September 2021
9. Jahrg.
Seite 73 – 140

RAW

2

Recht ■ Automobil ■ Wirtschaft
Unternehmen | Technologie | Beratung

dfv Mediengruppe · Frankfurt am Main

Die neue, strenge Berichtspflicht des LkSG mag den Anschein der Transparenz zwar erzeugen. Sie unterstellt aber, dass alle Unternehmen bereits einen vollen transparenten Überblick über ihre gesamte Lieferkette haben. Das ist in der Praxis heute nicht der Fall. Strenge Qualitätsanforderungen für die eigenen Produkte zwingen global agierende Unternehmen zwar längst dazu, nicht nur den unmittelbaren Vertragspartner in den Blick zu nehmen. Ein vollständiger Überblick über die gesamte Lieferkette, und über Fragestellungen menschenrechtlicher oder umweltrechtlicher Compliance dürfte aber nicht der Realität entsprechen.

Es müssen also zusätzliche Instrumente gefunden werden, mit denen „*auf Knopfdruck*" Standardinformationen zu den Risikobereichen in der Lieferkette abgerufen werden können. Solche Informationen sind anlasslos zu generieren und dauernd vorzuhalten. Sie müssen fälschungssicher sein, anonym weitergegeben werden können und müssen jederzeit leicht zur Verfügung stehen – und das von der Quelle bis zum Endkunden. Solch ein Informationstransfer ist über Unternehmensgrenzen hinweg nicht ganz unproblematisch. Handelt es sich um vertrauliche oder wettbewerbsrelevante Informationen, die unsachgemäß in fremde Hände geraten, kann damit zum Nachteil eines Unternehmens ein großer Schaden entstehen.

Es liegt auf der Hand, dass diese Aufgaben in erster Linie technisch zu lösen sind. Zertifizierungssysteme[39] und digitale Rückverfolgbarkeit von Produktbestandteilen und Verarbeitungsstufen können technisch helfen, den gesetzlichen Anforderungen nachzukommen. Ein weiterer, vielversprechender Ansatz ist die Blockchain-Technik, mittels derer Daten fälschungssicher und verschlüsselt generiert werden können. Die in der Blockchain abgelegten Informationen, z. B. über Ursprung der Rohstoffe, verwendete Materialien, Einhaltung von Arbeitsschutzbestimmungen usw. sind jederzeit abrufbar, werden in der Lieferkette von jedem weiteren Kettenmitglied ergänzt und stehen allen Beteiligten bei Bedarf zur Verfügung.

Ein deutscher Automobilhersteller hat Marktberichten zufolge bereits 2020 das Projekt PartChain[40] gestartet, um mittels Blockchain- und Cloudtechnik Rohstoffe und Bauteile in seinen weltweiten Lieferketten nahtlos zurückverfolgen zu können. In der Praxis kann man sich das so vorstellen, dass z. B. ein am Anfang der Lieferkette gewonnener Rohstoff mit einem QR-Code markiert wird, der alle erforderlichen Daten über Herkunft, Gewinnung des Rohstoffs, usw. enthält. Dieser Code wird im Hintergrund mit einer Blockchain verknüpft und „*reist*" dann als digitaler Datensatz entlang der Lieferkette. Jedes Kettenmitglied fügt seinen eigenen Datensatz hinzu, so dass am Ende eine transparente Entstehungsgeschichte des Endprodukts digital verfügbar wird.

V. Zusammenfassung

Die potentielle Verletzung menschenrechtlich geschützter Rechtspositionen stellte für große international tätige Unternehmen auch schon vor der politischen Debatte um ein Lieferkettengesetz ein erhebliches Reputationsrisiko dar. Das neue Lieferkettensorgfaltspflichtengesetz wird die Bedeutung der Lieferketten-Compliance für die betroffenen Unternehmen gleichwohl wesentlich erhöhen, da die Risiken vielfältig und die nun drohenden gesetzlichen Sanktionen empfindlich sind.

Daher müssen die betroffenen Unternehmen bestrebt sein, die vom Gesetzgeber vorgegebenen Maßnahmen schnell und konsequent umzusetzen. Grundsatzerklärungen, Lieferantenkodizes und Lieferverträge müssen überarbeitet und an die Vorgaben des Gesetzes angepasst werden. Mitarbeiter sind zu schulen und die erforderliche interne, personelle Organisation, bestehend u. a. aus dem Menschenrechtsbeauftragten, ist zu bestellen. Hinzu kommen die Einrichtung der neuen Instrumente bestehend aus Risikomanagementsystem, Beschwerdehotline und Reporting. Mit Spannung sind außerdem die Aktivitäten des EU-Gesetzgebers zu verfolgen: Eine europäische Lieferkettenregelung könnte noch deutlich über den deutschen Rechtsrahmen hinausgehen.

39 *Wagner/Ruttloff/Wagner/Hahn*, CB 2021, 89, 92.
40 https://www.electrive.net/2020/03/31/bmw-will-einkauf-per-blockchain-transparent-machen/, (Abruf: 1.7.2021).

RA Thomas Kahl, Frankfurt*

Datenschutz im Connected Vehicle Umfeld – Neue Guidelines des EDPB

Mit dem Entwurf der Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications unternahm das European Data Protection Board (EDPB) im Jahr 2020 einen ersten Versuch, die wesentlichen datenschutzrechtlichen Vorgaben und Aspekte im Connected Vehicle Umfeld zusammenzufassen. Die Ausführungen des EDPB stießen auf teils erhebliche Kritik im Rahmen der Konsultation, bevor im März 2021 die finale Fassung der Guidelines veröffentlicht wurde (nachfolgend „Guidelines").
Ist das Papier der „große Wurf"? Die Euphorie der Industrie dürfte verhalten sein. Viele der aktuell in der Praxis diskutierten Fragestellungen werden nicht beantwortet, dagegen viele neue aufgeworfen.
Ungeachtet dessen dürfte das Papier ein „Must Read" sein. Zum Einen sind die Guidelines für nationale Aufsichtsbehörden in der Auslegung und Anwendung der DS-GVO verbindlich. Zum Anderen scheint das EDPB zumindest einzelne Kernaussagen der Entwurfsfassung zu entschärfen, was nicht zuletzt auf die breite und konstruktive Beteiligung der Industrie zurückzuführen ist.

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

I. Rechtlicher Rahmen für den Datenschutz im Connected Vehicle Umfeld

Das EDPB beschreibt in den Guidelines[1] eingangs den (datenschutz-)rechtlichen Rahmen, in dem sich die Automobilindustrie bei der Verarbeitung von personenbezogenen Daten aus dem Connected Vehicle Umfeld bewegt.

Es stellt bei seiner Bewertung – wenig überraschend – zunächst die DS-GVO in den Vordergrund. Als weitere zentrale Regelung wird wie in der Entwurfsfassung Art. 5 Abs. 3 der ePrivacy-Richtlinie identifiziert und das vernetzte Fahrzeug als „Endgerät" im Sinne von Art. 1, Nr. 1, lit. a der Richtlinie 2008/63/EG eingeordnet.[2] In der Folge werden vereinzelt weitere Gesetze in Bezug genommen, u. a. die eCall-Verordnung[3].

Eine weitergehende Auseinandersetzung und Einordnung datenschutzrechtlicher Vorgaben in den komplexen und stark fragmentierten Rechtsrahmen, in dem sich Automobilhersteller und Dienstleister im Connected Vehicle Umfeld bewegen, erfolgt dagegen nicht.

Genannt seien hier zum einen Regelungen aus dem regulatorischen Bereich, die für die datenschutzrechtliche Bewertung der Verarbeitung von Fahrzeugdaten von erheblicher Bedeutung sind, z. B. die Datenverarbeitungsregelungen für Fahrassistenzsysteme in der Verordnung (EU) 2019/2144[4], die Bestimmungen der Verordnung (EU) 2018/858[5], u. a. mit Regelungen zur Bereitstellung von sog. Repair and Maintenance Information (RMI), das Straßenverkehrsgesetz (StVG) in Deutschland mit seinen Regelungen u. a. zur sog. „Blackbox" in §§ 63a, 63b StVG oder der aktuelle Entwurf des Gesetzes zum autonomen Fahren vom 20.5.2021[6], der u. a. Regelungen zur Weitergabe personenbezogener Daten an Behörden beinhalten soll.

Zum anderen unterfallen bestimmte Datenverarbeitungsvorgänge im Fahrzeugumfeld den Vorgaben für Telekommunikation, so dass neben den Vorgaben der ePrivacy-Richtlinie ggf. zusätzliche Vorgaben nach dem in Deutschland geltenden Telekommunikationsgesetz (TKG) bzw. dem unlängst verabschiedeten Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)[7] von Bedeutung sein können.

Zuletzt sehen sich Automobil-Unternehmen mit einer Vielzahl von Vorgaben zur Datensicherheit und Cybersecurity im Fahrzeugumfeld konfrontiert, die über eine Vielzahl von Gesetzen verteilt sind. So wird die Datensicherheit und Cybersecurity im Fahrzeugumfeld nicht mehr nur in der DS-GVO, sondern u. a. den Bestimmungen der Verordnung (EU) 2018/858[8] und den mittlerweile verabschiedeten UN.ECE-Regelungen zur Cybersecurity im Fahrzeugumfeld geregelt.[9] Im Bereich der kritischen Infrastrukturen existieren spezielle nationale Bestimmungen im BSiG in Umsetzung der NIS-Richtlinie[10], zuletzt geändert durch das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme[11], und den auf dieser Basis erlassenen KRITIS Verordnungen.

Insbesondere das Zusammenspiel der Datenschutzprinzipien der DS-GVO (u. a. zur Datenminimierung), der engen Tatbestandsvoraussetzungen des Art. 5 Abs. 3 ePrivacy-Richtlinie, der Vorgaben zur Errichtung eines Cyber Security Management Systems im Fahrzeug nach den Vorgaben der UN.ECE-Regelungen der Art. 29 Gruppe und der wachsende Einsatz von Artificial Intelligence im Fahrzeugumfeld[12] stellt sich für die Praxis als große Herausforderung dar und erfordert pragmatische Antworten. Mögen diese und andere offene Fragen auf Grund ihrer Komplexität an anderer Stelle zu diskutieren sein als in den Guidelines. Sie zeigen jedoch, wie dringend eine umfassende Betrachtung des sich stetig fortentwickelnden Rechtsrahmens im Umgang mit personenbezogenen Fahrzeugdaten von Nöten ist und noch aussteht.

II. Scope der Guidelines

Die Guidelines erfassen eine große Bandbreite an Verarbeitungsszenarien im Connected Vehicle Umfeld. Bemerkenswert ist zum Einen, dass einzelne, auf den ersten Blick unverdächtige Verarbeitungshandlungen den Guidelines unterfallen sollen, wie z. B. „standalone mobile applications", die hierfür weder mit dem Fahrzeug verbunden sein noch Daten aus diesem beziehen müssen, solange sie mit dem „environment of driving" „related" sind.[13] Zum Anderen werden praktisch wichtige Anwendungsbereiche wie Verarbeitungssituationen im Beschäftigungsverhältnis[14] oder der Einsatz von Kameras im Fahrzeugumfeld[15] ausgenommen. Das scheint im Ergebnis konsequent, da entsprechende Fragestellungen vielfach von nationalen Besonderheiten überlagert werden, die eine einheitliche Guidance durch das EDPB wohl deutlich erschwert hätten. Nach vielfacher Kritik in der Konsultationsphase enthalten die Guidelines nun entsprechende Klarstellungen.

1 Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications (Version 2.0) vom 9.3.2021, abrufbar unter https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf (Abruf: 29.6.2021); vgl. im Übrigen Vorversion der Guidelines (Version 1.0) vom 28.1.2020, abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-12020-processing-personal-data_en (Abruf: 29.6.2021).

2 Guidelines, Rn. 13.

3 Verordnung (EU) 2015/758 vom 29.4.2015 über die Typengenehmigung und eCall In-Vehicle Systeme.

4 Verordnung (EU) 2019/2144 vom 27.11.2019 über die Typengenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern.

5 Verordnung (EU) 2018/858 vom 30.5.2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern.

6 Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren vom 27.7.2021, abrufbar unter https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html (Abruf: 2.8.2021).

7 Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23.6.2021.

8 Verordnung (EU) 2018/858 vom 30.5.2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern.

9 Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, abrufbar unter https://www.escrypt.com/sites/default/files/2020-07/ECE-TRANS-WP29-2020-079-Revised-2.pdf (Abruf: 2.7.2021).

10 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union zur Aufhebung der Richtlinie (EU) 2016/1148, abrufbar unter https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)823&lang=de (Abruf: 2.7.2021).

11 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.5.2021.

12 So i. E. auch *Seewald*, RAW 2020, 130 unter Verweis auf *ENISA*, Towards a framework for policy development in cybersecurity, 2018, S. 15, abrufbar unter: https://www.enisa.europa.eu/publications/considerations-in-autonomous-agents (Abruf: 2.7.2021).

13 Guidelines, Rn. 21, 28, unter Verweis auf GPS Navigation Applications, die den Guidelines stets unterfallen sollen.

14 Guidelines, Rn. 32.

15 Guidelines, Rn. 35.

III. Datenschutzrechtliche Verantwortlichkeit im Umgang mit Fahrzeugdaten

Der für die Anwendbarkeit datenschutzrechtlicher Regelungen erforderliche Personenbezug ergibt sich oftmals aus der Verknüpfung von (technischen) Fahrzeugdaten mit der Fahrzeugidentifikationsnummer (FIN)[16] oder anderer personenbezogener Identifier im Fahrzeugumfeld wie z. B. der SIM-Kartennummer oder Kunden-ID für Connectivity Dienste. Das EDPB sieht hier einen naturgemäß weiten Anwendungsbereich,[17] den es sinnvoll u. a. für rein technische bzw. anonymisierte Daten oder bestimmte Arten von Fahrzeugumgebungsdaten zu beschränken gilt.[18]

Fraglich erscheint nach Lektüre der Guidelines, in welchem Umfang Hersteller und Dienstleister für reine „In-Car" Datenverarbeitungsvorgänge als Verantwortliche anzusehen sind. Deuten frühere Behördenstellungnahmen darauf hin, dass reine „In-Car" Datenverarbeitungsvorgänge ohne Verarbeitung personenbezogener Daten durch den Hersteller oder Dritte grundsätzlich nicht den Vorgaben der DS-GVO unterfallen,[19] scheint die Position des EDPB unklar. So nimmt es auf der einen Seite reine In-Car Datenverarbeitungen über die sog. „Haushaltsausnahme"[20] vom Anwendungsbereich der DS-GVO aus,[21] um an anderer Stelle unter Verweis auf Erwägungsgrund (EG) 18 der DS-GVO die Anwendbarkeit der DS-GVO auf Unternehmen herauszustellen, die die Mittel („means"), also z. B. die entsprechende Technologie im Fahrzeug, für die im Rahmen der Haushaltsausnahme erfolgende Verarbeitung bereitstellen.[22]

Die Einordnung hat weitreichende Folgen, u. a. im Hinblick auf das Bestehen einer den Vorgaben der Art. 12 ff. DS-GVO entsprechenden Informationspflicht durch den Hersteller auch für reine In-Car Datenverarbeitungsprozesse, was wenig sachgerecht erscheint.

Ob das EDPB hier eine besondere Form der Gesamtverantwortung der Hersteller sieht und wenn ja mit welchen genauen Folgen, bleibt unklar.[23] Unter Bezugnahme auf die EG 18 und 78 der DS-GVO sieht das EDPB Hersteller zumindest in der Pflicht, die Vorgaben von Privacy-by-Design und Privacy-by-Default gemäß Art. 25 GDPR im Stadium der Entwicklung umzusetzen. Systematisch vermag die Argumentation des EDPB nicht zu überzeugen.[24] Die zitierten Erwägungsgründe dürften den Anwendungsbereich der DS-GVO nicht auf Datenverarbeitungsprozesse ausweiten (können), an denen der Hersteller nicht beteiligt ist. Selbiges gilt für die Verlagerung der Anwendbarkeit der DS-GVO in das bloße Entwicklungsstadium von Produkten, was sich bereits daran zeigt, dass Hersteller zur Umsetzung dieser Grundsätze nach der DS-GVO bloß „ermutigt" werden sollen (vgl. EG 78).[25]

Ungeachtet dessen dürfte es sich in der Industrie als Standard durchgesetzt haben, dass Hersteller entsprechender Technologien und Dienste Privacy-by-Design als wesentlichen Baustein in die Entwicklung integrieren,[26] nicht zuletzt im Hinblick auf etwaige Folgefragen, die sich ggf. aus der nicht datenschutzkonformen Nutzbarkeit eines Produktes oder Dienstes ergeben könnten.[27]

IV. Rechtsgrundlagen der Verarbeitung von Fahrzeugdaten

Aus Sicht des EDPB ist die Einwilligung die wesentliche Rechtsgrundlage für die Verarbeitung von Fahrzeugdaten. Ungeachtet der teils heftigen Kritik aus der Industrie folgt das EDPB weiter der Anwendung von Art. 5 Abs. 3 der ePrivacy-Richtlinie und versteht das vernetzte Fahrzeug als „Endgerät" im Sinne der ePrivacy-Richtlinie. Dies hat zur Folge, dass insbesondere die Erhebung von Daten aus dem Fahrzeug und deren anschließende Nutzung der Einwilligung der Betroffenen bedürfen, wenn die Verarbeitung nicht (i) für den Telekommunikationsvorgang (ii) oder zur Erbringung eines vom Nutzer erbetenen Dienstes zwingend erforderlich ist. Weitere Ausnahmen u. a. für die Verarbeitung im Fall berechtigter Interessen sind nicht vorgesehen.

Die Sichtweise erscheint fraglich, betrachtet man sich die verschiedenen gesetzlichen und richterrechtlich geprägten Vorgaben zur Produktbeobachtung oder die umfassenden Cyber-Security Pflichten für Automobilhersteller. Mangels ausdrücklicher gesetzlicher Vorgaben werden diese oftmals die Verarbeitung personenbezogener Daten auf Basis einer Interessenabwägung i. S. v. Art. 6 Abs. 1 lit. f DS-GVO erfordern und auf der Grundlage einer Einwilligung nur schwer umsetzbar sein.[28]

Gegen die ausufernde Auslegung sprechen freilich gute Gründe. Connected Vehicles sind im Unterschied zu Smartphones geschlossene Systeme, deren Netzwerke nicht öffentlich verfügbar sind und können schon deshalb nicht ohne Weiteres miteinander verglichen werden. Allenfalls einzelne Komponenten können die Eigenschaft als Endgerät erfüllen, wenn zusätzlich die jeweiligen Tatbestandsvoraussetzungen erfüllt sind, insbesondere dass die Verar-

16 Gemeinsame Erklärung der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26.1.2015, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Gemeinsames%20Papier%20DSK%20und%20VDA.pdf (Abruf: 4.7.2021).

17 Guidelines, Rn. 29.

18 Vgl. hierzu u. a. *Eul*, in: Leupold/Wiebe/Glossner (Hrsg.), Münchner Anwaltshandbuch IT-Recht, 4. Aufl. 2021, Teil 10.2, Rn. 29 mit weiteren Nachweisen.

19 *CNIL*, Compliance Package Connected Vehicles and Personal Data, Oktober 2017, S. 19, 20, abrufbar unter https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf (Abruf: 4.7.2021).

20 Zum Begriff *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 2, Rn. 23 f.

21 Guidelines, Rn. 74, 75.

22 Guidelines, Rn. 30.

23 So wohl i. E. *Weichert*, SVR 2014, 205.

24 Guidelines, Rn. 75.

25 So i. E. wohl auch *Spindler/Horvath*, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 25 DS-GVO, Rn. 5; *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 837; vgl. hierzu auch Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, S. 15, 17, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf (Abruf: 3.7.2021): „*Die DS-GVO stellt mit ‚data protection by design/data protection by default' Grundsätze auf, die sich an Hersteller richten, nimmt Hersteller aber nicht als solche in die Pflicht. Die Forderung (…) läuft, wenn sie ausschließlich an die Verantwortlichen gerichtet wird, häufig ins Leere.*"

26 Gemeinsame Erklärung der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26.1.2015, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Gemeinsames%20Papier%20DSK%20und%20VDA.pdf (Abruf: 4.7.2021); vgl. hierzu jetzt auch die Pflicht der Hersteller zur Instruktion des Halters über bestimmte Verarbeitungsprozesse im Fahrzeug gem. § 1g Abs. 3 des Gesetzes zum autonomen Fahren (vgl. Fn. 6), auf die hier nicht weiter eingegangen werden soll.

27 Vgl. hierzu u. a. *Potthoff*, ZD 2020, 348.

28 *Kahl/Behrendt*, RAW 2020, 86 f.; *Eul*, in: Leupold/Wiebe/Glossner (Hrsg.), Münchner Anwaltshandbuch IT-Recht, 4. Aufl. 2021, Teil 10.2, Rn. 29 m. w. N.

beitung auf Daten beruht, die von einer externen Quelle, etwa einem anderen Endgerät, mittels elektronischer Kommunikation in die Systeme des Fahrzeugs gelangen.[29]

Zudem scheint die Anwendung des Begriffs des „Endgeräts" auf Multi-User-Situationen und die vielschichtigen Beziehungen im Connected Vehicle Umfeld zwischen „machine to machine" (M2M), „vehicle to vehicle" (V2V) oder „vehicle to infrastructure" (V2I) Kommunikation nicht recht zu passen.[30] Ein entsprechendes Einwilligungserfordernis wirft vielfältige Folgefragen auf, die sich nur schwer auflösen lassen.[31]

Zudem erscheint die Bezugnahme auf die noch geltende ePrivacy-Richtlinie im Lichte der aktuellen Entwicklungen rund um eine neue ePrivacy-Verordnung unglücklich.[32] So ist unklar, ob die kommende ePrivacy-Verordnung entgegen der aktuellen Fassung[33] nicht doch wie frühere Entwurfsversionen mehr Spielräume für die Verarbeitung von Daten aus Endgeräten für berechtigte Interessen bringen wird.[34]

Ungeachtet aller Kritik folgt das EDPB weiterhin der Anwendbarkeit des Art. 5 Abs. 3 ePrivacy-Richtlinie und lehnt zugleich die Möglichkeit einer zweckändernden Verarbeitung gemäß Art. 6 Abs. 4 GDPR neben Art. 5 Abs. 3 ePrivacy-Richtlinie ab.

Dass die Verarbeitung von Fahrzeugdaten für die Erfüllung gesetzlicher Pflichten und verschiedener berechtigter Interessen möglich bleiben muss, dürfte einleuchten. Eine Klarstellung des EDPB in diese Richtung wäre wünschenswert gewesen. Die Industrie wird sich bis auf Weiteres mit der Position des EDPB arrangieren müssen und ihrerseits nach kreativen Lösungen suchen, um u. a. die Anforderungen im Bereich der Produktbeobachtung, Qualitätsmanagement und Cybersecurity mit den Sichtweisen des EDPB in Einklang zu bringen.

V. Spezielle Verarbeitungsszenarien

Die Verarbeitung spezieller Kategorien personenbezogener Daten, namentlich Positionsdaten, biometrischer Daten und Daten, die Aufschluss über mögliche Gesetzesverfehlungen liefern, soll nach Auffassung des EDPB nur unter Einhaltung sehr restriktiver Vorgaben möglich sein.[35]

So soll der Einsatz biometrischer Verfahren zur Autorisierung im Fahrzeug nur auf Basis einer Einwilligung erfolgen. Das überrascht auf den ersten Blick wenig, handelt es sich bei diesen Daten regelmäßig um besondere Kategorien personenbezogener Daten, für deren Verarbeitung gemäß Art. 9 DS-GVO in der Regel eine Einwilligung erforderlich ist. Eine Art. 6 Abs. 1 lit. b DS-GVO (Vertragserfüllung) vergleichbare Rechtsgrundlage findet sich in der DS-GVO für die Verarbeitung dieser Daten gerade nicht.

Biometrische Daten sind danach ausschließlich im Fahrzeug zu verarbeiten, ohne dass sie an Stellen außerhalb des Fahrzeugs übermittelt werden (z. B. an einen Cloud-Dienst). Zudem sind dem Betroffenen alternative Lösungen anzubieten, die ohne Verarbeitung entsprechender Daten auskommen (z. B. Entsperren eines Accounts oder Autorisierung einer Transaktion auch ohne Nutzung biometrischer Daten).

Dürften die Vorgaben den aktuellen Branchenstandards weitestgehend entsprechen, stellen sie Hersteller jedoch weiterhin vor vielfältige Herausforderungen, u. a. bei der Umsetzung der strikten formalen Vorgaben an eine wirksame Einwilligung im Fahrzeugumfeld oder den noch nicht abschließend geklärten Anforderungen bei reiner In-Car Verarbeitung entsprechender Daten.

Anders als biometrische Daten unterfallen Positionsdaten *de lege lata* grundsätzlich keinen besonderen Verarbeitungsvoraussetzungen.[36] In der Kritik steht deshalb insbesondere die Anforderung des EDPB, dass die Positionsbestimmung im Fahrzeug nur aktiviert werden soll, wenn der Nutzer seinerseits einen entsprechenden Dienst nutzt. Gleiches gilt für die Forderung, dem Nutzer die Möglichkeit einzuräumen, die Positionsbestimmung (jederzeit) deaktivieren zu können.[37] Die Vorgaben berücksichtigen nur unzureichend die Anforderungen im Bereich der vernetzen Assistenzsysteme und Schutz vor Cyber-Angriffen, die oftmals auf Positionsdaten angewiesen sind, ohne dass mit ihnen zwingend ein konkreter, vom Nutzer in Anspruch genommener Dienst verbunden ist.[38]

Revidiert zu haben scheint das EDPB erfreulicherweise seine zuletzt ungewöhnlich weite Interpretation des Art. 10 DS-GVO, die es nach der Vorversion der Guidelines auch auf die Verarbeitung bloßer Angaben zur Geschwindigkeit oder anderer, eine mögliche Verletzung von Straßenverkehrsvorschriften indizierender Daten, ausweiten wollte.

VI. Datenminimierende Strategien und Transparenz

Das EDPB betont in den Guidelines erneut, dass die umfassende Kontrolle des Betroffenen über die im und außerhalb des Fahrzeug stattfindenden Datenverarbeitungsvorgänge

29 Vgl. Stellungnahme des ACEA im Konsultationsverfahren vom 29.4. 2020, S. 8 ff., abrufbar unter https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_guidelines_connected_vehicles_acea_comments_final.pdf (Abruf: 4.7.2021).

30 Stellungnahme VDA zum Referentenentwurf für ein Telekommunikations-Telemedien-Datenschutz-Gesetz vom 13.1.2021, abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-TTDSG/vda.pdf?__blob=publicationFile&v=4 (Abruf: 4.7.2021), dort konkret zum mit Art. 5 Abs. 3 ePrivacy-Richtlinie identischen § 22 TTDSG-E; zu den Begriffen der M2M, V2V und V2I Kommunikation und deren Implikationen für die Einordung unter der ePrivacy Richtlinie vgl. die Stellungnahme von HERE Technologies im Konsultationsverfahren vom 2.4.2020, S. 2, abrufbar unter https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/here_comments_on_edpb_guidelines_2703.pdf (Abruf: 4.7.2021).

31 Vgl. *Eul*, in: Leupold/Wiebe/Glossner (Hrsg.), Münchner Anwaltshandbuch IT-Recht, 4. Aufl. 2021, Teil 10.2, Rn. 35 m. w. N.

32 So i. E. auch die Stellungnahme des ACEA, S. 8, abrufbar unter https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/edpb_guidelines_connected_vehicles_acea_comments_final.pdf (Abruf: 4.7.2021).

33 Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EG (Regulation on Privacy and Electronic Communication), abrufbar unter https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf (Abruf: 2.7.2021).

34 Vgl. *Kahl/Behrendt*, RAW 2020, 85 m. w. N.; vgl. hierzu nunmehr auch § 25 TTDSG (Fn. 7), mit dem die Formulierung aus Art. 5 Abs. 3 ePrivacy-Richtlinie fast wortgleich in deutsches Recht umgesetzt wird, auf den an dieser Stelle aber nicht weiter eingegangen werden soll.

35 Guidelines, Rn. 62 ff.

36 Ausnahmen bestehen für Positionsdaten im Bereich der Telekommunikation, für die ggf. weitergehende Vorgaben der §§ 91 ff. TKG gelten.

37 Guidelines, Rn. 64.

38 So i. E. zutreffend wohl auch die Stellungnahme von HERE Technologies im Konsultationsverfahren, S. 2–4, abrufbar unter https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/here_comments_on_edpb_guidelines_2703.pdf (Abruf: 4.7.2021).

Grundvoraussetzung für ein datenschutzkonformes Setup sind. Besonderes Augenmerk legt das EPDB auf datenminimierende Technologien, die frühzeitige Löschung und Anonymisierung bzw. Pseudonymisierung von Fahrzeugdaten sowie die gezielte Verteilung von Datenverarbeitungsprozessen im und außerhalb des Fahrzeugs je nach Erforderlichkeit (sog. „hybrid processing").[39]

Gefordert wird zudem die Implementierung eines „Profile Management Systems", mit dem der Nutzer die Datenerhebung, -speicherung und -verarbeitung im Fahrzeug gezielt und mit einfachen Mitteln steuern kann. Zudem wird erneut die Umsetzung bzw. Ermöglichung der Ausübung des Rechts auf Datenportabilität betont.[40]

Erfreuliche Klarstellungen finden sich zur Frage der Transparenz und Bereitstellung der Pflichtinformationen gemäß Art. 13, 14 DS-GVO im Fahrzeugumfeld. Auch wenn bereits gängige Praxis, bestätigt das EDPB die Möglichkeit eines „layered approaches", der die Bereitstellung der maßgeblichen Informationen u. a. in Vertragsunterlagen, der Bedienungsanleitung oder einer elektronischen Dokumentation im On-Board Computer ermöglicht.[41]

Die vom EDPB angesprochenen Icons u. a. zur Anzeige des Status der Vernetzung des Fahrzeugs dürften als Beispiel für die Umsetzung der Informationspflichten und nicht als zwingende Vorgabe zu verstehen sein.[42] Dass der Trend jedoch zur verstärkten Sichtbarmachung und vereinfachten Übersicht von aktiven Funktionen und Datenverarbeitungsprozessen im Fahrzeug geht, zeigen die in China geplanten PRC Data Rules.[43] Hersteller müssen die Entwicklung deshalb im Auge behalten.

Klingt die Herangehensweise des EDPB insgesamt schlüssig und deckt sich weitestgehend mit bisherigen Forderungen der Datenschutzaufsichtsbehörden,[44] bleiben viele Fragen offen, die die Branche aktuell umtreiben.

So stellt sich u. a. die Frage, wie weit Konfigurationsmöglichkeiten für den Nutzer bei komplexen Services und Funktionen tatsächlich reichen müssen, um den Vorgaben der DS-GVO zu Privacy-by-Default zu entsprechen, ohne dabei den Sinn und Zweck einzelner Funktionen (z. B. die Erhöhung der Verkehrssicherheit) zu konterkarieren.

Unklar bleibt auch, welche Daten der Nutzer nach Auffassung des EDPB einsehen bzw. löschen können muss, insbesondere, wenn es sich bei diesen um system-relevante Daten handelt, die für die Sicherheit des Fahrzeugs oder einzelner Funktionen erforderlich sind.

VII. Security

Zuletzt fordert das EDPB von Herstellern, Service Providern und anderen Anbietern die Umsetzung hoher IT-Sicherheitsstandards im Connected Vehicle Umfeld, um unberechtigte Datenzugriffe wirksam verhindern zu können.[45] Der Katalog an vorgeschlagenen Maßnahmen enthält auf den ersten Blick viele Standards, die Hersteller und Anbieter bereits umsetzen oder zumindest in ihre Planungen integriert haben dürften.

Einzelne Punkte springen jedoch ins Auge:

U. a. soll das Schlüsselmanagement individuell pro Fahrzeug und nicht pro Fahrzeuglinie gestaltet werden. Das Fahrzeug soll mit einem Alarmsystem für Cyberangriffe versehen werden und die Speicherung einer Log-Historie von (maximal) sechs (6) Monaten ermöglichen, um Angriffe auf das Fahrzeugsystem nachvollziehen zu können. Entsprechende Logdaten sind (wohl) zwingend auszuwerten.

Zudem soll das Fahrzeug ein Patchmanagement erhalten, dass das umgehende Patchen von Schwachstellen während der gesamten Nutzungsdauer des Fahrzeugs ermöglichen soll.

Scheinen sich die Vorgaben auf den ersten Blick stark an die Vorgaben zur Cyber-Security für (vernetze) Fahrzeuge der UN.ECE WP.29 anzulehnen,[46] stellt sich zum einen die Frage, ab wann Hersteller bzw. Anbieter entsprechender Dienste die jeweiligen Vorgaben umsetzen müssen. Entfalten die Vorgaben der Verordnungen Nr. 155 und Nr. 156 der UN.ECE WP.29 erst ab dem kommenden Jahr und dann auch nur schrittweise ihre Wirksamkeit,[47] dürften die Vorgaben des EDPB ab sofort zu berücksichtigen sein.

Vor diesem Hintergrund wäre ein Abgleich der sich inhaltlich überschneidenden Regelungen sowie eine entsprechende Klarstellung zum Verhältnis der Normenkreise zueinander hilfreich gewesen. Zudem wäre in Anbetracht der strikten Position des EDPB zu Art. 5 Abs. 3 ePrivacy-Richtlinie eine Klarstellung zur Zulässigkeit der Verarbeitung personenbezogener Fahrzeugdaten zu Zwecken der Cybersecurity sinnvoll gewesen, um der bestehenden Rechtsunsicherheit zu begegnen.

VIII. Use Cases

Der Vollständigkeit halber sei darauf hingewiesen, dass das EDPB in den Guidelines die Prinzipien anhand vier (4) konkreter Use Cases erläutert, namentlich Pay-as-you-drive Services, eCall, Unfallforschung und Fahrzeugdiebstahl.[48] Auf eine weitere Darstellung hierzu soll an dieser Stelle jedoch verzichtet werden.

IX. Fazit und Ausblick

Das Papier bietet einen guten Überblick über die datenschutzrechtlichen Grundsätze im Umgang mit Fahrzeug-

39 Guidelines, Rn. 78.
40 Guidelines, Rn. 91.
41 Guidelines, Rn. 77, 88; vgl. hierzu weiterführend *Eul*, in: Leupold/Wiebe/Glossner (Hrsg.), Münchner Anwaltshandbuch IT-Recht, 4. Aufl. 2021, Teil 10.2, Rn. 38 m. w. N.
42 Guidelines, Rn. 89.
43 Several Provisions on Car Data Security Administration vom 12.5. 2021, abrufbar unter http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm (Abruf: 2.7.2021).
44 Vgl. hierzu u. a. Gemeinsame Erklärung der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26.1.2015, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Gemeinsames%20Papier%20DSK%20und%20VDA.pdf (Abruf: 4.7.2021); sowie CNIL, Compliance Package Connected Vehicles and Personal Data, Oktober 2017, abrufbar unter https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf (Abruf: 4.7.2021).
45 Guidelines, Rn. 94, 95.
46 Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, abrufbar unter https://www.escrypt.com/sites/default/files/2020-07/ECE-TRANS-WP29-2020-079-Revised-2.pdf (Abruf: 2.7.2021).
47 Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, abrufbar unter https://www.escrypt.com/sites/default/files/2020-07/ECE-TRANS-WP29-2020-079-Revised-2.pdf (Abruf: 2.7.2021).
48 Guidelines, Rn. 103 ff.

daten. Es dürfte der Industrie ein gutes Gespür dafür vermitteln, in welche Richtung sich das EDPB zukünftig bei der Bewertung entsprechender datenschutzrechtlicher Fragestellungen bewegen wird: in Richtung einer weiterhin strikten Interpretation der gesetzlichen Vorgaben mit Transparenz und Selbstbestimmung als die wesentlichen Grundprinzipien, die es nach Ansicht des EDPB beim Fahrzeugdatenschutz zu verwirklichen gilt. Ein effizientes Privacy-by-Design Konzept in der Fahrzeug-Entwicklung bleibt somit ein unverzichtbarer Bestandteil eines jeden Datenschutzmanagementsystems in der Automobilindustrie, sei es durch entsprechende interne Guidelines für Entwickler („Kochbuch"), die frühzeitige Prüfung von Verarbeitungsprozessen mit Fahrzeugdaten im Wege eines Privacy Impact Assessments,[49] oder die Entwicklung eines individuellen Car Data Management Systems zur proaktiven Steuerung und Dokumentation der Fahrzeugdatenverarbeitung.

Die strikten Sichtweisen des EDPB werden es Herstellern und Anbietern von Diensten im Connected Vehicle Umfeld auch weiterhin erschweren, klare Antworten auf drängende Fragen der Vereinbarkeit datenschutzrechtlicher Vorgaben und der steigenden Anforderungen u. a. an die IT Sicherheit im vernetzten Fahrzeug zu finden und die insoweit bestehenden Konflikte sachgerecht aufzulösen.

Dabei dürften die gesetzlichen Vorgaben durchaus einen gewissen Spielraum zur Umsetzung praktikabler Lösungen bieten, die jedoch eine umfassende Auseinandersetzung mit den verschiedenen Rechtsregimen und – wie so oft im Datenschutz – ein gewisses Maß an Kreativität erfordern werden!

49 Guidelines, Rn. 82.

RA Dr. Marc Ruttloff und RAin Rebecca Schulga, Stuttgart*

Digitalisierung im Verkehrssektor – Regulierungsbedarf im PBefG und im StVG!

Infolge zunehmender Digitalisierung und technischen Fortschritts entstehen alternative Personenbeförderungsangebote, die bis vor Kurzem noch zeitlich befristete Ausnahmegenehmigungen erforderten, weil sie nur bedingt mit dem bestehenden Rechtsrahmen vereinbar sind. Die Neuerungen im PBefG und StVG sollen nun Betreibern von alternativen Personenbeförderungsangeboten, insbesondere bei der Nutzung autonomer Fahrfunktionen, die nötige Innovations- und Planungssicherheit geben.

I. Digitalisierung und alternative Personenbeförderungsangebote

Mit der Digitalisierung steigt das Angebot an alternativen Personenbeförderungsangeboten und damit auch das Erfordernis, den bestehenden Rechtsrahmen an die neue Mobilitätswelt anzupassen. Im Fokus stehen hierbei die sog. *Pooling-Dienste*, das heißt digitalbasierte Beförderungsangebote, bei denen sich mehrere Personen mit unterschiedlichen Ankunftszielen eine Fahrstrecke teilen, nachdem sie per App ihren Anfangs- und Endpunkt der Fahrstrecke angegeben haben. Das große Potential der Pooling-Dienste besteht darin, dass die Verkehrsmittel per Anfrage (on demand) herbeigerufen und durch die Nutzung mehrerer Fahrgäste effizient ausgelastet werden können. Vor allem auf dem Land können hierdurch Angebotslücken zwischen dem Öffentlichen Personennahverkehr (ÖPNV) und dem Individualverkehr geschlossen werden. Die Geschäftsmodelle sind dabei unterschiedlich ausgestaltet: Teilweise werden Kraftfahrzeuge eingesetzt, die auf Wunsch des Fahrgastes auch als Ganzes unter Ausschluss weiterer Fahrgäste und ohne Bindung an Haltepunkte gebucht werden können[1] oder aber es werden beispielsweise Kraftomnibusse eingesetzt, die zusätzlich autonome Fahrfunktionen nutzen, indem sie führerlos ausschließlich zwischen fiktiven Haltestellen umherfahren, die der Fahrgast per App als Anfangs- und Endpunkt auswählen kann.[2]

II. Regulierungsbedarf im Personenbeförderungsrecht

Die oben beschriebenen Personenbeförderungsangebote unterliegen den Regularien des Personenbeförderungsrechts und sind genehmigungspflichtig, wenn sie der entgeltlichen oder geschäftsmäßigen Beförderung von Personen mit Straßenbahnen, mit Oberleitungsomnibussen (Obussen) und mit Kraftfahrzeugen dienen.

1. Zur bisherigen Rechtslage

Die bislang im Personenbeförderungsgesetz (PBefG) gesetzlich normierten Verkehrstypen waren für die alternativen Personenbeförderungsangebote zu eng, sodass eine reguläre Genehmigungsfähigkeit ausgeschieden ist. Pooling-Dienste sind Mischverkehr, der in der Praxis bislang ausschließlich über Ausnahmetatbestände genehmigt wurden. Während Betreibern von regulär genehmigungsfähigen Personenbeförderungsangeboten ein durchsetzbarer Anspruch auf Erteilung der Genehmigung zusteht, liegt die Entscheidung über die Erteilung einer Ausnahmegenehmigung für Mischverkehr im Ermessen der zuständigen Landesbehörde. Die Genehmigungspraxis nach dem PBefG war bislang uneinheitlich.[3] Die bisherige Rechtslage war für

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

1 So etwa bei dem Mietwagenverkehr des Fahrdienstes „MOIA" aus dem Volkswangen-Konzern, https://www.hamburg.de/pressearchiv-fhh/10970098/2018-04-26-bwvi-moia/ (Abruf: 16.6.2021).

2 So etwa bei dem Projekt „HEAT" der Hamburger Hochbahn AG, https://www.hochbahn.de/hochbahn/hamburg/de/Home/Naechster_Halt/Ausbau_und_Projekte/projekt_heat (Abruf: 16.6.2021) und geplant im Forschungsprojekt „RABus", www.projekt-rabus.de (Abruf: 17.6.2021).

3 *Zeil/Prinz zur Lippe*, GewArch 2018, 405, 406.