrechtlicher Sicht sollte das Berechtigungsmanagement konsistent und einfach zu bedienen sein und somit für Fahrzeugdaten beim Hersteller als zentralem Ansprechpartner der Datenerhebung liegen. Grundsätzlich darf die Ausleitung der Daten an user/third Party nicht zu einem Einfallstor für Kriminelle werden, sodass die Security/Safety/Privacy des users gefährdet wird.

12. Ausschluss sog. Gatekeeper

Grundsätzlich befürwortet der VDA den Ausschluss der Gatekeeper bezüglich des „right to access data as third party“. Der User soll seine nach Art. 3 erhaltenen Daten gem. Erwägungsgrund 28 an jeden Dritten weitergeben dürfen – und damit auch an Gatekeeper. Die Beschränkungen der Artikel 5, 6 und 9 beziehen Art. 3 aber nicht ein und werden damit ausgehebelt. In der Praxis wird diese Möglichkeit dazu führen, dass die Gatekeeper Anwendungen/Geräte entwickeln werden, mit denen Daten direkt aus dem Fahrzeug ausgeleitet und an die Gatekeeper in Echtzeit weitergeleitet werden können.

Eine Schärfung hinsichtlich Umgehungspraktiken für Gatekeeper ist daher aus VDA-Sicht dringend erwünscht. Nur so kann der Zweck des DA erreicht werden und das Level Playing Field nach dem FRAND-Prinzip.

13. EU-Datenbank-Rl – „sui generis Recht“

Artikel 35 sieht vor, dass der in Artikel 7 der Richtlinie 96/9/EG vorgesehene sui generis Datenbankschutz nicht für Datenbanken gelten soll, die Daten enthalten, die durch die Nutzung eines Produktes oder eines damit verbundenen Dienstes gewonnen oder generiert wurden. Dadurch will der DA explizit verhindern, dass Zugangsrechte der Nutzer zu Daten und deren Nutzung nach Art. 4 oder das Recht auf Weitergabe dieser Daten an Dritte gemäß Art. 5 behindert werden. Dieses nachvollziehbare Regelungsziel wird durch den aktuellen Entwurf leider nur mit erheblichen Nebenwirkungen erreicht. Diese innovationshemmenden Nebenwirkungen lassen sich problemlos vermeiden, ohne die Ziele des DA zu gefährden.

Der Art. 35 hat aktuell die folgende Konsequenz: Sobald eine Datenbank (auch) Daten enthält, die durch die Nutzung eines Produktes oder eines damit verbundenen Dienstes gewonnen oder generiert wurden, entfällt nach Art. 35 der Datenbankschutz per se für die gesamte Datenbank. Dies gilt unabhängig vom wirtschaftlichen Wert der Daten und den zugrunde liegenden Investitionen in die Datenbankerstellung. Durch Art. 35 werden der Datenbankschutz und die damit verbundenen Investitionsanreize also massiv eingeschränkt. Eine derart weitgehende Einschränkung ist zur Erreichung des erklärten Ziels, die Rechte nach Art. 4 und Art. 5 abzusichern, aber weder erforderlich noch angemessen. Die in Erwägungsgrund 28 geforderte Balance zwischen Datenzugangsrechten und Investitionsanreizen wird so nicht erreicht („Gleichzeitig soll damit verhindert werden, dass die Investitionsanreize für den Produkttyp, von dem die Daten erlangt werden, z. B. durch die Verwendung von Daten zur Entwicklung eines konkurrierenden Produkts, untergraben werden.”).

Daneben bleibt unklar, ob Art. 35 auch dann noch eingreifen soll, wenn die durch die Nutzung eines Produktes oder eines damit verbundenen Dienstes gewonnen oder generierten Daten vorher aufbereitet wurden. Die Daten also nicht mehr als Rohdaten in die Datenbank aufgenommen werden, sondern vorab mit weiteren Investitionen aufbereitet wurden (vgl. „Datenbanken, die Daten enthalten“).

Das Ziel, die Rechte nach Art. 4 und Art. 5 abzusichern, kann durch eine andere Regelungstechnik einfach erreicht werden. Anstatt den Datenbankschutz vollständig entfallen zu lassen, sollte das Datenbankschutzrecht (nur) erschöpft sein, wenn Datenzugang oder -nutzung nach dem DA erlaubt sind. Eine solche Erschöpfungsregelung hätte auch die wünschenswerte Konsequenz, dass ein Verstoß gegen die Nutzungsbeschränkungen im DA (z.B. Art. 6 Abs. 2) dazu führte, dass der Inhaber eines Datenbankschutzrechts – sofern es denn besteht – gegen die vom Data Act nicht gestattete Nutzung vorgehen könnte. Eine Alternativregelung könnte lauten:

“In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC ~~does not apply to databases containing data obtained from or generated by the use of a product or a related service~~ shall not entitle the data holder or proprietor of a sui generis right to prohibit the access and use of data that is permitted under this regulation.”

Der Umgang mit solchen „Erschöpfungsregelungen” ist in der Praxis bestens erprobt, was die Auslegung und Handhabung sicherlich erleichtern würde.

14. Unfaire Vertragsklauseln nach Art.13 Data Act und AGB-Recht

Gemäß Artikel 13 des geplanten DA sollen unfaire Vertragsklauseln in Datennutzungs- und -lizenzverträgen mit KMU‘s, welche als unwirksam anzusehen sind, die Wirksamkeit der Verträge im Übrigen grundsätzlich unberührt lassen. Hier ist noch zu klären, wie sich diese Bestimmung des Data Acts zum bestehenden AGB-Recht verhält und inwiefern die Wertungen der neuen Klauselverbote auch auf Verträge außerhalb des KMU-Bereichs übertragen werden können.

15. Kritische Systematik des DA im Verhältnis zum EU-Datenwirtschaftsrecht

Generell ist festzustellen, dass durch die geplanten Regelungen des DA die Regelungsdichte in Bezug auf Daten und deren Nutzung immer enger und unübersichtlicher wird. Es ist bislang nicht klar, wie sich der DA genau in das hochkomplexe Geflecht bestehender und geplanter europäischer Vorgaben für die Daten- und Digitalwirtschaft einfügen soll. Der Anwendungsbereich des DA ist sehr weit, da er über personenbezogene Daten hinausgeht. Im Einzelfall kann die Frage, welches Normregime anwendbar ist, sehr schwierig werden,

denn in der Praxis lassen sich personenbezogene Daten nicht immer leicht von nicht-personenbezogenen Maschinendaten abgrenzen. Dies gilt insbesondere für die Verarbeitung von Daten in hochautomatisierten Fahrzeugen. Insofern ist es aus Praxissicht unabdingbar, klare Abgrenzungsregelungen zwischen den einzelnen Regelungsregimen für die Daten- und Digitalwirtschaft einzuführen. Zur bestehenden Unübersichtlichkeit tragen auch die Verweise und Überschneidungen im DA auf andere Gesetzgebungsverfahren bei, deren Inhalte noch nicht final ausverhandelt sind, so z. B. Digital Markets Act, Data Governance Act oder ePrivacy Verordnung.

Die zunehmende Regelungsdichte birgt für Fahrzeughersteller das Risiko, dass sie mit diversen technischen Anforderungen an ihre Produkte überfrachtet und damit digitale Innovationen insgesamt behindert werden. Aus Sicht der Automobilindustrie ist es vorzugswürdig, die vielfältigen Datenwünsche mit einer integrierten Lösung zu bedienen, die mit dem Konzept Extended Vehicle/ADAXO bereits besteht.

16. Unklare Systematik des DA im Verhältnis zum Datenschutzrecht (EU-DSGVO)

a) Verhältnis DA zur DSGVO sowie unklarer Begriff Daten

Mit seinem weiten Verständnis von „Daten“ sind von den Vorgaben des DA personenbezogene Daten gleichermaßen erfasst. Notwendige Klarstellungen und Harmonisierungen mit der DSGVO fehlen. Zumindest über die „Vehicle Identification Number“ (VIN) bei Kfz, die einen Personenbezug herstellt, gibt es an diversen Stellen Überschneidungen zwischen den beiden Verordnungen, so dass eine Klarstellung unbedingt erforderlich ist. Es wird die Chance nicht genutzt, eines der zentralen praktischen Hemmnisse von Unternehmen in der Datenwirtschaft aufzugreifen.

Da in der industriellen Praxis die Abgrenzung zwischen personenbezogenen Daten und nicht personenbezogenen Daten mit großer Rechtsunsicherheit verbunden ist, besteht mit Blick auf Kapitel 2 des DA, der dem Dritten unbewusst Zugang zu personenbezogenen Daten verschafft, ohne dass ein solcher von der DSGVO legitimiert wäre.

Hinsichtlich der Prüfung der Rechtsgrundlage ist zudem zu berücksichtigen, dass dem „Dateninhaber“ regelmäßig nicht alle Informationen zur Verfügung stehen, um das Vorliegen der Rechtsgrundlage rechtssicher prüfen zu können, sofern der „Datennutzer“ die Herausgabe an einen Dritten verlangt. Der „Dateninhaber“ kann weder beurteilen, ob der „Datennutzer“ vom Dritten ausreichend über die Art und den Umfang der personenbezogenen Daten aufgeklärt wurde, noch, ob die vom „Datennutzer“ für den Dritten beanspruchten Daten erforderlich sind. Hier ist eine klare Regelung zu treffen, welche Anforderungen an die Prüfung durch den „Dateninhaber“ gestellt werden bzw. darüberhinausgehenden Beibringungspflichten dem Nutzer/Dritten obliegen.

Es sollte im DA klargestellt werden, dass der Datenzugangsanspruch des „Nutzers“ aus Kapitel 2 keinen Rechtsanspruch zur Anforderung von personenbezogenen Daten anderer Betroffener begründet. Der derzeitige Wortlaut suggeriert, dass ein solcher Anspruch besteht und es dem für die Datenverarbeitung Verantwortlichen (Dateninhaber) obliegt, nach der DS-GVO zu beurteilen, dem Nutzer Zugang zu den personenbezogenen Daten anderer betroffener Personen zu gewähren.

Zudem ist in derartigen Fällen der genaue Mechanismus zwischen den Portabilitätsrechten nach Artikel 20 DSGVO einerseits und den Rechten nach Art. 4 und 5 des DA noch nicht ausreichend geklärt. Dies gilt auch für Auskunftsrechte in Situationen, in denen die Rechte Dritter als Betroffener berührt werden.

Daneben benötigen Unternehmen verlässliche und zugleich praktikable Orientierungshilfen bei der Anwendung und Auslegung der DSGVO im Zusammenhang mit den Rechten aus dem DA. Dies gilt exemplarisch für Orientierungshilfen hinsichtlich der Anforderungen für eine datenschutzkonforme Anonymisierung personenbezogener Daten. Deshalb haben viele Industrieunternehmen ein großes Interesse daran, in deutlich größerem Maße mit anonymisierten Daten zu arbeiten. Mit Blick auf die legislativen Vorgaben ist zu konstatieren, dass die DSGVO keine konkreten Vorgaben zur Anonymisierung personenbezogener Daten enthält. Diese Problematik wird durch den DA zum einen nicht gelöst und zum anderen sogar noch perpetuiert.

Schließlich widerspricht die aktuelle Definition des Begriffs „Daten“, welcher grundsätzlich auch Daten erfassen würde, die bislang nicht vom Automobilhersteller weitergehend verarbeitet und gespeichert werden (z.B. Sensordaten, rein fahrzeuginterne Daten, „flüchtige Daten“), dem in der DSGVO verankerten Grundsatz der Datenminimierung. Die aktuelle Ausgestaltung des DA würde dazu führen, dass Daten, die derzeit nicht verarbeitet werden, gespeichert werden müssten, um dem Nutzer den nach Art. 4 Abs. 1 DA geforderten Echtzeitzugang gewähren zu können.

b) Datenzugang für Behörden

Der VDA hat mit seinem ADAXO-Konzept auch die Bereitstellung von Daten an Behörden vorgesehen. Allerdings ist nach dem DA nicht klar, welche Behörden etwa im Bereich der öffentlichen Sicherheit und Ordnung dazu zählen sollen.

Hinsichtlich Art. 14 ff. DA, in denen der Zugang zu „Daten“ für Behörden geregelt ist, stellt sich insbesondere die Frage, ob dies eine eigenständige Rechtsgrundlage ist bzw. ob es allein auf eine entsprechende Aufforderung („request“) seitens der Behörde ankommen soll. Auch sollte u.E. der Umfang einer solchen Auskunft an die Behörde beschrieben sein (z.B. nur anonymisierte Daten o.ä.). Bezüglich der Nutzung von Daten durch öffentliche Stellen gemäß Art. 14 ff. des DA sollten klare und umfassende Bedingungen festgelegt werden, unter welchen Behörden die Zurverfügungstellung von Daten beantragen können, wobei ein enges und genau definiertes „öffentliches Interesse“ der Behörden vorausgesetzt wird.

Dem Legislativvorschlag fehlt es in Art. 15 DA darüber hinaus an einem expliziten und präzisen Anwendungsbereich, in denen ein obligatorischer B2G-Datenaustausch aufgrund einer „außergewöhnlichen Notwendigkeit“ erforderlich wäre. Die Definitionen eines „öffentlichen Notstands“ und der in Art. 15 a) und b) DA und insbesondere eine „bestimmte, gesetzlich ausdrücklich vorgesehene Aufgabe im öffentlichen Interesse“ in Art. 15 c) sind sehr weit gefasst und bieten Unternehmen keine notwendige Rechtssicherheit, in welchen Konstel-

lationen eine Datenbereitstellungspflicht vorgesehen ist. Selbiges gilt für den Schutz von Geschäftsgeheimnissen gem. Art. 17 Abs. 2 c) DA. Hier bedarf es dringend einer Präzisierung, um ein unionsweit einheitliches Verständnis für die Vielzahl an anspruchsberechtigten öffentlichen Stellen zu gewährleisten.

Neben dem Anwendungsbereich ist es für die Unternehmen zwingend erforderlich, auch die datenschutzrechtlichen und (nicht-)technischen Anforderungen an Sicherheitsvorkehrungen für die Informationssicherheit im Zuge der Datenbereitstellung mit der öffentlichen Stelle zu präzisieren. Um den Schutz der informationellen Selbstbestimmung und der Datensicherheit unternehmensseitig gewährleisten zu können, müssen zudem die Datenbereitstellungsfristen von fünf bzw. fünfzehn Arbeitstagen verlängert werden. Schließlich führen bereits eine datenschutzadäquate Pseudonymisierung und Anonymisierung personenbezogener Daten zu einem erheblichen Zeit- und Arbeitsaufwand, der nicht nur in den zeitlichen Fristen zu berücksichtigen, sondern auch über eine angemessene Entschädigung ausgeglichen werden muss.

Schließlich müssten B2G-Datenteilungspflichten zugleich rechtssicher und praktikabel ausgestaltet werden. Dies gilt mit Blick auf personenbezogene und personenbeziehbare Daten in Form von rechtssicheren und zugleich praktikablen Orientierungshilfen zur hinreichenden Anonymisierung und Pseudonymisierung personenbezogener Daten. Analog zu den Diskussionen im laufenden Verfahren zum Data Governance Act ist in der Anwendungspraxis völlig unklar, welche technischen Maßnahmen zu einer hinreichenden Anonymisierung personenbezogener Daten erforderlich sind. Es ist insofern auch völlig unklar, über welche technischen „Kanäle“ die Datenbereitstellung erfolgen soll und welche Stelle für die Einrichtung einer entsprechenden technischen Einrichtung zuständig ist. Es bestehen zum aktuellen Zeitpunkt keine technischen Einrichtungen, die eine rechtssichere und praktikable Übermittlung von ggf. sogar sehr großen Datensätze mit Behörden ermöglichen.

Darüber hinaus sollten entsprechende Verpflichtungen ausschließlich an Dateninhaber („data controller“) gerichtet werden, damit nicht etwaige Datenverarbeiter („data processor“) entgegen ihren vertraglichen Verpflichtungen gezwungen werden, Kundendaten an öffentliche Stellen weiterzugeben.

c) Zuständigkeit der Aufsichtsbehörden bei Konkurrenz zum Datenschutzrecht

Es ist weiterhin unklar, welche nationalen Aufsichtsbehörden für die Umsetzung des DA zuständig sein sollen. Dabei ist unseres Erachtens unbedingt zu berücksichtigen, dass die betreffenden Behörden über die erforderliche IT- bzw. digitale Erfahrung verfügen, was etwa auf die Datenschutzbehörden zutreffen würde.

17. Fehlen des Begriffes Konkurrenzprodukt

Es fehlt gänzlich an einer Definition des Begriffes „Konkurrenzprodukt“, welcher für die Wirtschaft und den fairen Wettbewerb von größter Bedeutung ist. Im Rahmen einer solchen sollten unter anderem die beiden folgenden Punkte adressiert werden:

a. Unklar ist, was unter dem Begriff „competing products“ zu verstehen ist. Könnten aus einem engen Definitionsansatz folgen, dass gerade große Softwareanbieter oder Serviceanbieter (außerhalb der EU) aufgrund der ausgeleiteten Daten davon profitieren könnten? Auch hier muss im DA weitere definitorische Klarheit geleistet werden.

b. Es sind Abgrenzungskriterien in Bezug auf Absatzmärkte (ist ein chinesisches Unternehmen ein Konkurrent für einen europäischen OEM?), zeitliche Inverkehrbringung (ist ein Produkt in zehn Jahren auf der Grundlage der Daten von heute ein Konkurrenzprodukt?), gesellschaftsrechtliche Besonderheiten (ist eine neu gegründete Tochter eines bestehenden Unternehmens ein Konkurrent?) etc. notwendig.

18. Prozessrechtliche Auswirkungen

Im deutschen Zivilprozessrecht gilt der Beibringungsgrundsatz, d.h. jede Partei muss die ihren Anspruch begründenden Tatsachen belegen. Der diesem Grundsatz zuwiderlaufende Ausforschungsbeweis ist daher grundsätzlich unzulässig. Die Datenzugangsansprüche des DA dürfen insofern nicht zu einer Verschiebung dieses verfassungsrechtlich anerkannten Gerichtsverfahrensgrundsatz führen (wie bei einer Discovery nach amerikanischem Verfahrensrecht).

Ansprechpartner

Dr. Ralf Scheibach
Abteilungsleiter Recht & Compliance
ralf.scheibach@vda.de

Dr. Viola Gomoll
Referentin Recht, Compliance & Gesetzesanalyse
viola.gomoll@vda.de

Herausgeber
Verband der Automobilindustrie e.V.
Behrenstraße 35, 10117 Berlin
www.vda.de

Registrierter Interessenvertreter R001243
EU-Transparenzregister-Nr. 95574664768-90

Version
Version 1.0, Mai 2022