RA Thomas Kahl und RAin Teresa Kirschner, Frankfurt*

Auswirkungen EU-Digitalstrategie auf die Automobilindustrie – ein 360 Grad Blick

Die EU-Digitalstrategie ist der umfassende Plan der Europäischen Union, Europa in eine weltweit führende digitale Wirtschaft zu verwandeln. Sie wurde im Februar 2020 von der Europäischen Kommission vorgestellt. Sie besteht aus verschiedenen Digital-Gesetzen wie dem AI Act, dem Data Act oder dem Digital Services Act, die schon heute erhebliche Auswirkungen auf die Automobilindustrie haben. Der folgende Beitrag gibt einen 360-Grad Überblick, welche der Regelwerke der EU-Digitalstrategie Legal Teams in der Automobilindustrie in den kommenden Jahren besonders beschäftigen und welche Fragen sich heute und in Zukunft stellen werden.

1. Wesentliche Regelungsinhalte der EU-Digitalstrategie

Wesentliche Zielsetzung der EU-Digitalstrategie[1] sind Innovationsförderung, Stärkung des Wettbewerbs und des Binnenmarktes sowie die Resilienz der Wirtschaft. Kernregelungen sind der Data Governance Act[2] (DGA), der Data Act[3] (DA), der Cyber Resilience Act (CRA)[4], der Digital Service Act[5] (DSA) sowie die Regelungen zu den EU-Datenräumen (oder auch EU Data Spaces) für 14 dedizierte Industriezweige (z. B. den European Mobility Data Space für den Mobilitätssektor)[6]. Die einzelnen Initiativen stehen dabei in logischer und kohärenter Verbindung.[7] Sie werden ergänzt durch weitere Regelungen wie den Artificial Intelligence Act (AI Act oder AIA)[8], die Neuregelung des digitalen Kaufrechts[9] oder die IT-Sicherheitsvorgaben der Network Information Directive 2 (NIS-2)[10], die – obgleich nicht im eigentlichen Sinne Teil der EU-Digitalstrategie – oftmals im gleichen Atemzug genannt und in der Beratungspraxis von großer Bedeutung sind. Sie bilden die „Peripherie" der EU-Digitalstrategie, sind im Rahmen der Umsetzung mit zu betrachten und sollen nachfolgend kursorisch mit dargestellt werden.

Betrachtet man Kern und Peripherie der EU-Digitalstrategie gemeinsam, lassen sich die EU Digital-Regelungen in vier (4) Themenkomplexe und jeweils dazugehörige Regelwerke unterteilen:

Data	Platform & eCommerce	Tech-Competition & AI	IT Security
Data Act	Digital Service Act	Arificial Intelligence Act	Cyber Resilience Act
Data Governance Act	Digital Sales Law	AI- Liability-Directive	NIS-2-Directive / DORA / CER-RCE
Data Spaces	European Accessibility Act	Digital Markets Act	Product- Liability-Directive

Abb. 1: Überblick EU-Digitalstrategie und Peripherie

Die *erste Säule (Data)* beinhaltet mit den Regelwerken DA, DGA und den EU Data Spaces die Regelungen für den neuen Rechtsrahmen der Datenregulierung.

Die *zweite Säule* (*Plattform- & eCommerce*) beinhaltet das neue „digitale Kaufrecht" einschließlich des neuen digitalen Gewährleistungsrechts, den DSA mit der europaweit nunmehr vereinheitlichten Betreiber-Haftung im Online-Bereich sowie den Regelungen zur digitalen Barrierefreiheit auf Basis des European Accessibility Acts (EAA)[11].

Kern der *dritten Säule* (*Tech-Competition & AI*) ist der ab dem 1.8.2024 geltende AI Act, der zukünftig die Entwicklung, den Vertrieb und den Einsatz von AI bzw. AI-gestützten Produkten und Diensten reguliert.

Komplettiert wird der Rechtsrahmen durch Regelungen einer *vierten Säule* (*IT-Security*), u. a. mit der NIS-2-Richtlinie, CRA und der Revised Product Liability Directive[12].

2. Rechtliche und praktische Herausforderungen

Die Automobilindustrie stand und steht nicht im Fokus der EU-Digitalstrategie. Die Regelungen sind technikneutral und branchenunabhängig, auch wenn an einzelnen Stellen Bezug auf Automobil-spezifische Anwendungsfälle genommen wird (vgl. hierzu u. a. Erwägungsgrund 14 im DA). Die Anwendung der Regelungen der EU-Digitalstrategie auf automotive-spezifische Sachverhalte beispielsweise in der Head Unit des Fahrzeugs führt vielfach zu Schwierig-

* Mehr über die Autoren erfahren Sie auf S. III.

1 Europäische Kommission: Gestaltung der digitalen Zukunft Europas, 19.2.2020, COM (2020) 67 final, S. 2 ff.

2 Verordnung (EU) 2022/868 vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724.

3 Verordnung (EU) 2023/2854 vom 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).

4 Angenommen durch das Parlament im März 2024, Zustimmung des Rates ausstehend: https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products (zuletzt abgerufen am 1.8.2024).

5 Verordnung (EU) 2022/2065 vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste).

6 Vgl. beispielhaft die Initiative für den European Mobility Data Space (EMDS), https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_1114 (abgerufen zuletzt am 1.8.2024).

7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz), 25.11.2020, COM (2020) 767 final S. 2.

8 Verordnung (EU) 2024/1689 vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

9 U. a. Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags sowie Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen in Umsetzung der Richtlinie (EU) 2019/770 („Digitale-Inhalte-Richtlinie") und Richtlinie (EU) 2019/771 über bestimmte vertragsrechtliche Aspekte des Warenkaufs („Warenkaufrichtlinie").

10 Richtlinie (EU) 2022/2555 vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie).

11 Directive (EU) 2019/882 of the European Parliament and the Counsel of 17.4.2019 on the accessibility requirements for products and services (European Accessibility Act).

12 Angenommen durch das Parlament im März 2024, Zustimmung des Rates ausstehend: https://www.europarl.europa.eu/news/en/press-room/20240308IPR18990/defective-products-revamped-rules-to-better-protect-consumers-from-damages

keiten, da sie für gänzlich andere Fälle (u. a. Social-Media Plattformen) konzipiert wurden.

Bei den Regelungen der EU-Digitalstrategie handelt es sich um gänzlich neue und mit „heißer Nadel" gestrickte Regelwerke, zu denen bislang keine bzw. nur wenig „Guidance" existiert. Die Umsetzung erfolgt „auf der grünen Wiese". Das eröffnet zwar Umsetzungsspielräume, birgt aber ebenso erhebliche Rechtsunsicherheit.

Fehlende Regelungen zum Verhältnis der neuen Regelwerke untereinander sowie zu bereits bestehenden Regelwerken wie der DSGVO erschweren die Implementierung und führen zu erheblichen Abgrenzungsschwierigkeiten.

Hinzu kommt der enorme Compliance-Druck durch teils drakonische Sanktionen und Haftungsfolgen bei Verstoß gegen die neuen Regelwerke, die je nach Regelwerk bis zu 10 % des weltweiten Jahresumsatzes der gesamten Unternehmensgruppe im vorangegangenen Geschäftsjahr betragen können. Daneben steht das aus dem Datenschutz bereits bekannte und nur schwer kalkulierbare Risiko der Rechtsdurchsetzung durch Betroffene, Verbraucherverbände oder andere Interessengruppen, ggf. auch im Wege kollektiver Rechtsverfolgung.

Die auf Basis der strikten EU-Vorgaben entwickelten Lösungen lassen sich zudem oft nicht ohne Weiteres auf Märkte außerhalb der EU übertragen, da dort abweichende Vorgaben und Geschäftspraktiken existieren. Dies erschwert die einheitliche Gestaltung von Fahrzeugfunktionen und -diensten für verschiedene Regionen der Welt.

Last but not least führen das Tempo der Gesetzgebung und die schiere Masse an neuer Regulierung zu einem oft nur schwer zu bewältigenden Umsetzungsaufwand, dem Legal Teams begegnen müssen.

3. Auswirkungen und aktuelle Fragestellungen

Um der Flut an neuen Vorgaben Herr zu werden, gilt es sich einen Überblick über die wesentlichen Vorgaben, relevanten Fragestellungen und To Do's zu verschaffen. Die Darstellung folgt dem zuvor dargestellten Vier-Säulen Modell.

3.1 Datenregulierung

Mit dem DA wird ein harmonisierter Rahmen für die Datennutzung aus vernetzten Produkten geschaffen. Vernetze Fahrzeuge sind vernetzte Produkte im Sinne des DA (vgl. Art. 2 (5) DA), so dass die Nutzung von Fahrzeugdaten den Vorgaben des DA unterfällt (vgl. Erwägungsgrund 14). Dateninhaber (z. B. Automobilhersteller oder Anbieter vernetzter Fahrzeugdienste, die Zugang zu entsprechenden Daten haben) sind verpflichtet, Nutzern (z. B. Fahrzeughaltern) Zugang zu verfügbaren Fahrzeug- und Dienstedaten zu gewähren. Dies umfasst in der Regel alle Daten, für die eine Extraktion aus dem Fahrzeug vorgesehen bzw. ohne größeren Aufwand möglich ist („readily available data"; vgl. Art. 2 (17) DA). Die Bereitstellung muss u. a. leicht, in der gleichen Qualität wie beim Dateninhaber (z. B. dem Automobilhersteller), kostenlos, soweit relevant und technisch machbar, kontinuierlich und in Echtzeit erfolgen. Berechtigte Nutzer können auch Unternehmen (B2B) sein, z. B. Leasingnehmer einer Fahrzeugflotte.

Entsprechender Datenzugang muss auf Nachfrage des Nutzers auch Drittanbietern einschließlich Wettbewerbern im Aftermarket gewährt werden, vgl. Art. 4 DA. Die kommerziellen Auswirkungen sind immens. Die Wertschöpfungskette wird hierdurch erheblich verschoben. Der wirtschaftliche Druck erhöht sich weiter. Es gelten strikte Vorgaben für die Form der Bereitstellung (u. a. Bereitstellung in *real time;* vgl. Art. 5 DA). Um die Anforderungen zu erfüllen, ist ein spezifisches Prozess- und Schnittstellendesign zwischen Fahrzeug, Hersteller-Backend, Benutzerschnittstelle und Drittanbieter erforderlich. OEMs, die in der Vergangenheit Datenzugangsmöglichkeiten z. B. auf Basis des ADA-XO-Konzepts[13] realisiert haben, sind hiermit bereits vertraut und können dies nutzbar machen. Andere betreten „Neuland" mit nicht unerheblichem Entwicklungsaufwand.

Im Rahmen der Umsetzung stellen sich noch viele Fragen: Wie verhält sich der DA zu den Datenzugriffsregeln gemäß Art. 61 ff. Verordnung (EU) 2018/858? Wie würde eine Schnittstelle für Dritte genau aussehen? Wie kann eine sinnvolle Clustering der bereitzustellenden Datenpakete aussehen? Welche technischen und organisatorischen Maßnahmen kann der OEM nach dem aktuellen EuGH-Urteil[14] zum Datenzugriff nach VO (EU) 2018/858 von Dritten verlangen? Und unter welchen Voraussetzungen („exceptional circumstances", vgl. Art. 5 (11) DA) kann die Bereitstellung unter Verweis auf Betriebs- und Geschäftsgeheimnisse verweigert werden?

Parallel zu den datenschutzrechtlichen Informationspflichten gemäß Art. 13, 14 DSGVO sind DA-spezifische Transparenzpflichten zu erfüllen, und zwar bereits bei Abschluss des entsprechenden (Nutzungs-)Vertrags. Die Nutzung nicht personenbezogener Fahrzeugdaten für Sekundär-Zwecke wie Produktentwicklung wird eine „Datenlizenz" erfordern. Entsprechende Regelungen werden sich zukünftig in den jeweiligen Nutzungsbedingungen der Hersteller finden. Dies erfordert die Anpassung bestehender Nutzungsbedingungen.

Der DA wird zukünftig durch spezifische Regelungen der EU-Data Spaces für Fahrzeugdaten ergänzt. Die Regelungen stehen nach mehrfacher Ankündigung immer noch aus.[15] Neben dem angekündigten Update der Regelungen für den Zugang zu Reparatur- und Wartungsinformationen (u. a. Art. 61 ff. VO (EU) 2018/858)[16] werden die Regelungen für Fahrzeugdaten (hoffentlich) weitere „Guidance" für die Ausgestaltung der DA-Zugangsrechte unter Berücksichtigung der Besonderheiten der Branche liefern, sobald sie verfügbar sind.

Zuletzt ist das Verhältnis des DA zu den Anforderungen der **DSGVO** unklar: Welche Prüftiefe haben Hersteller bei der datenschutzrechtlichen Bewertung gemäß Art. Art. 5 (7) DA

13 VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten (abrufbar unter: https://www.vda.de/de/aktuelles/publikationen/publication/adaxo–automotive-data-access-–extended-and-open, zuletzt abgerufen am 1.8.2024).

14 Vgl. EuGH, Urteil C-319/22 in Sachen Gesamtverband Autoteile-Handel eV v. Scania CV AB (abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?text=&docid=279492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=312775, zuletzt abgerufen am 1.8.2024).

15 Vgl. Stellungnahme von Thierry Breton im Namen der Europäischen Kommission vom 15.5.2024 (abrufbar unter https://www.europarl.europa.eu/RegData/questions/reponses_qe/2024/000706/P9_RE(2024)000706_DE.pdf, zuletzt abgerufen am 1.8.2024).

16 Vgl. Aufforderung zur Stellungnahme/Mitteilung der Kommission über die Schaffung eines gemeinsamen europäischen Mobilitätsdatenraums (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=PI_COM:Ares(2022)7735749, zuletzt abgerufen am 1.8.2024).

vor Bereitstellung von Daten an Nutzer anzulegen? Was ist die richtige Rechtsgrundlage (z. B. Einwilligung, gesetzliche Erlaubnis oder Interessenabwägung)? Und welche Rolle nimmt der OEM ein (z. B. die eines Auftragsverarbeiters)? Die Klärung dieser Fragen sind entscheidend, u. a. um die jeweiligen Datenschutzhinweise korrekt gestalten zu können.

Dieser Konflikt zeigt, dass „Daten" ein Querschnittsthema ist, das in Zukunft nicht von einem Team im Unternehmen allein bewältigt werden kann. Die Fragen, die sich stellen, sind: Wo ist das Thema „Daten" am besten in der Compliance-Organisation verortet? Gibt es Interessenkonflikte, wenn die Datenschutzorganisation auch für die „Daten"-Compliance zuständig ist? Und wie kann ein „Data Compliance Management System" (DCMS) aussehen, das effizient mit dem Datenschutzmanagementsystem (DPMS) vernetzt ist?

Die Vorgaben gelten ab dem 12.9.2025. Für den Datenzugang direkt über das vernetzte Produkt gilt eine Übergangsfrist bis zum 12.9.2026. Dies ändert nichts an der ab September 2025 bestehenden Pflicht, Nutzern wie Drittanbietern Daten gemäß Art. 4, 5 DA außerhalb des Produkts (z. B. über einen Webservice) zur Verfügung zu stellen.

Ergänzt werden Regelungen des DA durch den bereits heute geltenden DGA. Er enthält u. a. Regeln für Anbieter von Datenvermittlungsdiensten (sog. Datenvermittler, wie z. B. Datenmarktplätze), um sicherzustellen, dass sie als vertrauenswürdige Intermediäre des Datenaustauschs agieren. Die Vorgaben sind für Hersteller, Zulieferer sowie Anbieter entsprechender Datendienste von großer Bedeutung, da der Handel mit Fahrzeug- und Mobilitätsdaten bereits heute ein wichtiges Geschäftsfeld (u. a. für die Produktentwicklung) darstellt. Entsprechende Datenmarktplätze werden durch den DGA reguliert. So dürfen Intermediäre u. a. gehandelte Daten nicht für eigene Geschäftszwecke verarbeiten (Neutralität), müssen „faire" Preismodelle anwenden und sich bei den zuständigen Behörden registrieren lassen.

3.2 Plattformregulierung, eCommerce und Barrierefreiheit

3.2.1 Regulierung unter dem DSA

Die Plattform-Regulierung unter dem seit Februar 2024 vollständig geltenden DSA macht Legal Teams der Automobilindustrie zu schaffen.[17] Verschiedene Dienste, die Automobilhersteller ihren Kunden und/oder Geschäftspartnern anbieten, sind von den neuen Vorschriften betroffen. Dies gilt u. a.

- im Bereich der vernetzten Fahrzeugdienste, wenn Inhalte oder Dienste von Dritten in das Angebot der OEMs aufgenommen werden („Plattform"; Art. 12, 19 ff. DSA),
- im Bereich des mobilen eCommerce, wenn OEMs ihre Connected Vehicle Services und/oder die Head Unit im Fahrzeug für Drittanbieter (z. B. Händler) zur Vermarktung ihrer Produkte und Dienstleistungen bereitstellen („Marktplatz"; Art. 12, 19, 29 ff. DSA), oder
- bei denen OEMs IT-Services einschließlich des Hostings von Daten und Systemen als IT-Service für Dritte, einschließlich Gruppenunternehmen, anbieten („Hosting"; Art. 12 ff. DSA).

Der DSA bringt verschiedene Verpflichtungen mit sich, u. a. in Bezug auf Transparenz (Bereitstellung von Kontaktdaten für Nutzer, Behörden und Dritte), Reportingpflichten, die Bereitstellung von Beschwerdekanälen und Abhilfeverfahren, spezifische Regeln für die Ausgestaltung von Marketing- und Empfehlungssystemen oder die Überprüfung der Einhaltung spezifischer Vorgaben durch Drittanbieter (Händler). Die Umsetzung erfordert neben der Anpassung der jeweiligen Nutzungsbedingungen und Erstellung dedizierter „Plattform-Rules" die Gestaltung neuer Prozesse im Bereich des Beschwerde- und Suppliermanagements, die so je nach Geschäftsbereich oftmals noch nicht existieren. Die Umsetzung ist meist mit erheblichem Entwicklungsaufwand verbunden, beispielsweise im Rahmen der Implementierung des Marktplatz-Supplier-Managements in Connected Vehicle Services und des Beschwerdemanagements für Plattformen. Da die Regelungen bereits scharf geschaltet sind, ist Eile bei der Umsetzung geboten.

3.2.2 eCommerce

Die Neuerungen des digitalen Kaufrechts[18] und die Umsetzungsgesetze zur Omnibus-Richtlinie[19] sind bereits seit dem 1.1.2022 in Kraft. Sie bringen neue Anforderungen für digitale Produkte und Dienstleistungen und haben erhebliche Auswirkungen auf die Gestaltung u. a. von Connected Vehicle Services.[20] Sie können auch für kostenlose Dienste gelten, bei denen beispielsweise personenbezogene Daten als Gegenleistung für einen „kostenlosen" Dienst wie einen Connected Vehicle Service bereitgestellt werden (vgl. § 327 Abs. 3 BGB).

Die Gewährleistungs- und Widerrufsrechte werden erweitert. Für digitale Produkte gelten neue Updatepflichten (u. a. für Betriebssysteme und Software; vgl. §§ 327e und f BGB), um ihre Nutzung für die Dauer der typischen Verwendung sicherzustellen, was über die im bisherigen Recht geltenden Gewährleistungsfristen (in der Regel zwei Jahre) deutlich hinausgehen und diese faktisch auf mehrere Jahre ausweiten kann. Die Regelungen schaffen ein komplexes Zusammenspiel mit anderen regulatorischen Anforderungen, u. a. mit den UNECE R156 Update-Regelungen. Dies gilt insbesondere dort, wo over-the-air (OTA) Updates in Zukunft auch zur Behebung von gewährleistungsrelevanten Mängeln am Fahrzeug eingesetzt werden.

Zudem stellt sich bei der Einbeziehung von Drittanbieterdiensten im Fahrzeug vermehrt die Frage der gewährleistungsrechtlichen Verantwortlichkeit im Fall von Mängeln oder Fehlfunktionen bei digitalen Produkten bzw. Produkten mit digitalen Elementen (vgl. § 327 ff. BGB, § 327a Abs. 3 BGB). Hersteller müssen die Verantwortlichkeiten vertraglich und in der Außenkommunikation klar abgrenzen, um zukünftig nicht ungewollt gegenüber Kunden für Diensteangebote Dritter zu haften. Dieses Geflecht von Verpflichtungen ist komplex und erfordert eine Befassung verschiedener Stellen im Haus der Automobilhersteller wie IT-Security, Produkthaftung und Product Compliance oder Vertrieb.

---

17 Vgl. zum Ganzen Kahl/Kling, Connected Vehicle Services und der Digital Services Act, RAW 2023, S. 104 ff.

18 Vgl. Fn 9 m. w. N.

19 Richtlinie (EU) 2019/2161 zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften. Durch die „Onmibus"-Richtlinie werden die Verbraucherrechte-Richtlinie (2011/83/EU), die Richtlinie über Preisangaben (98/6/EG), die Richtlinie über unlautere Geschäftspraktiken (2005/29/EG) sowie die Richtlinie über missbräuchliche Vertragsklauseln (93/13/EWG) angepasst.

20 Vgl. zum Ganzen Kahl/Lie, Auswirkungen des neuen digitalen Kaufrechts auf Connected Vehicle Services; RAW 2022, S. 106 ff.

3.2.3 Barrierefreiheit

Ab dem 28.6.2025 erfordert das auf Basis des EEA erlassene Barrierefreiheitsstärkungsgesetz (BFSG)[21] die barrierefreie Gestaltung besonders relevanter Produkte und Dienstleistungen. Dies betrifft auch die meisten Formen von Online-Shops, Dienste mit Shop-Funktion und Buchungsplattformen. Die neuen Vorschriften erfordern die Umsetzung konkreter technischer Standards und Leitlinien zur Beseitigung von Hindernissen bei der Nutzung bestimmter digitaler Produkte und Dienste.[22]

Die Regelungen sind für OEMs von großer Relevanz. Sie gelten für Webshops und Reservierungsplattformen (z. B. im Sales/Aftersales, u. a. für Reservierungen von Testdrives) und andere eCommerce-Anwendungen in Connected Vehicle Services. Inwieweit die technischen Anforderungen auch im Fahrzeug (z. B. Head Unit) umgesetzt werden müssen, lässt das Gesetz offen. Dass die Head Unit des Fahrzeugs als „interaktives Selbstbedienungsterminal" i. S. d. § 1 (2) Nr. 2 b) dd) BFSG den Vorgaben unterfällt, scheint fraglich. Schwierige Abgrenzungsfragen ergeben sich zudem bei der Umsetzung der Vorgaben in „gemischten" Diensten, d. h. solchen mit Funktionen, die nur zum Teil den Vorgaben des BFSG unterfallen. Hier wird eine möglichst trennscharfe Abgrenzung und genaue Analyse der User Journey erforderlich, um die jeweils geltenden Anforderungen zu bestimmen. Auf Grund der verbraucherfreundlichen weiten Auslegung der Anforderungen ist es für OEMs dringend ratsam, die jeweiligen Dienste auf die Anwendbarkeit der Regelungen zu prüfen und – wenn noch nicht geschehen – möglichst bald mit der Umsetzung zu beginnen.

3.3 KI Regulierung

Mit dem ab dem 1.8.2024 geltenden AI Act schafft die EU die weltweit erste und umfassende Regelung für die Entwicklung, den Einsatz und die Nutzung von KI in der EU. Sie gilt für Anbieter, Einführer und Vertreiber von KI-Systemen und KI-Modellen sowie für Organisationen, die KI-Systeme und Modelle in der EU nutzen oder betreiben. Bestimmte KI-Systeme sind verboten (vgl. Art. 5 AI Act). Die Entwicklung und Nutzung von Hochrisiko-KI-Systemen wird stark reguliert. Für hiervon betroffene Unternehmen enthält der AI Act umfassende Pflichten zur Konformitätsbewertung und Zertifizierung, Einrichtung von Qualitäts- und Risikomanagement-Systemen, Data Governance, Überwachung und Dokumentation sowie umfassende Transparenzpflichten. Die Pflichten ähneln stark denen aus der Produktregulatorik (Zulassungsrecht) bekannten Mechanismen und haben ihren Schwerpunkt im Bereich der Product-Compliance, was für die Verortung des AI-Compliance Managements innerhalb der Organisation von Bedeutung ist.

Hochrisiko-KI-Systeme sind KI-Systeme, die Produkte oder Sicherheitsbauteile von Produkten sind, die nach bestimmten Unionsrechtsakten (vgl. Anhang I AI Act) einer Konformitätsbewertung unterzogen werden müssen (Art. 6 (1) AI Act). Wird im Automobilbereich ein KI-System eingesetzt, dass seinerseits in den Anwendungsbereich bestimmter EU-Verordnungen wie z. B. der (EU) 2018/858 und 2019/2144 (z. B. Fahrerassistenz-Systeme) fällt, gelten diese als KI-Systeme mit hohem Risiko, für die jedoch besondere Vorschriften im Kontext der jeweiligen EU-Verordnungen erlassen werden (vgl. Art. 6 (1), Anlage I AI Act). Die Vorgaben des AI Act gelten somit nur mittelbar.

Entsprechende Regelungen werden erst erarbeitet und liegen noch nicht vor. In dieser Hinsicht ähnelt die Situation der beim DA: Auch dort sind spezifischere Regelungen zu erwarten, die (hoffentlich) besser auf die Bedürfnisse der OEMs zugeschnitten sind. Ob die Automobilindustrie – ähnlich wie in anderen Bereichen (z. B. IT-Sicherheit) – eigene Branchenvorgaben entwickeln und diese zum Gegenstand von Zertifizierungen machen wird, bleibt abzuwarten, scheint aber denkbar.

Kommen in der Automobilindustrie KI-Systeme oder Modelle zum Einsatz, die nicht als Hochrisiko-KI Systeme reguliert sind, können die übrigen Vorgaben des AI Act dennoch gelten. Für bestimmte KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (z. B. Chatbots) oder die eine Emotionserkennung ermöglichen und/oder biometrische Daten verarbeiten, bestehen besondere Transparenzpflichten. Entsprechende Anwendungsfälle sind auch im vernetzten Fahrzeug denkbar, so dass eine genaue Analyse der jeweiligen Systeme und Prozesse erforderlich wird.

Ergänzt wird der AI Act um eine gesonderte Richtlinie über KI-Haftung, die sich derzeit in der politischen Abstimmung befindet.[23] Die Umsetzung der Vorgaben des AI Act wird in jedem Fall eines der (wenn nicht das) beherrschende Thema der nächsten Jahre.

3.4 IT- und Produktsicherheit

Automobilhersteller arbeiten derzeit mit Hochdruck an der Umsetzung der Anforderungen der UNECE-Regelungen R155[24] und R156[25], die ab 2024 über die Verordnung (EU) 2019/2144 unmittelbar in der EU gelten.

Bisher unterlagen Automobilhersteller daneben nicht direkt den strengen IT-Sicherheitsanforderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechik (BSiG). Infolge der Änderungen der NIS-2-Richtlinie und deren Umsetzung in den jeweiligen Mitgliedsstaaten werden Automobilhersteller vorrausichtlich ab Ende 2024 den strikten Anforderungen der NIS-2 unterfallen. Diese bringen deutlich umfangreichere technische und vor allem organisatorische Anforderungen im Bereich des IT-Sicherheitsmanagements mit sich (u. a. bei der Cyber Governance, im Risikomanagement, Business Continuity Management und der persönlichen Verantwortlichkeit des Managements; vgl. Art. 20 ff. NIS 2 Richtlinie).

21 Gesetz zur Umsetzung der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates über die Barrierefreiheits-anforderungen für Produkte und Dienstleistungen (BFSG).

22 Vgl. weiterführende Hinweise auf den Webseiten des BFAS (abrufbar unter https://www.bmas.de/DE/Service/Gesetze-und-Gesetzesvorhaben/barrierefreiheitsstaerkungsgesetz.html, zuletzt abgerufen am 1.8.2024).

23 Vorschlag für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI Haftung), (abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52022PC0496, zuletzt abgerufen am 1.8.2024).

24 UN Regulation No. 155 – Cyber security and cyber security management system (abrufbar unter: https://unece.org/sites/default/files/2023-02/R155e %282%29.pdf, zuletzt abgerufen am 1.8.2024).

25 UN Regulation No. 156 – Software update and software update management system (abrufbar unter: https://unece.org/sites/default/files/2021-03/R156e.pdf, zuletzt abgerufen am 1.8.2024).

Der Entwurf des CRA befindet sich derzeit noch in der politischen Abstimmung und soll die IT-Sicherheitsanforderungen für eine breite Palette von (vernetzten) Produkten mit digitalen Elementen verschärfen. Der CRA ergänzt bestehende Regelungen (u. a. das digitale Gewährleistungsrecht; vgl. 3.2) um produktbezogene Vorgaben (u. a. die Pflicht zur Durchführung produktbezogener Cybersecurity-Risikobewertungen, Updatepflichten, Dokumentation für Produkte und Drittkomponenten). Ähnlich wie im Fall des AI Act und des DA sollen auch hier spezielle Regelungen für den Automotive-Sektor als *lex specialis* dem CRA vorgehen (vgl. Art. 2 (2) lit. c) und Erwägungsgrund 13 des CRA, wonach ein Anwendungsvorrang u. a. für VO (EU) 2019/2144 bestehen soll). Abgrenzungsschwierigkeiten bestehen u. a. dort, wo im Fahrzeug nicht sicherheitsrelevante bzw. durch das Zulassungsrecht nicht gesondert regulierte Komponenten zum Einsatz kommen (z. B. im Entertainment-Bereich), was für das Design und IT-Sicherheitsmanagement im Fahrzeug von erheblicher Bedeutung ist.

Die überarbeitete EU-Produkthaftungsrichtlinie (RPRL) verschärft die Haftung von Produktherstellern, Importeuren und Inverkehrbringern für Schäden, die natürlichen Personen durch fehlerhafte Produkte entstehen. Sie verfolgt einen strikten verschuldensunabhängigen Haftungsansatz und beinhaltet umfassende Transparenz- und Meldepflichten, auch beim Online-Vertrieb von entsprechenden Produkten über Plattformen und Marktplätze (vgl. Art. 7 (6) RPRL). Aus diesem Grund sind die Vorgaben im Rahmen der Umsetzung des DSA im Plattformumfeld stets parallel zu beachten (vgl. 3.2). Software wird nunmehr ausdrücklich in den Anwendungsbereich der Regelungen einbezogen (vgl. Art. 4 (1) RPRL). Mängel bei der IT-Sicherheit können produkthaftungsrechtliche Verantwortlichkeit nach sich ziehen (vgl. Art. 6 (1) lit. f RPRL), was für Automobilhersteller vor dem Hintergrund der Digitalisierung von Fahrzeugfunktionen und Diensten und der traditionell erhöhten *Exposure* im Bereich der Produkthaftung von erheblicher Bedeutung ist.

4. Fazit

Automobilhersteller stehen vor großen Herausforderungen bei der Umsetzung der EU Digital-Regelwerke. Die Umsetzung erzeugt erheblichen Aufwand, insbesondere im Bereich vernetzter Fahrzeugdienste. Das Gesetzgebungstempo wird hoch bleiben, der Aufwand für Legal Teams in der Automobilindustrie ebenso.

Der Beitrag zeigt: Die enge Verknüpfung der Regelwerke erfordert einen 360 Grad Blick bei der Umsetzung. Eine getrennte Betrachtung führt dazu, dass Prozesse mehrfach einer Prüfung unterzogen werden (müssen) und erhöht Aufwand und Kosten. Die Umsetzung im Rahmen eines oder mehrerer zentraler Projekte erscheint zielführend.

Sie erfordert aber – wie immer – die genaue Analyse des Produkt- und Dienstleistungsportfolios, um zu verstehen, wo die neuen Gesetze in welchem Umfang gelten (und wo nicht). Nachdem die generischen rechtlichen Anforderungen bestimmt sind, ist die Umsetzung in Anbetracht des engen Zeitrahmens nach Risikogesichtspunkten und Umsetzungsfrist zu priorisieren. Für die technische Umsetzung ist genügend Zeit einzuplanen. Dies ist (erfahrungsgemäß) ein iterativer und langwieriger Prozess mit vielen Schleifen zwischen Legal, Compliance/Datenschutz, IT-Sicherheit und den beteiligten Business Units, bevor praktikable und gleichzeitig rechtskonforme Konzepte entwickelt sind, die in die Umsetzung gehen können. Die rechtzeitige Einbeziehung aller Stakeholder ist – wie immer – ein wesentlicher Erfolgsfaktor, damit es gleich gemeinsam in die richtige Richtung geht!

RA Martin Egner, München*

Blick in die Zukunft – Haftung für KI nach dem Vorschlag einer KI-Haftungs-RL

Gerade auch im Automotive- und Mobilitätsbereich werden sich – mit fortschreitender Digitalisierung – Kontrolle und Verantwortlichkeit verstärkt auf die Hersteller der Fahrzeuge und anderer digitaler Produkte verlagern. Von Bedeutung sind in diesem Zusammenhang insbesondere auch die Initiativen der EU zum regulatorischen Rahmen und der Haftung beim Einsatz von KI. Dieser Beitrag beleuchtet den Vorschlag einer KI-Haftungs-RL und zeigt mögliche Auswirkungen sowie bestehende Anpassungsbedarfe auf.

I. Einleitung

Digitale Komponenten und softwarebasierte Funktionen gehören in vielen Industriebereichen mittlerweile zum *State of the Art* der Produktentwicklung. In diesem Zusammenhang gewinnt auch der Einsatz von Künstlicher Intelligenz (KI) zunehmend an Bedeutung.

Nach dem Verständnis der Bundesregierung beschreibt KI die Fähigkeit von Maschinen, basierend auf Algorithmen Aufgaben autonom auszuführen und dabei die Problemlösungs- und Entscheidungsfähigkeiten des menschlichen Verstandes nachzuahmen.[1]

In der Automobil- und Mobilitätsindustrie werden schon seit längerer Zeit KI-basierte Systeme in verschiedenen abgesicherten und geprüften Bereichen verwendet.[2] Weitere Einsatzfelder (sog. Use Cases) betreffen u. a. Connected-Car-Technologien, die Integration von Sprachsteuerungsassistenten oder automatisierte bzw. autonome Fahrfunktionen. Auch im Rahmen der Predictive Maintenance wer-

* Mehr über den Autor erfahren Sie auf S. III.

1 https://www.bundesregierung.de/breg-de/themen/digitalisierung/kuenstliche-intelligenz/ai-act-2285944 (Abruf: 26.7.2024).

2 https://www.vda.de/de/aktuelles/artikel/2023/ki-schluesseltechnologie-mit-herausforderungen (Abruf: 26.7.2024).