MMR
Zeitschrift für IT-Recht und Recht der Digitalisierung

in Kooperation mit: Bitkom · davit im DAV · eco · game · Legal Tech Verband · VAUNET

CLEMENS ARZT / STEVEN KLEEMANN / CHRISTIAN PLAPPERT / ROLAND RIEKE / DANIEL ZELLE

Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung

Rechtliche und technische Anforderungen im Verbund

www.mmr.de

twitter.com/MMRZeitschrift

de.linkedin.com/showcase/zeitschriftmmr

Beilage zu MMR
7/2022

Seiten 593–614
25. Jahrgang · 15. Juli 2022
Verlag C.H.BECK München

1851202207

MMR
Zeitschrift für IT-Recht und Recht der Digitalisierung
TK · IT-Security · Medien · Robotik · KI · Datenschutz · Games
In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

Beilage zu MMR 7/2022

CLEMENS ARZT / STEVEN KLEEMANN / CHRISTIAN PLAPPERT / ROLAND RIEKE / DANIEL ZELLE

Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung

Rechtliche und technische Anforderungen im Verbund

Durch die Novelle des Straßenverkehrsgesetzes vom 12.7.2021 wurde mit §§ 1d bis 1l StVG ein umfassender Rechtsrahmen für zunehmend vernetzte Kraftfahrzeuge mit autonomen Fahrfunktionen in Deutschland geschaffen, um Rechtssicherheit für deren Betrieb zu gewährleisten. Dabei fanden auch Regelungen zur Datenverarbeitung in solchen Kraftfahrzeugen Eingang in das Gesetz. Ob die Novelle gelungen ist, wird die weitere Diskussion und Umsetzung in die Praxis zeigen. Im vorliegenden Beitrag werden die rechtlichen Neuregelungen mit Blick auf Datenschutz sowie IT- und Datensicherheit thematisiert und aus technischer Sicht hinterfragt.

Die notwendigen umfangreichen technischen Vorgaben zum Schutz der Cybersicherheit in vernetzten Kraftfahrzeugen sind in der zugehörigen „Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften (AFGBV)" geregelt.

Das Gesetz wie die Verordnung werden hier einer umfangreichen Analyse unterworfen, die indes nicht in der rechtlichen Betrachtung stehen bleibt, sondern zugleich umfangreiche technische Anforderungen hiermit verbindet und damit Cybersicherheit, Datenschutz und Recht verwebt.

Der Beitrag erörtert ausführlich die neue Rechtslage vor dem Hintergrund des nationalen und europäischen Datenschutzrechts und den Vorgaben der dazugehörigen UNECE-Regelungen. Von besonderem Interesse sind in diesem Zusammenhang der neue § 1g StVG und die in der AFGBV enthaltenen Regelungen für den Betrieb eines digitalen Datenspeichers sowie die Anforderungen an die Sicherheit im Bereich der Informationstechnologie bei Datenspeicherung und Datenübermittlung automatisierter Kraftfahrzeuge. Die hier als relevant identifizierten UNECE-Regelungen 155 (Cybersicherheit) und 156 (Software-Updates) werden in Folge dieser Neuregelung künftig einen noch wichtigeren Stellenwert im Automobilbereich einnehmen.

Die an die rechtlichen Ausführungen anschließende technische Analyse in diesem Beitrag leitet IT- und Datensicherheitsanforderungen sowie beispielhafte Maßnahmen zur wirkungsvollen Umsetzung ab und vergleicht diese mit den Maßgaben der einschlägigen UNECE-Regelungen. Dabei wird aufgezeigt, welche technischen Maßnahmen erforderlich sind, um diesen Anforderungen gerecht zu werden. Die hieraus abgeleiteten technischen Maßnahmen nehmen Bezug auf die rechtlichen Regelungen und ermöglichen dadurch einen belastbaren Abgleich von Technik und Recht. Der Nachweis, dass die UNECE-Regelungen erfüllt sind, kann durch Dokumentation bzw. Audit erfolgen. Es gibt aber zurzeit noch einen großen Spielraum für die Interpretation, durch welche konkreten Maßnahmen die Anforderungen abgedeckt werden. Dies gilt insbesondere auch im Hinblick auf den geforderten Datenschutz.

Im Ergebnis wird ein aktueller Gesamtüberblick über die Thematik aus rechtlicher wie technischer Sicht gegeben, wobei auch konkrete rechtliche und technische Vorschläge für den künftigen Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion vorgestellt werden.

I. Einleitung

Automatisierte und vernetzte Kraftfahrzeuge prägen die rechtliche[1], technische und auch allgemeine gesellschaftliche Debatte um künftige Mobilität maßgeblich. Mit der Novelle des Straßenverkehrsgesetz (StVG) vom Juli 2021[2] wurden in §§ 1d bis 1l StVG gesetzliche Regelungen geschaffen, die weltweit den ersten Rechtsrahmen für automatisiertes Fahren auf SAE-Level 4 bilden sollen.[3] Neben den gesetzlichen Neuerungen im StVG tritt zudem mit Beschluss des Bundesrats v. 20.5.2022[4] und der darauffolgenden Veröffentlichung im Bundesgesetzblatt die „Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV)"[5] zum 1.7.2022 in Kraft.

Dieser Beitrag beinhaltet eine rechtliche und technische Analyse der gesetzlichen Neuregelungen. Einführend werden die Neuerungen zur Datenverarbeitung durch die Novelle für das „autonome" Fahren im neuen § 1g StVG behandelt und daran anschließend die AFGBV sowie deren Anhänge und darin enthaltenen Regelungen zu Cybersicherheit vertieft betrachtet. In Teil V.1. werden technische Anforderungen (TA) aus den Normtexten abgeleitet, die dann in Teil V.2. des Beitrags für eine technische Evaluation genutzt werden. Dazu werden die abgeleiteten TA zunächst tabellarisch zusammengefasst und beschrieben. Beispielhaft werden anschließend generische technische Maßnahmen in einem Maßnahmenkatalog vorgeschlagen, die geeignet sind, die TA umzusetzen. Den Abschluss der technischen Analyse bildet einen Abgleich der von uns abgeleiteten TA mit den Maßnahmen, die in der UNECE-Regelung 155 zur Cybersicherheit in Kraftfahrzeugen vorgeschlagen werden. Die UNECE-Regelung 155 zu Cybersicherheit und die UNECE-Regelung 156 zu Software-Updates gehören neben den Ausführungen zur StVG-Novelle zu den Kernthemen des Beitrags. Dabei wird die rechtliche Betrachtung angereichert durch Betrachtungen aus Sicht der IT-und Cybersicherheit.

Zentraler Begriff des Datenschutzrechts ist das Tatbestandsmerkmal des personenbezogenen Datums. Das Vorhandensein eines Personenbezugs stellt die Verknüpfung zwischen technischer Datenverarbeitung und einem davon betroffenen Menschen her und löst die Anwendbarkeit des Datenschutzrechts aus.[6] Dabei wird mit der Verarbeitung personenbezogener Daten der europa- und verfassungsrechtliche Schutz dieser Daten und das Recht auf informationelle Selbstbestimmung iSv Art. 7 und 8 GRCh sowie Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG eröffnet.[7]

Ob es sich bei der Datenverarbeitung beim Betrieb von Kraftfahrzeugen mit autonomen Fahrfunktion um personenbezogene Daten handelt oder rein technische, kann nicht abstrakt beantwortet werden, sondern muss im konkreten Fall geprüft werden. Nur erstere unterliegen den Anforderungen des Datenschutzrechts. Handelt es sich hingegen ausschließlich um technische Daten ohne Personenbezug, müssen für diese nur die Anforderungen an die IT- und Cybersicherheit eingehalten werden, was selbstverständlich auch für personenbezogene Daten gilt. Der Beitrag ist daher so aufgebaut, dass die rechtliche Betrachtung den potenziellen Personenbezug in den Fokus rückt, während die technische Ausarbeitung datenschutzrechtliche Aspekte wie auch die cybersicherheitsrelevanten Aspekte einer rein technischen Datenverarbeitung mitberücksichtigt. Der sich an die rechtliche Betrachtung anschließende technische Teil arbeitet in einem ersten Schritt die aus der Analyse der neuen Vorschriften im StVG und den hierzu erlassenen Verordnungen resultierenden Anforderungen bezüglich der Cybersicherheit heraus, für die in einem nächsten Schritt die dazugehörigen Maßnahmen näher ausgeführt werden. Die im zweiten Teil herausgearbeiteten technischen Anforderungen finden sich bereits (in Klammern) an den entsprechenden Stellen der vorab beschriebenen Rechtslage und können als Verweis nach unten betrachtet werden. Damit versucht der Beitrag eine vertiefte Analyse der neuen Rechtslage unter Berücksichtigung der tatsächlichen technischen Möglichkeiten und den wiederum aus diesen abzuleitenden Anforderungen zu präsentieren. So wird hier (soweit ersichtlich) erstmals ein vertiefter „Gesamtblick" auf die Datenverarbeitung und Cybersicherheit von Kraftfahrzeugen mit autonomen Fahrfunktionen vorgestellt.

Der Beitrag gliedert sich wie folgt. Kapitel II und III beschäftigen sich mit der rechtlichen Analyse der hier relevanten und beschriebenen Neuregelungen. Nach einem kurzen Zwischenfazit in Kapitel IV folgt unter V die umfangreiche technische Analyse. Diese setzt sich aus einer Zusammenfassung und Beschreibung der technischen Anforderungen, der Definition des generischen Maßnahmenkatalogs und dem Abgleich der TA mit den in der UNECE-Regelung 155 vorgeschlagenen Maßnahmen zusammen. Dem folgen ein Fazit und ein Ausblick auf offene Fragen.

II. Datenverarbeitung nach § 1g StVG

Datenverarbeitung im Rahmen von Fahrzeugautomatisierung stellt ein kontroverses Thema dar. Die Neuregelung in § 1g StVG wird diese Diskussionen nicht beenden. Das zeigt sich bereits darin, dass das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) deutliche Bedenken im Vorfeld der Neuregelung geäußert hat und es womöglich mit der neuen Regierung Nachbesserungen geben oder die Ausarbeitung eines übergreifenden Mobilitätsdatengesetz erfolgen könnte.[8]

Nach § 1g Abs. 1 S. 1 StVG sind Kraftfahrzeughalter verpflichtet, 13 verschiedene Kategorien von Daten beim Betrieb des Kraftfahrzeugs zu speichern (TA04: Datenisolation). Fraglich ist indes, wie diese eine solche Speicherung vornehmen sollen, legen doch die Hersteller fest, wie und wo Daten im Kraftfahrzeug automatisch gespeichert werden und welche Schnittstellen es für den Datenaustausch dort geben soll. Zweifelhaft erscheint auch, ob die Norm in der jetzigen Fassung als rechtliche Verpflichtung in Sinne der Art. 6 Abs. 1 lit. c DS-GVO genügt.[9] Die rechtliche Verpflichtung aus Art. 6 Abs. lit. c DS-GVO ist keine Verpflichtung, die vertraglich begründet wird, sondern diese besteht Kraft objektiven Rechts der Europäischen Union oder eines Mitgliedstaats.[10] Grundlegende Voraussetzung der Datenverarbeitung auf Grund einer rechtlichen Verpflichtung ist dabei die klare und präzise Festlegung zumindest des Verarbeitungszwecks.[11]

---

1 Grundlegend dazu bereits: Gasser/Arzt et al., Rechtsfolgen zunehmender Fahrzeugautomatisierung, Berichte der Bundesanstalt für Straßenwesen (BASt), Heft F 83, 2012.

2 Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren v. 12.7.2021, BGBl. 2021 3108.

3 S. zu den Neuregelungen Kleemann/Arzt, RAW 2/2021, 99-105, abrufbar unter: https://www.hwr-berlin.de/prof/clemens-arzt/#c5053.

4 VO zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften, BR-Drs. 86/22 v. 24.2.2022; BR-Drs. 86/22(B) Beschl. v. 20.5.2022.

5 VO zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften v. 24.6.2022 BGBl. 2022 986.

6 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Karg, 2019, DSGVO Art. 4 Nr. 1 Rn. 1.

7 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Karg, 2019, DSGVO Art. 4 Nr. 1 Rn. 1.

8 Abrufbar unter: www.handelsblatt.com/politik/deutschland/plaene-des-verkehrsministers-mangelnder-datenschutz-justizministerin-lehnt-scheuers-gesetz-zum-autonomen-fahren-ab/26830532.html; Verbraucherzentrale Bundesverband e.V., Stellungnahme zum Entwurf eines Gesetzes zum Autonomen Fahren sowie der Autonome Fahrzeug-Genehmigungs- und Betriebsverordnung v. 1.2.21, S. 10 f.

9 Steege SVR 2021, 128 (135).

10 Paal/Pauly, DS-GVO BDSG/Frenzel, 3. Aufl. 2021, DS-GVO Art. 6 Rn. 16; BeckOK DatenschutzR/Albers/Veit, DS-GVO Art. 6 Rn. 48.

11 Kühling/Buchner, DS-GVO – BDSG/Buchner/Petri, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 82.

Ungeklärt ist auch, in welchem Format solche Daten dem Kraftfahrt-Bundesamt (KBA) und den dort in § 1g StVG genannten Stellen[12] zur Verfügung gestellt werden sollen. Wenn die in § 1g Abs. 1 S. 1 Nr. 1–13 StVG genannten Daten gespeichert und ggf. übermittelt werden sollen, müssten hier die Kraftfahrzeughersteller selbst adressiert und festgelegt werden, dass diese die genannten Daten in einem für die empfangenden Stellen lesbaren Format zur Verfügung stellen oder dies den Kraftfahrzeughaltern oder über das Fahrzeug verfügenden Personen technisch und organisatorisch ermöglichen müssen. Die in § 1g Abs. 1 StVG gelisteten Daten enthalten sowohl solche, bei denen ein Personenbezug angenommen werden kann (zB Nr. 1 Fahrzeugidentifikationsnummer und Nr. 2 Positionsdaten), wie auch solche, die rein technische Daten darstellen. Die Norm beschränkt sich demnach nicht auf rein technische Daten, sondern beinhaltet auch die Verarbeitung von personenbezogenen Daten. Inwiefern damit die Anwendbarkeit des Datenschutzrechts gegeben ist, gilt es im Einzelnen festzustellen.

Die in § 1g Abs. 1 StVG aufgeführten Daten wurden im Gesetzgebungsvorgang teilweise angepasst und konkretisiert. Auffällig ist, dass ein früherer Referentenentwurf noch vorsah, diese Daten nur „beim Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion zu speichern" während das Gesetz dies nun für den gesamten „Betrieb des Kraftfahrzeugs" fordert. Unklar bleibt auch, in welchem Verhältnis § 1g Abs. 1 StVG gegenüber den Absätzen 2, 4 und 5 steht. Scheint die Pflicht zur Speicherung der Daten gemäß dem Wortlaut in § 1g Abs. 1 StVG während des gesamten Betriebs zu bestehen, sollen die genannten Daten gem. § 1g Abs. 2 StVG jedoch lediglich anlassbezogen in den in Absatz 2 Nr. 1–4 genannten Fällen gespeichert werden.

Fraglich ist auch, ob § 1g Abs. 2 StVG eine hinreichend präzise Abgrenzung zu den Regelungen zur Datenspeicherung nach § 63a StVG[13] beinhaltet. Zwar gilt § 63a StVG nur für die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion iSd § 1a StVG, während § 1g StVG die Datenverarbeitung von Kraftfahrzeugen mit autonomen Fahrfunktionen regelt. Die Regelungsorte scheinen indes keiner konsistenten Systematik zu folgen.

Beachtlich ist die im Laufe des Gesetzgebungsprozesses erweiterte Begründung zu § 1g Abs. 3 StVG. Hier wird nunmehr gesetzlich verankert, dass die Kraftfahrzeughersteller technisch und organisatorisch den Kraftfahrzeughaltern die „Datenhoheit"[14] über die beim Betrieb der autonomen Fahrfunktion anfallenden Daten (TA05: Interventionsfähigkeit) ermöglichen müssen.[15] Grund dafür – und das ist bedeutsam – ist die Annahme, dass Kraftfahrzeughalter die Berechtigten hinsichtlich der Daten beim autonomen Fahren sind.[16] Hiermit bezieht die Bundesregierung Stellung zu einem in der Literatur höchst umstrittenen Thema.[17] Allerdings sind auch hier, wie bei den meisten Neuregelungen, lediglich die Kraftfahrzeughalter vom Gesetz erfasst. Nicht geregelt wurde, inwiefern zB die betroffenen Fahrzeugführer oder auch Passagiere und deren personenbezogenen Daten (zB zu Ort und Zeit der Kraftfahrzeugnutzung) vom Gesetz abgedeckt werden und welche Regelungen hinsichtlich ihrer personenbezogenen Daten gelten sollen. Hinzu kommen Daten aus der sensorischen Umfelderfassung. Auch hier sprechen gute Gründe dafür, diese offenen Punkte in einem verkehrsmittelübergreifenden Mobilitätsdatengesetz zu regeln.[18] In einem solchen Gesetz könnte eine Klassifikation von Daten und der Verteilung der Rollen von Betroffenen und Verantwortlichen geregelt werden, ebenso wie Anonymisierungspflichten oder die konkrete Ausgestaltung von „data protection by design" und „data protection by default" (Art. 25 DS-GVO, Erwägungsgrund 78). Die Umsetzung einer solchen Regelung sollte indes auf EU-Ebene geschehen, um nicht in Widerspruch mit der DS-GVO zu geraten.[19]

Darüber hinaus werden die Hersteller in § 1g Abs. 3 StVG verpflichtet, den Kraftfahrzeughaltern bestimmte Einstellungsmöglichkeiten zur Privatsphäre zu eröffnen (TA05: Interventionsfähigkeit) und über die Datenverarbeitung in der autonomen Fahrfunktion zu informieren (TA06: Transparenz). Fraglich ist, ob § 1g Abs. 3 StVG die Diskussion bezüglich „data protection by design" und „data protection by default" ausreichend abbildet. Dass die Regierung in der Begründung von „privacy by design" spricht (ein Terminus, welcher sich weder in der deutschen, noch in der englischen Version der DS-GVO findet) unterstreicht, dass hier offenbar noch kein abschließend durchdachtes Konzept zur Anwendung kommt. Nach Art. 25 Abs. 2 DS-GVO muss der für die Datenverarbeitung Verantwortliche, hier nach § 1g Abs. 3 S. 1 StVG zumindest hinsichtlich der Schaffung der Voraussetzungen, der Hersteller, geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung ausschließlich personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden (TA04: Datenisolation). Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, die Speicherfrist und ihre Zugänglichkeit (TA05: Interventionsfähigkeit, TA07: Sicheres Löschen). Solche Maßnahmen müssen insbesondere im Zusammenhang mit der Verarbeitung durch Dritte (zB Verkehrsplattformen, Road-Side-Units oder generell V2X-Kommunikation) sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person einem unbestimmten Kreis von Personen zugänglich gemacht werden (TA05: Interventionsfähigkeit, TA01: Vertrauliche Datenverarbeitung, TA03: Authentische Datenverarbeitung). Dass § 1g Abs. 3 StVG dies hinreichend umsetzt, muss bezweifelt werden.

Nach § 1g Abs. 6 StVG dürfen Behörden, die für die Genehmigung, Prüfung und Überwachung des Betriebsbereichs zuständig sind, Daten nach Absatz 1 und die Namen sowie Qualifikation der Technischen Aufsicht erheben, speichern und verwenden. Diese Daten sind gem. § 1g Abs. 6 S. 2 StVG, sobald sie für die Zwecke nach Satz 1 nicht mehr erforderlich sind, unverzüglich zu löschen, spätestens aber drei Jahre nach Einstellung des Betriebs des entsprechenden Kraftfahrzeugs (TA04: Datenisolation, TA07: Sicheres Löschen). Damit ist nur hinsichtlich nicht mehr in Betrieb befindlicher Kraftfahrzeuge eine konkrete Speicherdauer angegeben, wohingegen die Zulässigkeit sonst am eher vagen Maßstab der Erforderlichkeit zu messen ist. Die genannte Speicherdauer und unverzügliche Löschung nach Weg-

12 Nachfolgend als „zuständige Behörden" im Zusammenhang mit den Neuregelungen im StVG und der AFGBV genannt, s.a. § 1 Abs. 3 AFGBV.
13 Zur Kritik vgl. nur: Hoeren NZV 2018, 153; Lutz, DAR 2019, 125; Schirmer NZV 2017, 253; Steege NZV 2019, 459; Steinrötter ZD 2021, 513 ff.
14 Vgl. zur Diskussion u.a.: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hornung/Spiecker gen. Döhmann, 2019, Einleitung Rn. 310; Martini/Kolain/Neumann/Rehorst/Wagner MMR-Beil. 6/2021, 3; Schweitzer GRUR 2019, 569; Hoeren MMR 2019, 5; Stender-Vorwachs/Steege NJOZ 2018, 1361; 25; Kühling/Sackmann ZD 2020, 24; Michl NJW 2019, 2729; Wischmeyer/Herzog NJW 2020, 288; im speziellen Kontext der Fahrzeugautomatisierung beispielhaft: Bundesministerium für Verkehr und digitale Infrastruktur (BMVI, Hrsg.), „Eigentumsordnung" für Mobilitätsdaten?, August 2017; Hoeren NZV 2018, 153; Weichert NZV 2017, 507; Wendt ZD-Aktuell 2018, 06034.
15 BR-Drs. 155/21, 38.
16 BR-Drs. 155/21, 38.
17 Vgl. dazu zB die Positionen in: Weichert SVR 2014, 201; Weichert SVR 2014, 241; Stender-Vorwachs/Steege NJOZ 2018, 1361; Hoeren NZV 2018, 153; Kühling/Sackmann ZD 2020, 24; Steege SVR 2021, 1.
18 Vgl. Ausführungen in: vzbv – Verbraucherzentrale Bundesverband, Positionspapier Fahrerlos alle Mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht, Positionspapier v. 6.3.2021, S. 8 ff.
19 Wagner SVR 2021, 287 (291).

fall der Erforderlichkeit gilt auch für Daten, die nach § 1g Abs. 4 StVG beim KBA gespeichert werden (TA04: Datenisolation, TA07: Sicheres Löschen). Hinsichtlich der unverzüglichen Löschung nach Wegfall der Erforderlichkeit für Daten nach § 1g Abs. 4, Abs. 6 StVG ist daher unklar, was die erforderliche „Überwachung des sicheren Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion" konkret umfasst und wann und unter welchen Voraussetzungen diese entfällt. Hier ist eine Konkretisierung nötig, um auch die Löschfrist in datenschutzkonformer Art und Weise umzusetzen.

Problematisch ist zudem, dass die gesamte Neuregelung in § 1g StVG ausschließlich die Datenverarbeitung im Kraftfahrzeug selbst und deren Übermittlung an das KBA und zuständige Behörden regelt (§ 1g Abs. 1 S. 2 StVG), soweit dies für deren Aufgabenerfüllung (Überwachung des sicheren Betriebs und Betriebsbereichs, § 1g Abs. 4, Abs. 6 StVG) erforderlich ist. Was hingegen nicht geregelt scheint, ist die Datenverarbeitung für und aus der Vernetzung von Kraftfahrzeugen untereinander (Vehicle-to-Vehicle – V2V) wie auch solchen aus der Kommunikation mit der Infrastruktur oder anderen Entitäten (Vehicle-to-Everything – V2X). Auch Daten aus Kraftfahrzeugen, die bei den Herstellern selbst verarbeitet werden und zur Steuerung des Kraftfahrzeugs notwendig sind, werden von den Regelungen zur Datenverarbeitung nicht erfasst. Ferner finden sich keinerlei Regelungen bezüglich unterschiedlicher Kommunikationsstandards (WLAN oder Mobilfunk), was iSd Technologieneutralität zu erklären wäre. Diese Art der (externen) Datenverarbeitung ist lediglich in der Verordnung (AFGBV) spezifiziert (dazu s. unter III.1. im Detail). Hier hätten einerseits bereits Anknüpfungspunkte im StVG geschaffen werden können. Andererseits verfolgt der Gesetzgeber mit der gesamten Ausgestaltung der Neuregelungen im Gesetz einen dynamischen Ansatz. Grundsätzliche Anforderungen und Definitionen werden im Gesetz normiert, wohingegen die konkreten technischen Spezifika sodann in einer Rechtsverordnung geregelt werden.[20] Damit soll frühzeitig und flexibel auf künftige technische Weiterentwicklungen reagiert werden können, indem nicht ggf. das Gesetz geändert, sondern lediglich die Verordnung an technische Neuerungen angepasst werden muss.[21] Eine ähnliche Handhabung ist auch auf EU-Ebene zu erkennen. Bei der Ausgestaltung der am 6.7.2022 in Kraft tretenden VO EU 2019/2144[22], welche erstmalig auch unionsrechtliche Definitionen der Begriffe „automatisiertes"[23] und „vollautomatisiertes Fahrzeug"[24] enthält, werden grundsätzliche Definitionen und technische Vorgaben innerhalb der Verordnung geregelt und für die technischen Detailfragen ist eine noch zu erarbeitenden Durchführungsverordnung mit umfangreichen und detaillierten Anhängen vorgesehen.[25]

III. Cybersicherheit und Software-Updates

Cybersicherheit und Software-Updates spielen im Automobilbereich eine immer wichtigere Rolle. Insbesondere mit Blick auf die zunehmende Vernetzung von Kraftfahrzeugen untereinander wie auch mit der Infrastruktur und anderen Entitäten, steigt die Gefahr von potenziellen Cyberbedrohungen und -angriffen. Relevant ist daher vornehmlich die AFGBV, welche konkret Cybersicherheitsmaßnahmen für Kraftfahrzeuge adressiert und dabei auf die UNECE-Regelung 155 (Uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems)[26] verweist. Zu beachten ist zudem die UNECE-Regelung 156 (Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system)[27], die Vorgaben für Software-Updates enthält. Mit steigender Fahrzeugautomatisierung werden die Nutzung von Software und relevante Security-Updates, welche auch sog. „Software-over-the-air-Updates" beinhalten können, für die Kraftfahrzeugsteuerung immer relevanter. Daher ist es notwendig, diese auch gegen potenziell sicherheitsrelevante Cyberangriffe über eine für Over-the-air-Updates vorgesehene Schnittstelle abzusichern.

1. Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV)

Ergänzung sollen die neuen Normen des StVG in der AFGBV finden. Hiermit sollen die in §§ 1d bis 1l StVG neu geregelten Anforderungen konkretisiert und die für die Genehmigung autonomer Fahrfunktionen zu erfüllenden Vorgaben bestimmt werden. Regelungen zur Datenverarbeitung sind in § 15 AFGBV vorgesehen, wonach nähere Anforderungen zu den genauen Zeitpunkten der Datenspeicherung, den Parametern der Datenkategorien und den Datenformaten in Anlage 2 der AFGBV geregelt werden sollen. Dort werden die in § 1g Abs. 1 Nr. 1–13 StVG genannten Daten teilweise hinsichtlich des Zeitpunkts der Datenspeicherung, Parametern der Datenkategorien und Datenformaten spezifiziert. Dabei werden in der Anlage lediglich beispielhaft Datenformate genannt. Welche Daten im konkreten Einzelfall bei welchem Kraftfahrzeug von spezifischen Herstellern anfallen und in welchem Datenformat, kann daher nicht aus der Norm selbst abgeleitet werden, sondern bedarf einer Einzelfallbetrachtung.

Unstreitig ist dabei, dass es sich bei einer Datenverarbeitung in Verbindung mit der Fahrzeugidentifikationsnummer (FIN) und bei Positionsdaten um personenbezogene Daten iSv Art. 4 Nr. 1 DS-GVO handelt. Während ein früherer Entwurf der AFGBV[28] noch Beispiele enthielt, welche Daten etwa als Vernetzungsparameter nach § 1g Abs. 1 Nr. 7 StVG angesehen werden können (IMSI, IMEI oder einer Rufnummer)[29], fehlt hierzu in der verabschiedeten Version jegliche Konkretisierung. In Bezug auf die weiteren genannten Daten stellt sich in allen Fällen die Frage, inwiefern es technisch möglich oder auch sinnvoll ist, einzelne Daten, welche in den Steuergeräten der Kraftfahrzeuge generiert werden, von der Fahrzeug-Identifizierungsnummer (FIN) zu trennen und wie in der Praxis tatsächlich dabei verfahren wird. Sollen Daten prinzipiell von der FIN getrennt werden, müsste sichergestellt werden, dass diese auch weiterhin für den eigentlichen Zweck (etwa der sicheren Erfüllung der Fahraufgabe oder der Datenspeicherung bei Konfliktszenarien) brauchbar sind. Darüber hinaus stellt sich die Frage, ob eine Identifikation später dennoch durch die Zusammenführung mit weiteren Daten möglich ist. Demzufolge stellen sich hier Fragen bezüglich der

20 Wolfers/Schlenkhoff RAW 1/2022, 24 (29).
21 Wolfers/Schlenkhoff RAW 1/2022, 24 (29).
22 VO (EU) 2019/2144 des Europäischen Parlaments und des Rates v. 27.11.2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der VO (EU) 2018/858.
23 Art. 3 Abs. 2 Nr. 21 VO (EU) 2019/2144.
24 Art. 3 Abs. 2 Nr. 22 VO (EU) 2019/2144.
25 Wolfers/Schlenkhoff RAW 1/2022 (31).
26 ECE/TRANS/WP.29/2020/79 REVISED, abrufbar unter: http://www.unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
27 ECE/TRANS/WP.29/2020/80, abrufbar unter: https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf.
28 Entwurf einer VO zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV), Referentenentwurf des Bundesministeriums für Verkehr und digitale Infrastruktur, Bearbeitungsstand 27.1.2021, Anlage III.
29 IMSI, IMEI oder Rufnummer stellen regelmäßig personenbezogene Daten dar, vgl. dazu: Beschluss des Düsseldorfer Kreises v. 16.6.2014, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, S. 5, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Archiv/DuesseldorferKreis/OHApps.pdf;jsessionid=31DF534E3CE16B7ABA6D9BE81835E33C.intranet222?__blob=publicationFile&v=2; Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes/Graulich, 2019, BKAG § 18 Rn. 23.

Zweckbindung gem. Art. 5 Abs. 1 lit. b DS-GVO (TA04: Datenisolation), aber auch hinsichtlich der wirksamen und sinnvollen Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) oder Anonymisierung (TA08: De-Identifikation). Bei einer Anonymisierung ist die DS-GVO nicht anwendbar (vgl. auch Erwägungsgrund 26 DS-GVO). Scheidet eine Trennung aus Gründen der zweckgemäßen Nutzbarkeit aus, können alle damit verbundenen Daten personenbezogene Daten darstellen. Hier gilt es, die Vorgaben der DS-GVO wie aus dem Recht auf informationelle Selbstbestimmung im Einzelfall einzuhalten.

Zu beachten sind darüber hinaus auch die Anforderungen an Kraftfahrzeuge mit autonomer Fahrfunktion, die in der Anlage 1 zur Verordnung beschrieben sind. Hier soll lediglich auf zwei Bereiche Bezug genommen werden: den digitalen Datenspeicher gem. Anlage 1 Teil 3 und die dort in Teil 5 beschriebenen Anforderungen an die Sicherheit im Bereich der Informationstechnologie.

a) Digitaler Datenspeicher

Im digitalen Datenspeicher von Kraftfahrzeugen mit autonomen Fahrfunktionen sollen (sobald dafür entsprechende datenschutzrechtliche Regelungen in Kraft getreten sind) die Daten ereignisbasiert ausschließlich für die in § 1g StVG genannten Zwecke gespeichert werden (TA04: Datenisolation). Dazu zählen die Durchführung von Verkehrssicherheitsanalysen und die Bewertung der Wirksamkeit spezifischer Maßnahmen wie etwa das Verhalten des Kraftfahrzeugs in Konfliktszenarien, die für die Zuordnung von Haftung und rechtlicher Verantwortung und für Forschung zum Zweck der Verbesserung der Verkehrssicherheit und der Gewährleistung datenschutzrechtlicher Vorgaben gespeichert werden.[30] Diese Daten sollen gem. § 15 Abs. 2 AFGBV nur für das KBA und die in § 1g StVG genannten zuständigen Behörden zum Zwecke einer Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten zur Verfügung stehen (TA01: Vertrauliche Datenverarbeitung). Konkret heißt es dazu in Anlage 1 Teil 3 der AFGBV, dass der integrierte Datenspeicher den Vorgaben der Art. 24, 25 und 32 DS-GVO entsprechen muss (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA07: Sicheres Löschen, TA08: De-Identifikation, TA09: Verfügbarkeit, TA10: Resilienz) und „ereignisbasiert und während des Betriebes nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfasst, speichert und verwendet" (TA04: Datenisolation). Dabei sind „die zu erfassenden Daten ... in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt."[31]

Diese ausschließliche Beschränkung der Nutzung und abschließende Aufzählung der zu verarbeitenden Daten ist auf den ersten Blick aus datenschutzrechtlicher Perspektive zu begrüßen. Allerdings fällt auf, dass bei den genannten Verkehrssicherheitsanalysen unklar ist, ob und ggf. welche weiteren Daten verarbeitet werden, die über die § 1g Abs. 1 StVG genannten hinausgehen. Darüber hinaus werden bereits in § 1g Abs. 2 Nr. 1–4 StVG nicht nur das Unfallszenario genannt, sondern explizit auch weitere Anlässe zur Datenspeicherung (TA04: Datenisolation). Weiter berechtigt § 1g Abs. 4 StVG das KBA alle in Absatz 1 genannten Daten und gem. Nr. 2 Vor- und Nachname der als Technische Aufsicht eingesetzten Person sowie Nachweise über ihre fachliche Qualifikation zu „speichern und zu verwenden, soweit dies für die Überwachung des sicheren Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion erforderlich ist" (TA01: Vertrauliche Datenverarbeitung).

Unklar bleibt indes der Maßstab der Erforderlichkeit.[32] In § 1g Abs. 5 StVG wird als Zweck der Datenverarbeitung die Forschung genannt (TA04: Datenisolation). Hier ist jedoch zu beachten, dass § 1g Abs. 5 S. 1 Hs. 3 StVG die Datenverarbeitung für Forschungszwecke auf nicht personenbezogene Daten beschränkt. § 1g Abs. 6 StVG erlaubt den für die Überprüfung des Betriebsbereichs zuständigen Behörden, die Daten gem. Absatz 6 Nr. 1 und 2 zu erheben, speichern und zu verwenden, sofern es für die Überprüfung und Überwachung des Betriebsbereichs notwendig ist (TA01: Vertrauliche Datenverarbeitung). Letztlich können auch Dritte die Herausgabe von Daten für die Geltendmachung von Haftungsansprüchen gem. § 1g Abs. 7 StVG verlangen. Die in der AFGBV beschriebene ausschließliche Beschränkung der Nutzung der Daten zum Zweck der Erhöhung der Verkehrssicherheit stimmt demzufolge nicht überein mit den anderen in § 1g StVG genannten Zwecken der Datenverarbeitung.

Das Datenschutzniveau des Datenspeichers soll von den Herstellern entsprechend dem Stand der Technik bezüglich Datenschutz- und Sicherheitsvorgaben sichergestellt werden. Es muss ein System zur Zugangskontrolle sowie kryptografische Schutzverfahren entsprechend den technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI-TR) genutzt werden (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA04: Datenisolation, TA05: Interventionsfähigkeit, TA06: Transparenz, TA07: Sicheres Löschen, TA08: De-Identifikation, TA11: Nachweisbarkeit), wobei das BSI bereits in die Ausgestaltung einzubeziehen ist. Der Datenspeicher darf nicht flüchtig sein und die Daten müssen auch im stromlosen Zustand erhalten bleiben (TA09: Verfügbarkeit). Laut AFGBV soll der Datenspeicher ab Beginn der Kraftfahrzeugzulassung die Daten ausschließlich im Kraftfahrzeug speichern.[33]

Der Zugang zu den gespeicherten Daten soll über die normierte 16-polige On-Board-Diagnose-Schnittstelle (OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 (Straßenfahrzeuge – Modulare Kommunikationsschnittstelle im Kraftfahrzeug (MVCI) – Teil 1: Hardwaredesign Anforderungen) unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle erfolgen. In bestimmten Situationen oder Ereignissen sollen die Daten auch über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige Stelle übermittelt werden können.[34] Hier stellt sich die Frage, wie realisiert werden soll, dass alle notwendigen Daten an das KBA über die OBD-Schnittstelle übertragen und abgesichert werden können, wenn nur in nicht näher definierten Ausnahmefällen oder nach ebenfalls nicht näher bestimmten Ereignissen diese über eine WAN-Verbindung an die zuständige staatliche Stelle gesendet werden.[35] Während in der Entwurfsfassung der AFGBV, welche der Europäischen Kommission zur Notifizierung vorlag,[36] noch ein etwaiger Hinweis auf eine solche Situation in der damaligen Anlage I Teil 5 Nr. 14 AFGBV zu finden war, in der es hieß: „[e]rkennt der Hersteller Manipulationen am Kraftfahrzeug mit autonomer Fahrfunktion, so sind diese unverzüglich dem Kraftfahrt-Bundesamt und der ... zuständigen Behörde ... mitzuteilen und entsprechende Maßnahmen

30 Vgl. Ausführungen in AFGBV Anlage 1 Teil 3 und § 1g StVG.
31 AFGBV Anlage 1 Teil 3.
32 Haupt NZV 2021, 172 (175).
33 Vgl. dazu AFGBV Anlage 1 Teil 3 Nr. 13.2 und Anlage 2.
34 Vgl. Ausführungen in AFGBV Anlage 1 Teil 3 Nr. 13.2.
35 Vgl. Ausführungen in AFGBV Anlage 1 Teil 3 Nr. 13.2.
36 Entwurf einer VO zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Notifizierungsnummer: 2021/344/D, Bearbeitungsstand 10.6.2021, abrufbar unter: https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2021&num=344.

einzuleiten", findet sich dieser in der verabschiedeten Fassung nicht mehr. Ob dieser versteckte Hinweis eine solche Situation gemeint haben könnte oder ob die in § 1g Abs. 2 StVG genannten Anlässe (TA04: Datenisolation) die „bestimmten Ereignisse" darstellen, die eine Übertragung[37] per WAN-Verbindung ermöglichen, bleibt völlig unklar. Hier bedarf es einer weiteren Konkretisierung durch den Verordnungsgeber. Darüber hinaus ist auch unklar, ob Kraftfahrzeughalter über die Datenübertragung per WAN benachrichtigt werden müssen und wie die Nachvollziehbarkeit des Inhalts der Datenübertragung gewährleistet ist.

Zugang und Abruf der gespeicherten Daten soll nur für das KBA und die zuständige Stelle (TA01: Vertrauliche Datenverarbeitung) möglich sein.[38] Gleiches (TA01: Vertrauliche Datenverarbeitung) gilt für die Datenspeicherung und Datenübermittlung.[39] Die Datenübertragung und Speicherung soll laut AFGBV den Anforderungen an die Sicherheit der Informationstechnologie, wie in Teil 5 der Anlage 1 zur AFGBV beschrieben, genügen. Insbesondere sollen die Daten gemäß dem Stand der Technik und unter Beachtung der Vorgaben aus Art. 24, 25 und 32 DS-GVO vor missbräuchlicher Verwendung und Manipulation geschützt werden (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung).

Die notwendige Schnittstelle birgt die Gefahr, dass Daten während der Übermittlung an die zum Empfang berechtigten Stellen abgefangen werden. Die nach § 1g StVG zu speichernden Daten können durchaus personenbezogene sein. Hier könnte im Zusammenhang mit der in der AFGBV getroffenen Regelung zur Übermittlung von Daten über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) eine potenzielle datenschutzrechtliche Schwachstelle geschaffen worden sein.

Die vorab beschriebenen Regelungen beziehen sich vorrangig auf die Datenverarbeitung im Kraftfahrzeug, auf den Zugriff auf diese Daten sowie teilweise die Übertragung an das Kraftfahrzeug. Für die Übertragung muss laut AFGBV eine sichere elektronische Steuereinheit (SECU) als Informationsgateway genutzt werden, welche den Schutz von Daten, die extern an das Kraftfahrzeug gesendet[40] werden, sicherstellen soll.[41] Für die Frage, ob es auch einer vertraulichen Datenübertragung aus dem Kraftfahrzeug bedarf, findet sich lediglich ein Hinweis in Anlage 1 Teil 1 Nr. 6 und insbesondere in Teil 3 Nr. 13.2 lit. d AFGBV, wonach die Datenspeicherung und die Datenübermittlung an das KBA und die in der AFGBV genannten zuständigen Behörden den Anforderungen an die Sicherheit im Bereich der Informationstechnologie genügen sollen. Die Daten müssen dem Stand der Technik gemäß und unter Beachtung der Vorgaben der Art. 24, 25, 32 DS-GVO vor Manipulation und missbräuchlicher Verwendung geschützt werden (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung). Hier bedarf es der Klärung, wie die durch die AFGBV geforderte Schnittstelle und der Zugang zu dieser autorisiert werden und die Authentizität des Auslesenden[42] geprüft werden kann. Offen ist demnach, wie eine Ende-zu-Ende-Vertraulichkeit auf beiden Seiten tatsächlich sichergestellt werden kann.

Weiterhin scheint noch nicht abschließend geklärt zu sein, ob eine vertrauliche Übermittlung der Daten innerhalb des Kraftfahrzeugs von der Speicherstelle zur WAN-Verbindung sichergestellt werden muss. Es ist hier also notwendig, zwischen verschiedenen Formen der Datenverarbeitung (Verarbeitung im Kraftfahrzeug, Übermitteln von Daten an das Kraftfahrzeug und Empfangen von Daten) zu differenzieren und das jeweilige Level an Schutz im Detail zu beschreiben. Bezüglich der Sicherheit der Funkverbindungen ist festzuhalten, dass diese gemäß der AFGBV gegen unerlaubte Zugriffe in der Art geschützt werden müssen, wie es die Art. 24, 25, 32 DS-GVO vorgeben (TA01: Vertrauliche Datenverarbeitung) und darüber hinaus der Aufbau der Verbindung und die Datenübertragung nach dem Stand der Technik mit offenen und etablierten Standards gesichert und verschlüsselt (TA: Alle Anforderungen) werden.[43] Dazu wird beispielhaft auf Transport Layer Security (TLS) Version 1.3 verwiesen, bei der wie in der technischen Richtlinie TR-02102-2[44] kryptografische Verfahren Empfehlungen und Schlüssellängen beschrieben sind.

Die Integrität der Datenverarbeitung in Kraftfahrzeugen kann auch durch die Wartung und Instandhaltung berührt werden, insbesondere mit Blick auf Kraftfahrzeuge mit autonomen Fahrfunktionen auf Grund der hohen Abhängigkeit dieser Kraftfahrzeuge von einer Vielzahl von Datenerhebungen und -verarbeitungen. Die Wartbarkeit von Kraftfahrzeugen mit autonomen Fahrfunktionen muss daher seitens der Hersteller sichergestellt werden. Deshalb haben diese Hersteller gem. § 12 Abs. 1 Nr. 1–7 AFGBV umfangreiche Dokumentationspflichten zu erfüllen. Dazu zählt u.a. nach Nr. 3 „ein Konzept zur Sicherheit im Bereich der Informationstechnologie nach Anlage 1 Nummer 15 zu erstellen und nach Anlage 3 Nummer 4 zu dokumentieren." Nach Nr. 4 ist „die Durchführbarkeit einer wiederkehrenden technischen Fahrzeugüberwachung nach Anlage 1 Nummer 7.3 zu dieser Verordnung sicherzustellen" (TA02: Integritätsgeschützte Datenverarbeitung). Gemäß Nr. 7 hat der Hersteller – wie bereits beschrieben – „nach den Anforderungen an den digitalen Datenspeicher nach Anlage 1 Nummer 13 ein Sicherheitskonzept zu erstellen, das den Vorgaben der Art. 24, 25 und 32 der [DS-GVO] entspricht und eine Datenschutzfolgeabschätzung nach Art. 35 der [DS-GVO] beinhaltet."

Die Halter sind wiederum gem. § 13 Abs. 1 Nr. 1, Nr. 3 AFGBV dazu verpflichtet sicherzustellen, dass, „unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeuges mit autonomer Fahrfunktion regelmäßig überprüft werden, [und] 3. unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuches für das Kraftfahrzeugs mit autonomer Fahrfunktion" durchzuführen (TA02: Integritätsgeschützte Datenverarbeitung). Weiterhin muss nach § 13 Abs. 1 Nr. 2 AFGBV täglich vor Betriebsbeginn eine erweiterte Abfahrkontrolle gemäß den Anforderungen nach Absatz 7 durchgeführt werden. Das bedeutet, dass vor jedem Betriebsbeginn eine Probefahrt mit aktiviertem autonomem System durchgeführt werden muss, bei welcher neben der Bremsanlage (§ 13 Abs. 7

37 Handelt es sich bei dem in der AFGBV genutzten Begriff „Übertragung" oder „Datenübertragung" um personenbezogene Daten, ist damit im hier behandelten Kontext eine Verarbeitung iSd Art. 4 Nr. 2 DS-GVO gemeint. Eine Übertragung kann in beide Richtungen erfolgen. Sowohl das Empfangen, als auch das Senden von personenbezogenen Daten an und in das Kraftfahrzeug sind davon umfasst.

38 AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. b.

39 AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. d.

40 Das Senden von Kraftfahrzeugdaten mit Personenbezug stellt eine Datenübertragung iSd Art. 4 Nr. 2 DS-GVO dar, wobei die Verantwortlichkeit im hier vorliegenden Kontext gem. Art. 4 Nr. 7 DS-GVO idR beim Hersteller liegen wird.

41 AFGBV Anlage 1 Teil 1 Nr. 6.

42 Das Auslesen von Kraftfahrzeugdaten mit Personenbezug stellt eine Datenübertragung iSd Art. 4 Nr. 2 DS-GVO dar, wobei der Auslesende als Verantwortlicher gem. Art. 4 Nr. 7 DS-GVO gilt.

43 AFGBV Anlage 1 Teil 5 Nr. 16.

44 Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf;jsessionid=9BC508348FB80D4169577C6B7A95BC97.internet461?__blob=publicationFile&v=4.

Nr. 1 AFGBV), Lenkanlage (Nr. 2) und weiteren Anforderungen (Nr. 3–7) auch gemäß Nr. 6 „sicherheitsrelevante elektronisch geregelte Fahrzeugsysteme sowie die Sensorik zur Erfassung externer und interner Parameter" überprüft werden müssen (TA02: Integritätsgeschützte Datenverarbeitung). Neben der Frage, wie eine solche Anforderung in der Praxis umgesetzt werden soll, ist auch nicht ersichtlich, was bei möglichen Fehlermeldungen geschehen soll. Eine Pflicht, die alle 90 Tage anstehende Gesamtprüfung nach § 13 Abs. 1 Nr. 3 an das KBA und die für ihre Aufgabenerfüllung weiteren zuständigen Behörden zu übermitteln, ist gemäß Nr. 4 auch nur auf diese Prüfung beschränkt und nicht auch auf die erweiterte Abfahrkontrolle nach Nr. 2.

In Anlage 3 Nr. 2 AFGBV werden die Anforderungen an das Betriebshandbuch spezifiziert. Ziel ist es „den sicheren Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten". Dafür „soll das Betriebshandbuch die Bedienung, Wartung, Gesamtprüfung, Diagnose des Kraftfahrzeuges und die dem Datenschutz und der Datensicherheit dienenden Parameter detailliert darstellen." Das Betriebshandbuch muss dabei mindestens die folgenden Punkte enthalten:

- ein Rollen-Rechte-Pflichten-Konzept für die zum Betrieb nötigen Tätigkeiten;
- Definition der erforderlichen Kompetenzen zur Ausübung der zum Betrieb nötigen Tätigkeiten;
- Umfang, Ablauf, Zeitpunkte und Intervalle von Wartungsmaßnahmen;
- Sicherheitshinweise iSd Beachtung von Grenzwerten für die technischen Funktionen;
- Entstörungs- oder Sicherheitsmaßnahmen, die im Falle einer Störung des Betriebes zu ergreifen sind;
- Dokumente für Wartungs- und Reparaturmaßnahmen inklusive der nötigen Vorlagen und
- eine Darstellung der dem Datenschutz und der Datensicherheit dienenden Funktionalitäten.

b) Anforderungen an die Sicherheit im Bereich der Informationstechnologie

Die Datenspeicherung und die Datenübermittlung sollen den Anforderungen an die Sicherheit im Bereich der Informationstechnologie genügen. Insbesondere müssen die Daten gemäß dem Stand der Technik vor Manipulation und missbräuchlicher Verwendung geschützt werden (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung). Die dafür notwendigen Anforderungen an die Sicherheit der Informationstechnologie sind sodann in Anlage 1 Teil 5 AFGBV beschrieben. Im Vergleich zum ersten Entwurf der AFGBV[45] ist in der verabschiedeten Version dieser Teil erheblich gekürzt worden. In Anlage 1 Teil 5 AFGBV ist vorgesehen, dass die vom Hersteller zu erfüllenden Anforderungen im Bereich der Informationstechnologie den Anforderungen der jeweils geltenden Fassung von UNECE-Regelung 155 zu entnehmen sind. Die Anforderungen der Ziffern 1., 3., 4. und 5.3.1. bis 5.3.5. der UNECE-Regelung 155 sollen dabei indes entfallen. Das zu erstellende Sicherheitskonzept muss den Vorgaben der Art. 24, 25, 32 DS-GVO entsprechen und eine Datenschutzfolgeabschätzung nach Art. 35 DS-GVO enthalten. Sämtliche weitere Anforderungen, die in der vorherigen Version enthalten waren und als Konkretisierung zu § 1f Abs. 3 Nr. 1–6 StVG gesehen werden konnten, sind in der beschlossenen Fassung nicht mehr enthalten.

Anforderungen, die die Hersteller in diesem Zusammenhang erfüllen müssen, sind jedoch weiterhin in § 1f Abs. 3 StVG zu finden. Diese geben vor, dass über den gesamten Entwicklungs- und Betriebszeitraum das Kraftfahrzeug mit autonomer Fahrfunktion vor Angriffen auf die elektronische und elektrische (E/E) Architektur des Kraftfahrzeuges sowie auf die mit dem Kraftfahrzeug in Verbindung stehende E/E Architektur abgesichert werden muss und dies auch gegenüber dem KBA und weiteren zuständigen Behörden nachzuweisen ist. Dass die mit dem Kraftfahrzeug in Verbindung stehende (E/E) Architektur mit abgesichert sein muss, kann eigentlich nur bedeuten, dass die Hersteller externe Cyberangriffe auf ihre Kraftfahrzeuge, welche über andere, mit dem Kraftfahrzeug in Verbindung stehende Entitäten durchgeführt werden, erkennen müssen bzw. unverzüglich nach Bekanntwerden einen solchen Angriff gem. § 1f Abs. 3 Nr. 6 StVG dem KBA und den im Gesetz genannten zuständigen Behörden melden und notwendige Maßnahmen einleiten müssen. In der früheren Version der AFGBV war hier zudem konkret die Absicherung vor Angriffen in Verbindung mit Software-Updates mit eingeschlossen,[46] wodurch auch indirekt UNECE-Regelung 156 im Kontext der Neuregelungen relevant geworden wäre. Die verabschiedete Verordnung enthält diesen wichtigen Zusatz nicht mehr. Dennoch wird es schwerlich möglich sein, die Vorgaben der UNECE-Regelung 156 bezüglich Software-Updates im Kontext von Kraftfahrzeugen mit autonomen Fahrfunktionen und deren Cybersicherheit auszuklammern. Die maßgeblichen Anforderungen an die Hersteller im Bereich der Cybersicherheit werden u.a. in der UNECE-Regelung 155 und der UNECE-Regelung 156 festgelegt und sind daher beide Untersuchungsgegenstand des Beitrags.

Um diesen Anforderungen zu entsprechen, ist seitens der Hersteller dem KBA und den zuständigen Behörden die Existenz und Nutzung eines Cyber Security Management-Systems (CSMS) nachzuweisen. Das CSMS soll Cybersicherheitsrisiken identifizieren, evaluieren und entschärfen. Die dort identifizierten Risiken und das entsprechende CSMS dürfen nicht die Sicherheit der Kraftfahrzeuginsassen oder anderer am Verkehr beteiligter Personen und insbesondere deren Leib oder Leben beeinträchtigen. Mit Bezug auf vom Kraftfahrzeug übermittelte oder empfangene Daten sollen die Schutzziele laut AFGBV mindestens die Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit, Authentizität und Verantwortlichkeit (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA09: Verfügbarkeit, TA11: Nachweisbarkeit, TA03: Authentische Datenverarbeitung) umfassen.[47]

Unter IT-Sicherheit können auch die im Datenschutzrecht vorgegebenen Schutzziele zu Datensicherheit verstanden werden, weil Datensicherheit ein Mittel der Gewährleistung von Datenschutz ist. Insbesondere Art. 32 DS-GVO ist hier einschlägig. Danach müssen die Verantwortlichen (hier: die Hersteller) geeignete technische und organisatorische Maßnahmen treffen, um Risiken im Kontext der Datenverarbeitung ein angemessenes Schutzniveau gegenüberzustellen. Dieser risikobasierte Ansatz der DS-GVO steht in einem engen Zusammenhang zur IT-Sicherheit.[48]

Darüber hinaus etabliert die DS-GVO verschiedene Gewährleistungsziele, welche sich auf die Schutzziele der Informationssi-

45 Entwurf einer VO zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Notifizierungsnummer: 2021/344/D, Bearbeitungsstand 10.6.2021, abrufbar unter: https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2021&num=344.

46 Entwurf einer VO zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Notifizierungsnummer: 2021/344/D, Bearbeitungsstand 10.6.2021, Anlage 1 Teil 5 Nr. 14.

47 S. hinsichtlich Integrität, Authentizität und Verfügbarkeit AFGBV Anlage I Teil 1 Nr. 6 und bezüglich Vertraulichkeit, Nachweisbarkeit und Verantwortlichkeit verweist die AFGBV auf die entsprechenden Art. 24, 25, 32 DS-GVO sowie auf die Vorgaben aus der UNECE-Regelung 155.

48 Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht/Conrad, 3. Aufl. 2019, § 33 Rn. 180.

cherheit beziehen.[49] Informationssicherheit umfasst dabei technische wie auch nicht-technische Systeme und orientiert sich in der Praxis im Rahmen des IT-Sicherheitsmanagements an ISO/IEC Normen und dem IT-Grundschutz, wodurch die Überschneidung hinsichtlich der Gewährleistungsziele der DS-GVO und der Schutzziele der Informationssicherheit kenntlich wird.

Zu diesen Zielen zählen die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.[50] Diese Schutzziele finden sich direkt[51] (TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA09: Verfügbarkeit) oder indirekt[52] (TA04: Datenisolation, TA01: Vertrauliche Datenverarbeitung, TA08: De-Identifikation, TA06: Transparenz, TA05: Interventionsfähigkeit) auch in der AFGBV und müssen demzufolge bei allen Kraftfahrzeugen mit autonomen Fahrfunktionen und deren elektronischer und elektrischer Architektur beachtet werden. Im Zusammenhang mit dem Datenschutzrecht sind diese in zentralen Normen der DS-GVO, zB in Artikel 5, zu finden. Dieser regelt zB die Transparenz für Betroffene von Verarbeitungen personenbezogener Daten (Art. 5 Abs. 1 lit. a DS-GVO) (TA06: Transparenz), Zweckbindung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. b DS-GVO) (TA04: Datenisolation), Datenminimierung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. c DS-GVO), Richtigkeit personenbezogener Daten (Art. 5 Abs. 1 lit. d DS-GVO), Speicherbegrenzung personenbezogener Daten (Art. 5 Abs. 1 lit. e DS-GVO) (TA07: Sicheres Löschen), Integrität personenbezogener Daten (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. b DS-GVO) (TA02: Integritätsgeschützte Datenverarbeitung) und die Vertraulichkeit personenbezogener Daten (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. b DS-GVO) (TA01: Vertrauliche Datenverarbeitung). Auch Art. 25, 32 DS-GVO regeln zentrale Aspekte mit Bezug zur Datensicherheit. Dazu zählen Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DS-GVO) (TA05: Interventionsfähigkeit), Verfügbarkeit der Systeme, Dienste und Daten (Art. 32 Abs. 1 lit. b und lit. c DS-GVO) (TA09: Verfügbarkeit), Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO) (TA10: Resilienz), Wiederherstellbarkeit der Daten und des Datenzugriffs (Art. 32 Abs. 1 lit. c DS-GVO) (TA10: Resilienz) und die Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO).[53]

Für die Datenspeicherung, insbesondere aber die Anforderungen an die Sicherheit im Bereich der Informationstechnologie, spielt die Integrität aus technischer und rechtlicher Sicht eine wesentliche Rolle. Integrität eines Systems bedeutet in diesem Zusammenhang, dass Daten und Informationen sicher und nachweislich nicht verändert worden sind. Integrität stellt demnach die nachvollziehbare Unversehrtheit und Korrektheit von elektronischen Daten dar.[54] Da Integrität eines der drei Hauptziele von Datensicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) darstellt, sind im Bereich von Kraftfahrzeugen mit autonomen Fahrfunktionen die Datensicherheitsmaßnahmen nach der DS-GVO von Bedeutung.

Im Gegensatz zu den Neuregelungen im StVG, welche sich hauptsächlich auf die Datenverarbeitung im Kraftfahrzeug beschränken, ist in Teil 1 Nr. 6 der Anlage 1 AFGBV für Kraftfahrzeuge mit autonomer Fahrfunktion auch die Übertragung von Daten an das Kraftfahrzeug erwähnt. Eine Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Kraftfahrzeugen oder mit Infrastruktureinrichtungen soll zulässig sein[55] und ist für deren Funktion essentiell. Demnach sollen die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (zB Backends oder Servern eines Anbieters, externe Sensoren, Smartphone oder zukünftig auch Anordnungen nach Straßenverkehrsrecht (wie etwa ein Stopp-Schild oder Anordnungen einer Lichtzeichenanlage) vom Kraftfahrzeug sicher empfangen und verwendet (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA08: De-Identifikation) werden können.[56] Eine solche Übertragung soll dem aktuellen Stand der Technik entsprechen und die Vorgaben der DS-GVO (insbesondere der Art. 24, 25, 32, 35 DS-GVO) erfüllen. Es sollen über eine Bedrohungsanalyse Risiken identifiziert werden und ein Absicherungskonzept mit wirksamen Maßnahmen eingeführt werden.[57] Weiter soll für die Datenübertragung eine zentrale sichere, elektronische Steuereinheit (SECU) genutzt werden. Diese dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluss (OBD II) oder an eine proprietäre Schnittstelle des Herstellers. Die Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind dabei ebenfalls in dem bereits o.g. Teil 5 der AFGBV zu finden. Hierzu zählt die Sicherstellung u.a. der Integrität, Authentizität und Verfügbarkeit der Datenübertragung (TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA09: Verfügbarkeit).

Maßnahmen zur Gewährleistung der Datensicherheit werden in den Art. 24, 25, 32 DS-GVO normiert. In Art. 24 DS-GVO wird neben der generellen Verpflichtung zum Schutz personenbezogener Daten auch die Gewährleistung der Datensicherheit, also die Durchführung technisch-organisatorischer Maßnahmen zum Schutz verarbeiteter personenbezogener Daten, festgeschrieben.[58] Art. 24 DS-GVO zur Verantwortung des für die Verarbeitung Verantwortlichen wird durch Art. 25 DS-GVO zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und Art. 32 DS-GVO zur Sicherheit der Verarbeitung personenbezogener Daten konkretisiert, indem Art. 25 DS-GVO dem Verantwortlichen spezifische Pflichten bezüglich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen vorgibt. Überdies regelt Art. 32 DS-GVO als nähere Konkretisierung des allgemeinen Grundsatzes der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO) die Pflicht, ein angemessenes Schutzniveau für die Sicherheit personenbezogener Daten (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung) zu gewährleisten.[59] Als notwendige Maßnahmen werden in Art. 32 DS-GVO u.a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DS-GVO) benannt (TA08: De-Identifikation, TA01: Vertrauliche Datenverarbeitung). Hinzu kommt die Notwendigkeit, die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen (Art. 32 Abs. 1 lit. b (TA01: Vertrauliche Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung, TA09: Verfügbarkeit) sowie die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder

49 Vgl. Standard-Datenschutzmodell, Version 2.0a, S. 9 f., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf.
50 Vgl. Standard-Datenschutzmodell, Version 2.0a, S. 9 f., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf.
51 AFGBV Anlage 1 Teil 1 Nr. 6 listet Integrität, Authentizität und Verfügbarkeit auf.
52 AFGBV Anlage 1 Teil 5 Nr. 15.
53 Vgl. Standard-Datenschutzmodell, Version 2.0a, S. 13 f., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf.
54 Auer-Reinsdorff/Conrad, HdB IT- und Datenschutzrecht/Conrad/Eckhardt, 3. Aufl. 2019, § 33 Rn. 9.
55 AFGBV Anlage 1 Teil 1 Nr. 6.
56 AFGBV Anlage 1 Teil 1 Nr. 6.
57 AFGBV Anlage 1 Teil 1 Nr. 6.
58 Kühling/Buchner, DS-GVO – BDSG/Hartung, 2. Aufl. 2018, DS-GVO Art. 24 Rn. 11.
59 Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 2.

technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DS-GVO) (TA09: Verfügbarkeit, TA10: Resilienz). Gefordert ist zudem ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO).

Die von den Herstellern entwickelten Systeme müssen demzufolge insbesondere die genannten Vorgaben erfüllen und dies muss nachweislich und dauerhaft bescheinigt werden, um eine Genehmigung für ein Kraftfahrzeug mit autonomen Fahrfunktionen zu erhalten. Kraftfahrzeuge müssen zwingend vor Hackerangriffen geschützt werden. Dabei ist ein Zusammenspiel von technischen Standards und rechtlichen Vorgaben notwendig. Nur eine holistische Kraftfahrzeugarchitektur kann Betriebssicherheit (safety) und Informationssicherheit (security) bei gleichzeitiger Berücksichtigung der datenschutzrechtlichen Vorgaben gewährleisten. Dazu gehört auch eine Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO vor der kommerziellen Einführung hiervon erfasster Datenverarbeitungen.

Da in der AFGBV u.a. direkt Bezug auf die UNECE-Regelung 155 genommen wird,[60] werden im Folgenden einschlägige UNECE-Regelungen näher betrachtet.

2. UNECE-Regelungen

Auf der internationalen Ebene werden wichtige Rechtsinstrumente im Bereich des Kraftfahrzeugverkehrs durch die Wirtschaftskommission der Vereinten Nationen für Europa (United Nations Economic Commission for Europe – UNECE) und dort die Working Party on Road Traffic Safety, welche 2017 in Global Forum for Road Traffic Safety -WP.1[61] (nachfolgend WP.1) umbenannt wurde, weiterentwickelt und interpretiert. Diese Arbeitsgruppen sind zwar nicht direkt zuständig auch datenschutzrechtliche Vorgaben zu definieren, allerdings werden dort Regelungen erarbeitet, welche Auswirkungen darauf haben, dass Daten im Kraftfahrzeug verarbeitet werden.[62] In den Arbeitsgruppen werden technische Regeln (nachfolgend UNECE-Regeln) erarbeitet, welche sich am Stand der Technik orientieren und genaue Maßgaben zu Bauteilen oder Kraftfahrzeugfunktionen enthalten.[63] Dazu zählen etwa Regelungen zur Lenkung (UNECE-Regelung 79) und die Überarbeitung von UNECE-Regelung 79,[64] die UNECE-Regelung 157 (Automated Lane Keeping Systems – ALKS) oder die UNECE-Regelung 13-H zu automatisierten Bremsen).

Neben der o.g. WP.1 ist für die Entwicklung im Bereich automatisierter Kraftfahrzeuge auch das World Forum for Harmonization of Vehicle Regulations – WP.29 (nachfolgend WP.29) zu nennen, wo seit 2018 die Unterarbeitsgruppe für Automated and Connected Driving (GRVA – Groupe Responsive Voiture Automatique) für automatisiertes und vernetztes Fahren verantwortlich ist.[65] Hier werden einerseits im Kontext des automatisierten Fahrens datenschutzrechtlich relevante Vorgaben erarbeitet, wie solche zum sog. „Fahrmodusspeicher", dem Data Storage System for Automated Driving (DSSAD) und zum Unfalldatenspeicher (Event Data Recorder – EDR).[66] Andererseits zählen zu den Schwerpunkten der GRVA im Rahmen von safety und security auch funktionale Anforderungen an Cybersecurity, Software-Updates oder auch Validierungsmethoden.[67] Zu Cybersecurity und Software-Updates wurden die UNECE-Regelungen 155[68] (Cybersicherheit) und 156[69] (Software-Updates) veröffentlicht. Die AFGBV schreibt in diesem Zusammenhang vor, dass „[d]ie vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie ... den Anforderungen der ... UN-Regelung Nr. 155" zu entnehmen sind.[70] Das Sicherheitskonzept muss den Vorgaben der Art. 24, 25, 32 DS-GVO entsprechen.[71] Hier wird durch die Verordnung explizit die UNECE-Regelung 155 zur Voraussetzung erklärt. Neben der völkerrechtlichen Bindung an die UNECE-Regelungen durch das Genfer Fahrzeugteileübereinkommen,[72] dessen Vertragsstaat Deutschland ist, hat zudem die Europäische Union als supranationales Mitglied die UNECE-Regelungen für die Mitgliedstaaten mit Verpflichtungswirkung ratifiziert. Aus Sicht der Kraftfahrzeughersteller ist weiterhin insbesondere von Bedeutung, dass die Anforderungen der relevanten UNECE-Regelungen im EU-Typengenehmigungsverfahren als Voraussetzung gelten.[73]

Untergesetzliche und gesetzliche Regelungen zur Cybersicherheit werden in Zukunft eine wichtige Rolle in der Fahrzeugautomatisierung spielen. Durch die feste Einbettung der UNECE- Regelungen in die AFGBV und über den Verweis auf diese Regelungen in der EG-Typenzulassung werden Kraftfahrzeughersteller die dort geforderten Anforderungen an die Cybersicherheit im Rahmen der Genehmigungsverfahrens vorweisen müssen.[74] Daher sollen im Folgenden insbesondere die UNECE-Regelung 155 und 156 thematisiert werden. Die Maßnahmen der UNECE-Regelung 155 werden hier nur beispielhaft aufgeführt. Daher werden nur Anforderungen aus den allgemeinen Gewährleistungszielen abgeleitet. Ein detaillierter Abgleich aller Maßnahmen der UNECE-Regelung 155 mit unseren Anforderungen wird dann in Abschnitt V. 3. durchgeführt.

a) UNECE-Regelung 155

Nachdem die von der WP.29 erarbeiteten Regelungen 2021 im Amtsblatt der Europäischen Union veröffentlicht wurden,[75] bestehen erstmalig auf europäischer Ebene einheitliche und verbindliche Regelungen bezüglich Cybersecurity und Software-Updates für den Automobilsektor. Der Kern der UNECE-Regelung 155 besteht in der Verpflichtung zur Einführung eines Cyber Sicherheitsmanagement-Systems (CSMS). Nach Ziffer 2.3. der Regelung bezeichnet ein CSMS einen „systematischen, risikobasierten Ansatz zur Festlegung von organisatorischen Abläufen, Zuständigkeiten und Governance beim Umgang mit Risiken im Zusammenhang mit Cyberbedrohungen für Fahrzeuge und beim Schutz von Fahrzeugen vor Cyberangriffen."[76] Gemäß Ziffer 5. ist ein solches CSMS fortan als Voraussetzung für die Genehmigung eines Kraftfahrzeugtyps anzusehen. Kraftfahrzeughersteller haben daher gemäß Ziffer 5.1.1. rele-

60 AFGBV Anlage 1 Teil 5 Nr. 15.
61 Vgl. www.unece.org/trans/main/welcwp1.html.
62 Wagner, Das neue Mobilitätsrecht, 2021, S. 136.
63 Wagner, Das neue Mobilitätsrecht, 2021, S. 35.
64 Lutz DAR 2021, 182 f.; Will NZV 2020, 163 (166 f.).
65 Vgl. https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction.
66 Wagner, Das neue Mobilitätsrecht, 2021, S. 130 ff.
67 Die Arbeiten und aktuellen Arbeitsstände der Informal Working Groups unter GRVA können online eingesehen werden: https://wiki.unece.org/pages/viewpage.action?pageId=63310525; zum Verfahren: Will NZV 2020, 163 (166).
68 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system E/ECE/TRANS/505/Rev.3/Add.154.
69 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system ECE/TRANS/WP.29/2020/80.
70 AFGBV Anlage 1 Teil 5 Nr. 15.
71 AFGBV Anlage 1 Teil 5 Nr. 15.
72 Genfer Übereinkommen der Wirtschaftskommission für Europa der Vereinten Nationen v. 20.3.1958 über die Annahme harmonisierter technischer Regelungen der Vereinten Nationen für Radfahrzeuge, Ausrüstungsgegenstände und Teile, die in Radfahrzeuge(n) eingebaut und/oder verwendet werden können, und die Bedingungen für die gegenseitige Anerkennung von Genehmigungen, die nach diesen Regelungen der Vereinten Nationen erteilt wurden – Revision 3, ABl. EU L 274/4 v. 11.10.2016.
73 Will NZV 2020, 163 (165 f.).
74 Wagner, Das neue Mobilitätsrecht, 2021, S. 186.
75 Abl. EU L 082 v. 9.3.2021, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2021:082:FULL&from=DE.
76 UNECE-Regelung 155, Ziff. 2.3.

vante Maßnahmen zu treffen, welche Folgendes gewährleisten sollen:

- Erfassung und Überprüfung der gemäß dieser Regelung erforderlichen Informationen über die gesamte Lieferkette hinweg, um nachzuweisen, dass lieferantenbezogene Risiken ermittelt und bewältigt werden;
- Dokumentation der Risikobewertung (während der Entwicklungsphase oder nachträglich), der Testergebnisse und der Minderungsmaßnahmen bezogen auf den Fahrzeugtyp, einschließlich konstruktionsbezogener Informationen zur Untermauerung der Risikobewertung;
- Implementierung geeigneter Cybersicherheitsmaßnahmen bei der Konzeption des Fahrzeugtyps;
- Erkennung von und Reaktion auf mögliche Cyberangriffe (TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA05: Interventionsfähigkeit, TA11: Nachweisbarkeit) und
- Protokollierung von Daten zur Unterstützung der Erkennung von Cyberangriffen und Bereitstellung von Datenforensik, um eine Analyse versuchter oder erfolgreicher Cyberangriffe zu ermöglichen (TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung, TA05: Interventionsfähigkeit, TA09: Verfügbarkeit, TA10: Resilienz, TA11: Nachweisbarkeit).

Durch die Pflicht, auch die gesamte Lieferkette nachweislich zu kontrollieren, sind Zuliefererfirmen, welche Teile mit cybersicherheitsrelevanten Komponenten produzieren, mittelbar ebenfalls dieser Regelung unterworfen. Das bedeutet konsequenterweise auch, dass das Gesamtsystem des Kraftfahrzeugs zur Einhaltung aller Schutzziele ebenfalls Cloud-Services mitberücksichtigen muss.

Die Anforderungen an das CSMS sind in Ziffer 7.2. UNECE-Regelung 155 beschrieben. Dazu zählen u.a. der kraftfahrzeugherstellerseitige Nachweis gegenüber den Genehmigungsbehörden, dass das CSMS in der Entwicklungs-, Produktions- und Postproduktionsphase anwendbar ist.[77] Nachzuweisen sind nach den Ziffern 7.2.2.2. ff. insbesondere die Verfahren, welche für eine angemessene Sicherheit sorgen sollen. Dazu zählen zB „Verfahren, die innerhalb der Organisation des Herstellers für das Cybersicherheitsmanagement eingesetzt werden"; „Verfahren zum Testen der Cybersicherheit eines Fahrzeugtyps" und „Verfahren zur Überwachung und Erkennung von Cyberangriffen, Cyberbedrohungen und Schwachstellen von Fahrzeugtypen sowie zur Reaktion darauf, und die Verfahren, mit denen bewertet wird, ob die implementierten Cybersicherheitsmaßnahmen angesichts neu ermittelter Cyberbedrohungen und Schwachstellen noch wirksam sind".[78] Für den hier behandelten Kontext ist darüber hinaus Ziffer 7.2.2.4. nennenswert, nach welcher der Kraftfahrzeughersteller nachweisen muss, dass die in Ziffer 7.2.2.2. lit. g vorgesehene Überwachung ununterbrochen erfolgt, wobei gem. Ziffer 7.2.2.4. lit. a Kraftfahrzeuge auch nach der Erstzulassung in die Überwachung einbezogen werden müssen sowie nach lit. b die Fähigkeit, Cyberbedrohungen, Schwachstellen und Cyberangriffe anhand von Kraftfahrzeugdaten und Fahrzeugprotokollen zu analysieren und zu erkennen. Hieraus ergeben sich Anforderungen an den Schutz personenbezogener Daten iSd Datenschutzrechts.

Mit Blick auf Ziffer 1.3. UNECE-Regelung 155 ist hervorzuheben, dass die gesamte Regelung „auch unbeschadet der Anwendung nationaler und regionaler Rechtsvorschriften zum Schutz der Privatsphäre und zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten", gilt. Das CSMS müssen sich die Kraftfahrzeughersteller zertifizieren lassen. Dieses Zertifikat soll maximal drei Jahre gültig sein und einmal im Jahr müssen die Hersteller den Genehmigungsbehörden über ihr Monitoring und über detektierte Cyberangriffe Auskunft geben.[79] Sollen Modifikationen vorgenommen werden, welche auch Sicherheitsmechanismen betreffen, ist dies ebenfalls zu melden. Bei Nonkonformität mit den Vorgaben aus der UNECE-Regelung soll als Sanktionsmittel die Konformitätsbescheinigung für das CSMS zurückgenommen werden (Ziffer 6.8.), was zur Rücknahme der Typengenehmigung hinsichtlich der Cybersicherheit führt.[80] Anstelle detaillierter technischer Vorschriften an das Endprodukt, soll so der Entwicklungsprozess der Hersteller sowie die Produktbeobachtung über den gesamten Produktionszyklus geregelt werden.[81] Ziel ist, damit einerseits ein hohes Sicherheitsniveau und andererseits die nötige Flexibilität in einem sich schnell weiterentwickelnden Feld zu wahren, um nicht langfristig an bereits überholte Sicherheitsstandards gebunden zu sein.[82]

Bezüglich Datenschutz und Cybersicherheit kann auch hier ein gewisses Spannungsverhältnis erkannt werden. Während das Datenschutzrecht sehr detailliert normativ geregelt ist, existieren hinsichtlich Cybersicherheit kaum gesetzliche Vorgaben, dafür aber diverse Industriestandards. Ähnlich verhält es sich hier mit der UNECE-Regelung 155, welche Cyberangriffe zwar als Bedrohung für personenbezogene Daten erkennt, allerdings keine konkret einzuhaltenden Anforderungen bezüglich des Datenschutzes benennt. Lediglich in Ziffer 1.3. heißt es, dass die Privatsphäre und der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten gewahrt werden muss. Eine positive Entwicklung ist dabei der erkennbare Versuch einer Synthese von Datenschutz und Cybersicherheit, welcher dem Anhang zu der UNECE-Regelung entnommen werden kann. Dort werden Schwachstellen oder Angriffsmethoden, bezogen auf verschiedene Bedrohungen, identifiziert und Minderungsmaßnahmen für dieselben erörtert. Zudem werden speziell Bedrohungen für personenbezogene Daten miterfasst. So werden zB in Anhang 5, Tabelle 1A, Ziffer 4.3.6. Bedrohungen für Fahrzeugdaten/-code genannt und als Schwachstelle im Zusammenhang mit unbefugtem Zugriff auf personenbezogene Daten des Eigentümers genannt. Unter Ziffer 7.2. in Tabelle B1 zu Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Fahrzeugkommunikationskanälen wird etwa mit Blick auf das Erlangen von unbefugtem Zugriff auf Dateien oder Daten vorgegeben, dass das Systemdesign und die Zugangskontrolle so ausgelegt sein müssen, dass Unbefugte nicht auf personenbezogene oder systemkritische Daten zugreifen können.

Beispiele für Sicherheitsmaßnahmen für Backend-Systeme bietet das Open Web Application Security Project[83] (OWASP). Die Regelungen in Tabelle B5, Ziffer 19.2. oder auch in Tabelle B7, Ziffer 31.1. sind dahingehend vergleichbar, dass bei der Speicherung personenbezogener Daten bewährte Verfahren zum Schutz der Datenintegrität und -vertraulichkeit zu befolgen sind. In Tabelle C3, Ziffer 30.1. wird die Aussage aus Tabelle B7, Ziffer 31.1., noch um den Zusatz ergänzt, dass Beispiele für Sicherheitsmaßnahmen in ISO/SC27/WG5 zu finden sind. Fraglich ist jedoch die Verbindlichkeit dieser „Minderungsmaßnahmen", insbesondere wenn es heißt, dass lediglich Beispiele dafür in ISO-Normen zu finden sind, welche ebenfalls keine rechtliche Bindungswirkung besitzen. Die Tabellen in den Anhängen können auch nicht als abschließend angesehen werden, was der

77 UNECE-Regelung 155, Ziff. 7.2.2.1.
78 Vgl. UNECE-Regelung 155, Ziff. 7.2.2.2. bis 7.2.2.5.
79 UNECE-Regelung 155, Ziff. 6.7. und 7.4.1.
80 Vgl. UNECE-Regelung 155, Ziff. 6.11. und 10.1.
81 Wagner, Das neue Mobilitätsrecht, 2021, S. 187 f.
82 Wagner, Das neue Mobilitätsrecht, 2021., S. 188; zur Kritik am aktuellen Entwurf: NPM – Nationale Plattform Zukunft der Mobilität, Handlungsempfehlungen zur Typengenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, Whitepaper 2020, S. 21 ff.
83 Vgl. https://wiki.owasp.org/?title=Special:Redirect/file/OWASP_Top_10-2017_de_V1.0.pdf

sonstigen flexiblen Ausgestaltung der Regelung auch zuwiderlaufen würde.

Zusammenfassend kann festgehalten werden, dass für eine EG-Typengenehmigung heute UNECE-Regelungen die entscheidenden materiellen Vorgaben für die Erteilung einer solchen Genehmigung enthalten.[84] Art. 57 Abs. 1 VO (EU) 2018/858[85] gibt vor, dass UN-Regelungen oder deren Änderungen, denen die Union zugestimmt hat oder die sie anwendet und die in Anhang II VO (EU) 2018/858 aufgeführt sind, Bestandteil der Anforderungen für die EU-Typgenehmigung für Kraftfahrzeuge, Systeme, Bauteile und selbstständige technische Einheiten sind. Damit werden auch künftig die Vorgaben zu Cybersicherheit aus der UNECE-Regelung 155 zumindest insofern zu beachten sein, wie eine EU-Typengenehmigung erteilt werden soll.

b) UNECE-Regelung 156

Die UNECE-Regelung 156 soll im Kern die Vorgaben an ein Softwareaktualisierungsmanagementsystem (Software Update Management System – SUMS) festlegen. Damit soll die Software im Kraftfahrzeug vor Manipulationen geschützt (TA02: Integritätsgeschützte Datenverarbeitung) und zudem die Cybersicherheit gewährleistet werden. Die beiden UNECE-Regelungen (155 und 156) können daher als eng miteinander verknüpft angesehen werden. Das SUMS ist in UNECE-Regelung 156 unter Ziffer 2.5. definiert als „systematische[r] Ansatz zur Festlegung organisatorischer Verfahren und Vorgänge, um den Anforderungen an die Bereitstellung von Softwareaktualisierungen gemäß dieser Regelung zu entsprechen." Die Hersteller sollen somit in die Lage versetzt werden, Sicherheitslücken oder Schwachstellen zu erkennen und diese auch aus der Ferne wirksam beheben zu können.[86] Weiterhin soll damit auch für Fahrer, Halter und zuständige Behörden deutlich werden, welche Auswirkungen Software-Updates auf die Typengenehmigungsparameter haben, um die Genehmigung und die Einhaltung von Governance-Richtlinien nachvollziehbar zu gewährleisten.[87]

Die allgemeinen Anforderungen an das SUMS, welche durch die Hersteller erfüllt werden müssen, sind unter den Ziffern 7.1. bis 7.1.4.2. der Regelung zu finden. Die Vorschriften für den Kraftfahrzeugtyp und die Softwareaktualisierungen sind in den Ziffern 7.2. bis 7.2.2.5. festgelegt. Zu den Anforderungen an das SUMS gehört zB gemäß Ziffer 7.1.1.1. Verfahren zu entwickeln, bei denen die für diese Regelung relevanten Informationen dokumentiert und beim Kraftfahrzeughersteller geschützt aufbewahrt werden und einer Genehmigungsbehörde oder einem technischen Dienst auf Anfrage zur Verfügung gestellt werden können. Nach Ziffer 7.1.1.2. muss ein Verfahren eingeführt werden, bei dem Informationen hinsichtlich aller ursprünglichen und aktualisierten Softwareversionen, einschließlich Validierungsdaten für die Integrität und einschlägige Hardwarekomponenten eines typgenehmigten Systems, eindeutig identifiziert werden können. Ziffer 7.1.1.6. regelt zudem, dass ein Verfahren zu etablieren ist, welches dem Kraftfahrzeughersteller ermöglicht, Zielfahrzeuge für eine Softwareaktualisierung zu identifizieren.

Vorschriften für Softwareaktualisierungen umfassen u.a. gemäß Ziffer 7.2.1.1., dass die Authentizität und Integrität von Softwareaktualisierungen so zu schützen sind, dass sowohl ihre Beeinträchtigung als auch eine ungültige Aktualisierung nach vernünftigem Ermessen ausgeschlossen sind, die Updates also nur erfolgen, wenn sie die Fahrt nicht beeinträchtigen und sicher abgeschlossen werden können (TA03: Authentische Datenverarbeitung, TA02: Integritätsgeschützte Datenverarbeitung). Hinsichtlich sog. Software-over-the-air-Updates (SOTA) muss der Kraftfahrzeughersteller nach Ziffer 7.2.2.1.1. sicherstellen, dass das Kraftfahrzeug im Falle einer fehlgeschlagenen oder abgebrochenen Aktualisierung in der Lage ist, die Vorversion des Systems wiederherzustellen bzw. das Kraftfahrzeug in einen sicheren Zustand zu versetzen (TA10: Resilienz). Dieser „sichere Zustand" ist nicht gleichzusetzen mit dem im deutschen Recht (§ 1d Abs. 4 StVG) beschriebenen „risikominimalen Zustand".[88] Eine Aktualisierung darf gemäß Ziffer 7.2.2.1.2. nur erfolgen, wenn das Kraftfahrzeug über genügend Energie (iSv Batteriekapazität) für sowohl das Software-Update als auch das etwaige Zurücksetzen auf den vorherigen Softwarestand und das Versetzen in den sicheren Zustand, verfügt (TA02: Integritätsgeschützte Datenverarbeitung, TA03: Authentische Datenverarbeitung). Die Vorgaben an die Sicherheit von SOTA-Updates, welche herstellerseitig erfüllt werden müssen, sind insbesondere in den Ziffern 7.2.2.1.3. bis 7.2.2.5. zu finden. Dort werden vorwiegend Organisationsprozesse, Dokumentationspflichten sowie Zertifizierungsprozesse festgelegt und Anforderungen an einen sicheren Softwareupdateprozess (inklusive SOTA-Updates) definiert. Diese Anforderungen werden die Hersteller vor deutliche Herausforderungen stellen.[89] Es müssen Systeme entwickelt werden, die sowohl die Kraftfahrzeugarchitektur, als auch mit dieser in Verbindung stehenden Cloud-Dienste mitberücksichtigen, da Änderungen in der Cloud-Struktur auch zunächst eingehaltene Schutzziele konterkarieren können. Ferner wird durch die Vorgabe des Zurücksetzens auf einen vorherigen Softwarestand ein technischer Pfad vorgegeben, in einer ansonsten eher dynamisch gestalteten Regelung. Technische Dienste und auch die Genehmigungsbehörden sollten bei Softwareänderungen und -updates miteinbezogen werden. Prüforganisationen sollte ein entsprechender Zugang über standardisierte Kommunikationsschnittstellen gewährleistet werden, damit diese im Rahmen ihres gesetzlichen Prüfauftrags regelmäßige Inspektionen durchführen können.[90]

Im Rahmen von Updates ist stets zu prüfen, ob diese relevant für die Typengenehmigung sein könnten. Bezüglich Software-Updates ist selbst bei Einhaltung aller Vorgaben in der UNECE-Regelung 156 damit zu klären, ob diese auch materiell-rechtlich zulässig sind und die Kraftfahrzeuge nach einem solchen Update weiterhin im öffentlichen Straßenverkehr bewegt werden dürfen.[91] Neben den eingangs skizzierten Vorgaben, die ein Kraftfahrzeughersteller mit Blick auf sein SUMS einhalten und implementieren muss,[92] benötigen diese auch eine Typengenehmigung für Software-Update-Prozesse der jeweiligen Kraftfahrzeugtypen (vgl. Ziffer 5.1.).

---

84 Will NZV 2020, 163 (166).

85 VO (EU) 2018/858 des Europäischen Parlaments und des Rates v. 30.5.18 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der VO (EG) Nr. 715/2007 und VO (EG) Nr. 595/2009 und zur Aufhebung der RL 2007/46/EG.

86 Vgl. Wuhrmann/Deeg/Hessel, Neue Cybersicherheits-und Softwareupdate-standards in der Automobilbranche, abrufbar unter: https://www.reuschlaw.de/fileadmin/user_upload/202103_Neue-Cybersicherheits-und-Softwareupdatestandards-in-der-Automobilbranche_DW-TD-StH.pdf.

87 Vector Consulting Services, UNECE CSMS und SUMS, abrufbar unter: https://consulting.vector.com/de/de/solutions/cybersecurity/unece-csms-and-sums/.

88 UNECE-Regelung 156 spricht in Ziff. 7.2.2.1.1. und 7.2.2.1.2. von „sicheren Zustand", wobei nach Ziff. 2.7. ein „Sicherer Zustand" einen Betriebsmodus ohne unverhältnismäßiges Risiko bei Ausfall eines Merkmals bezeichnet; zum „risikominimalen Zustand": Arzt/Ruth-Schumacher, Risikobewertung unterschiedlicher Umsetzungsszenarien des Überführens eines automatisch gesteuerten Fahrzeugs in den sog. „sicheren Zustand", abrufbar unter: www.hwr-berlin.de/fileadmin/portal/Dokumente/Prof-Seiten/Arzt/ARZT_Ruth-Schumacher_-_Rechtsfragen_%C3%9Cberf%C3%BChrung_in_risikominimalen_Zustand_2016.pdf; Arzt/Ruth-Schumacher RAW 2/2017, 89.

89 So auch Haupt NZV 2022, 166 (168), der die Auswirkungen der VO für alle, an Kraftfahrzeugen mit autonomen Fahrfunktionen beteiligten Akteure als erheblich einstuft.

90 NPM – Nationale Plattform Zukunft der Mobilität, Handlungsempfehlungen zur Typengenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, Whitepaper 2020, S. 19.

91 Geber NZV 2021, 14.

92 Vgl. auch gesamte Ziff. 7. UNECE-Regelung 156.

Die UNECE-Regelung 156 definiert in Ziffer 2.1. den Begriff des „Fahrzeugtyps" vom Gegenstand der Regelung her. Der Kraftfahrzeugtyp beschreibt nach dieser Regelung Kraftfahrzeuge als solche, die sich hinsichtlich der vom Hersteller angegebenen Bezeichnung des Kraftfahrzeugtyps und in wesentlichen Merkmalen der Konzeption des Kraftfahrzeugtyps in Bezug auf die Verfahren zu Softwareaktualisierung nicht unterscheiden. Eine solche auf den Gegenstand der Regelung bezogene Definition ist auch bereits aus anderen UNECE-Regelungen wie etwa in Nr. 79 (Lenksysteme) oder Nr. 83 (Schadstoffemissionen) bekannt. Diese Definition hat einen anderen Bezugspunkt für den Begriff des Kraftfahrzeugtyps als die allgemeinen Regelungen zur Typengenehmigung gem. Art. 3 Nr. 32 VO (EU) 2018/858.[93] Nach der VO (EU) 2018/858 setzt sich ein „Fahrzeugtyp" aus den Kraftfahrzeugen zusammen, die zumindest einen gemeinsamen Firmennamen eines Herstellers haben und in Konstruktion und Montage der wesentlichen Teile der Aufbaustruktur gleich sind. Der in UNECE-Regelung 156 gewählte Definitionsansatz lässt den Schluss zu, dass „ein Fahrzeughersteller die typgenehmigten Software-Update-Prozesse in mehreren Fahrzeugtypen iSd VO (EU) 2018/858 einsetzen können soll, ohne die Prozesse jeweils neu genehmigen zu lassen."[94]

Neben den o.g. technischen Anforderungen müssen Software-Updates, welche Änderungen des Kraftfahrzeugs bedingen, auch korrekt durch den Kraftfahrzeughersteller in den Genehmigungsunterlagen dargestellt werden.[95] Änderungen am Kraftfahrzeug (auch durch Software-Updates) können entweder für den betroffenen Kraftfahrzeugtyp oder für einzelne Kraftfahrzeuge vorgenommen werden. Soll der gesamte Kraftfahrzeugtyp durch Software-Updates geändert werden, richten sich die rechtlichen Anforderungen nach Art. 33 f. VO (EU) 2018/858. Danach müssen der Typengenehmigungsbehörde Änderung mit Emissions- oder Sicherheitsbezug angezeigt werden und diese Behörde entscheidet, ob dadurch eine Erweiterung oder Änderung (Revision) der Typengenehmigung erforderlich ist (Art. 33 Abs. 1 VO (EU) 2018/858) oder ob eine neue Typengenehmigung auf Grund weitreichender Änderungen beantragt werden muss (Art. 34 Abs. 1, 33 Abs. 5 VO (EU) 2018/858). Handelt es sich nur um geringfügige Datensatzanpassungen oder sog. Bugfixes mit lediglich beschränktem Sicherheits- oder Emissionsbezug, enthält jedenfalls der Wortlaut der VO (EU) 2018/858 trotzdem keine Ausnahme für solche Updates. Demgegenüber könnte aus teleologischer Sicht allerdings argumentiert werden, dass reine Funktionsverbesserungen nicht einen Genehmigungsprozess durchlaufen müssen und somit von der Notifizierungspflicht ausgenommen sind, da mit solchen Verbesserungen oder Fehlerbehebungen kein Risiko einhergeht.[96] Hier ist jedoch zu beachten, dass der Kraftfahrzeughersteller für diese Einschätzung der Geringfügigkeit bzw. lediglich Funktionsverbesserung das Prognoserisiko trägt.

Ausnahmen von der Notifizierungspflicht bestehen für Funktionen, die zwar bereits im Code vorhanden, aber noch deaktiviert sind. Hierzu finden sich auch Maßgaben in § 1h StVG, wonach Funktionen, welche in internationalen Standards noch nicht beschrieben sind, verbaut werden können, wenn diese deaktiviert sind und eine Einflussnahme dieser Fahrfunktionen auf die genehmigten Systeme ausgeschlossen ist. Wenn solche Funktionen später Gegenstand einer Typengenehmigung werden, sollen diese durch Software-Updates aktivierbar sein.[97] Eine für Kraftfahrzeughersteller weitere Möglichkeit zur Ausnahme von der Notifizierungspflicht besteht darin, die ggf. notifizierungspflichtigen Änderungen durch Software-Updates nicht im Rahmen von Anpassungen in der Typengenehmigung zu reflektieren. Damit würden allerdings alle Rechtsfragen auf Ebene der Einzelfahrzeuge und somit auf die nicht harmonisierten Rechtsordnungen der EU-Mitgliedstaaten verlagert.[98]

IV. Zwischenergebnis

Die im Juli 2021 neu in das StVG eingefügten Vorschriften sowie die ebenfalls für die Vertragsparteien verbindlich zu erfüllenden Vorgaben aus den UNECE-Regelungen und deren Aktualisierungen machen deutlich, dass der Bereich Cybersicherheit immer wichtiger für die Entwicklung von Kraftfahrzeugen wird. Dies führt zu einer zunehmenden Regulierung und der Notwendigkeit eines klaren rechtlichen Rahmens. Hochautomatisierte oder autonome Kraftfahrzeuge müssen vor Cyberattacken geschützt werden und es müssen Verteidigungsstrategien hiergegen implementiert werden. Um die zunehmende Digitalisierung von Kraftfahrzeugen sicher voranzutreiben, muss aus rechtlicher wie technischer Sicht ein ganzheitliches Verständnis von „Cybersicherheit by design" etabliert werden.

Rechtliche Fragen ergeben sich hierbei allerdings u.a. mit Blick auf die Bindung bzw. datenschutzrechtliche Beachtung konkreter Vorgaben im Rahmen eines CSMS. Dabei ist u.a. die materiell-rechtliche Zulässigkeit von Software-Änderungen durch Updates und deren Zulässigkeit und Auswirkungen auf die Typengenehmigung ein vertieft zu diskutierendes Problemfeld.

Die vorstehende Darstellung der rechtlichen Anforderungen, welche sich in den Neuregelungen zum StVG und den UNECE-Regelungen wie auch im Datenschutzrecht finden, eröffnet nachfolgend die Möglichkeit, diese Anforderungen mit dem Stand der Technik bzw. den technisch vorhandenen und möglichen Maßnahmen zu Datenschutz und Cybersicherheit abzugleichen.

V. Technischer Maßnahmenkatalog

Aus der rechtlichen Analyse können technische Anforderungen für Datenschutz und Cybersicherheit in der Fahrzeugautomatisierung abgeleitet werden, die dann in die zugehörigen Maßnahmen überführt werden. Diese sollen nachfolgend für die weitere Diskussion vorgestellt werden.

1. Abgeleitete Technische Anforderungen

In nachfolgender Tabelle werden zu den verschiedenen gesetzlichen Anforderungen von uns definierte Technische Anforderungen (TA) abgeleitet. Hierfür gleichen wir die Anforderungen mit allgemeinen Schutzzielen der IT-Sicherheit[99] ab. Bei dieser Vorgehensweise kann eine gesetzliche Anforderung nicht immer mit genau einer Technischen Anforderung abgebildet werden. Es ist auch möglich, dass sich mehrere rechtliche Anforderungen mit einer technischen abbilden lassen oder umgekehrt.

TA01 stellt die Vertraulichkeit der gespeicherten, verarbeiteten und übertragenen Daten sicher, sodass diese nicht durch unautorisierte Dritte eingesehen werden können. Dies verlangt auch die Anlage 1 Teil 3 Nr. 13.2 AFGBV bezüglich des Schutzes von Daten vor missbräuchlicher Verwendung und hinsichtlich der Vertraulichkeit der Datenübertragung. Sowohl die DS-GVO (Art. 5 Abs. 1, 32 Abs. 1 lit. b DS-GVO) wie auch die Anlage 1 Teil 5 AFGBV fordern, das Schutzziel der Vertraulichkeit sicherzustellen. Darüber hinaus regelt Art. 5 Abs. 1 lit. f DS-GVO und konkretisiert in Art. 32 DS-GVO, dass auch die datenverarbeitenden Systeme Vertraulichkeit gewährleisten müssen. Zudem verlangt Art. 25 Abs. 2 DS-GVO eine Beschränkung des Zugangs zu personenbezogenen Daten im Rahmen ihrer Verarbeitung. Insbesondere Daten aus dem digitalen Datenspeicher dür-

93 Geber NZV 2021, 14 (16).
94 Geber NZV 2021, 14 (16).
95 Geber NZV 2021, 14 (17).
96 Geber NZV 2021, 14 (17).
97 BT-Drs. 19/27439, 29.
98 S. dazu im Detail: Geber NZV 2021, 14; Solmecke/Jockisch MMR 2016, 359.
99 S. dazu zB die Ausführungen in: Eckert, IT-Sicherheit. Konzepte-Verfahren-Protokolle, 10. Aufl. 2018, S. 7 ff.

fen nur für das KBA und die dort genannten zuständigen Behörden zur Verfügung stehen (vgl. Anlage 1 Teil 3 Nr. 13.2 AFGBV).

TA02 verlangt, dass die Integrität der gespeicherten, verarbeiteten und übertragenen Daten sichergestellt ist. Die Anlage 1 Teil 1 Nr. 6 und Teil 3 Nr. 13.2 AFGBV schreibt vor, Daten vor Manipulation zu schützen sowie die Integrität der Datenübertragung sicherzustellen. Wie für die Vertraulichkeit, fordern sowohl AFGBV als auch DS-GVO (Art. 5 Abs. 1, 32 Abs. 1 lit. f DS-GVO), das Schutzziel Integrität sicherzustellen. Zusätzlich fordert die DS-GVO, dass die Integrität des datenverarbeitenden Systems sichergestellt ist. Die UNECE-Regelung 156 fordert den Schutz von Software gegen Manipulation und insbesondere die Integrität von Softwareaktualisierungen (UNECE-Regelung 156 Ziffer 7.2.1.1.). Zur Bewältigung der autonomen Fahraufgabe sollen zudem entsprechend Anlage 1 Teil 1 Nr. 6 AFGBV Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge, Infrastrukturkomponenten) iSd Integrität sicher empfangen und verwendet werden können.

Mit TA03 wird eine authentische Datenspeicherung, -verarbeitung und -übertragung sichergestellt, sodass der Ursprung und die Echtheit der Daten bzw. des Senders überprüft werden kann. Diese Anforderung leitet sich aus Anlage 1 Teil 1 Nr. 6 und Teil 3 Nr. 13.2 AFGBV zum Schutz von Daten gegen missbräuchliche Verwendung und die Authentizität der Datenübertragung ab. Die UNECE-Regelung 156 Ziffer 7.2.1.1. fordert die Authentizität von Softwareaktualisierungen und Art. 25 Abs. 2 DS-GVO verlangt, dass personenbezogene Daten nur einem begrenzten und für die Verarbeitung notwendigen Kreis von Personen zugänglich gemacht werden. Im Sinne der Authentizität wird in Anlage 1 Teil 1 Nr. 6 AFGBV zudem gefordert, dass zur Bewältigung der autonomen Fahraufgabe Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge oder Infrastrukturkomponenten) sicher empfangen und verwendet werden können.

TA04 fordert, dass Daten zur anlassbezogenen Speicherung (und (Weiter-)Verarbeitung) voneinander isoliert werden. So fordert § 1g Abs. 2 StVG eine nur für gesetzlich bestimmte Anlässe zulässige Speicherung der abschließend in § 1g Abs. 1 StVG aufgeführten und kategorisierten Daten. Die DS-GVO verlangt in Art. 5 Abs. 1 lit. b DS-GVO und Art. 25 Abs. 2 DS-GVO, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass nur zweckgebundene personenbezogene Daten verarbeitet werden und deren Menge, Umfang, Speicherfrist und Zugänglichkeit hierauf ausgerichtet ist. Insbesondere die in der Zweckbindung enthaltene Speicherbegrenzung wird in Art. 5 Abs. 1 lit. e DS-GVO herausgestellt. Diese Anforderung adressiert auch Anforderungen der DS-GVO bzw. der AFGBV bezüglich der Transparenz (Art. 5 Abs. 1 lit. a, Art 12 Abs. 1 DS-GVO, Anlage 1 Teil 3 AFGBV) und Datenminimierung personenbezogener Daten (Art. 5 Abs. 1 lit. c DS-GVO).

TA05 adressiert die Anforderung, dass es technisch möglich ist in die Datenverarbeitung einzugreifen, zB um die Datenverarbeitung zu stoppen. In § 1g Abs. 3 StVG wird gefordert, dass Kraftfahrzeughalter die „Datenhoheit" über die beim Betrieb der autonomen Fahrfunktion anfallenden Daten, technisch und organisatorisch, ermöglicht werden und Einstellungsmöglichkeiten zur Privatsphäre gegeben werden. Auch aus Art. 5 Abs. 1 DS-GVO ergibt sich Intervenierbarkeit als Datenschutzziel.

TA06 fordert, dass die Verarbeitung personenbezogener Daten für die Nutzer des Kraftfahrzeugs transparent gemacht wird. Dies verlangt auch Art. 5 Abs. 1 lit. a, 12 Abs. 1 DS-GVO, in dem die Transparenz für Betroffene einer Verarbeitung personenbezogener Daten gefordert wird. Insbesondere § 1g Abs. 3 StVG fordert, dass Kraftfahrzeughalter über die Datenverarbeitung in der autonomen Fahrfunktion informiert werden.

TA07 bezieht sich auf die im Rahmen der Zweckbindung erforderlichen Speicherfristen. Personenbezogene Daten sind in einer Form zu speichern, die eine Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Daher müssen gespeicherte Daten, nachdem ihre zweckgebundene Speicherung nicht länger erforderlich ist, so gelöscht werden, dass sie nicht wiederherstellbar sind, soweit nicht ein Ausnahmetatbestand der DS-GVO greift. Diese Anforderung kann aus Art. 5 Abs. 1 lit. e, 25 Abs. 2 DS-GVO abgeleitet werden.

TA08 sieht vor, dass der Personenbezug aus den verarbeiteten, gespeicherten und übermittelten Daten, wenn möglich, entfernt wird. Dies kann aus dem Grundsatz der Nichtverkettbarkeit abgeleitet werden. Nichtverkettbarkeit ist zwar nicht explizit in der DS-GVO geregelt, allerdings lässt sich diese aus Art. 5 Abs. 1 lit. f DS-GVO (Integrität und Vertraulichkeit) wie auch Art. 5 Abs. 1 lit. b DS-GVO, dem Zweckbindungsgrundsatz bei der Datenverarbeitung, herleiten. Art. 32 Abs. 1 lit. a DS-GVO fordert im Kontext der Sicherheit der Datenverarbeitung eine Pseudonymisierung der Daten. Auf Art. 32 DS-GVO verweist auch die AFGBV in Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2 sowie Teil 5 Nr. 15 und 16.

In TA09 wird gefordert, dass der fortwährende Zugriff auf zu verarbeitende personenbezogene Daten sichergestellt werden muss. Art. 5. Abs. 1 lit. f DS-GVO verlangt hier einen Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit"). Zudem verlangt Art. 32 Abs. 1 lit. b DS-GVO, dass die Verfügbarkeit der datenverarbeitenden Systeme sichergestellt wird. Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2, Teil 5 AFGBV fordert weiterhin, dass auch bei Datenübertragungen die Verfügbarkeit sichergestellt werden muss.

TA10 fordert, dass die Funktionen der datenverarbeitenden Systeme als auch die Daten selbst nach einem Ausfall, zB technisch bedingt oder durch einen Cyberangriff, wiederherstellbar sein müssen. Die Resilienz der datenverarbeitenden Systeme wird auch in Art. 32 Abs. 1 lit. b DS-GVO verlangt. Weiterhin fordert Art. 32 Abs. 1 lit. c DS-GVO, dass Daten und der Datenzugriff nach einem physischen oder technischen Zwischenfall wiederherstellbar sein müssen. Von der UNECE-Regelung 156 Ziffer 7.2.2.1.1. wird zudem vorgegeben, dass im Falle einer fehlgeschlagenen oder abgebrochenen Aktualisierung das System in der Lage sein muss, eine Vorversion des Systems wiederherzustellen bzw. das Kraftfahrzeug in einen sicheren Zustand zu versetzen.

Abschließend wird in TA11 gefordert, dass Absender wie auch Empfänger von Nachrichten das Absenden bzw. das Empfangen einer Nachricht im Nachhinein nicht abstreiten können. Dies kann aus Anlage 1 Teil 1 Nr. 6, Teil 3, Teil 5 AFGBV entnommen werden, wonach Datenübertragung u.a. das Schutzziel Nachweisbarkeit umfassen müssen. Das ergibt sich aus den in der AFGBV enthaltenen generell zu erfüllenden Anforderungen hinsichtlich IT-Sicherheit wobei Nachweisbarkeit zu den grundsätzlichen Schutzzielen der IT-Sicherheit gehört.[100] Auch aus Anlage 1 Teil 1 Nr. 6 AFGBV kann das Schutzziel der Nachweisbarkeit abgeleitet werden, da dort gefordert wird, dass zur Bewältigung der autonomen Fahraufgabe Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge oder Infrastrukturkomponenten) sicher empfangen und verwendet werden können.

100 Vgl. Standard-Datenschutzmodell, Version 2.0a, S. 9 f., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf.

Tabelle 1

Technische Anforderung (TA)	Beschreibung	Gesetzliche Anforderung [der Teil in eckigen Klammern ist für die jeweilige Technische Anforderung nicht relevant]
TA01: Vertrauliche Datenverarbeitung	Gespeicherte, verarbeitete und/oder übertragene rechtlich geschützte Daten dürfen nur durch berechtigte Personen/Prozesse einsehbar sein.	(a) Daten sollen nur für das KBA und die in § 1g StVG genannten zuständigen Behörden zum Zwecke einer Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten zur Verfügung stehen (§ 15 Abs. 2 AFGBV) (b) Zugang, Abruf und Übermittlung der gespeicherten Daten soll nur für das KBA und andere zuständige staatliche Stellen möglich sein (AFGBV Anlage 1 Teil 3 Nr. 13.2) (c) Das KBA darf die in Absatz 1 genannten Daten speichern und verwenden (§ 1g Abs. 4 StVG) (d) Behörden dürfen Daten gem. Absatz 6 Nr. 1 und 2 erheben, speichern und verwenden (§ 1g Abs. 6 StVG) (e) Daten müssen gemäß dem Stand der Technik vor [Manipulation und] missbräuchlicher Verwendung geschützt werden (AFGBV Anlage 1 Teil 3 Nr. 13.2 und Teil 5 Nr. 16) (f) Datenübertragungen müssen die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit, Authentizität und Verantwortlichkeit umfassen (AFGBV Anlage 1 Teil 1 Nr. 6 und Teil 5) (g) Datenschutzziele sind [Datenminimierung, Verfügbarkeit, Integrität,] Vertraulichkeit, [Nichtverkettung, Transparenz und Intervenierbarkeit] für Daten und datenverarbeitende Systeme (Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. a DS-GVO, Art. 32 Abs. 1 lit. b DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2 und Teil 5) (h) Maßnahmen müssen sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person einem unbestimmten Kreis von Personen zugänglich gemacht werden (Anforderungen aus Art. 25 Abs. 2 DS-GVO, wird nicht vollumfänglich durch § 1g Abs. 3 StVG geregelt) (i) Der Zugriff auf den Datenspeicher soll durch ein Zugangskontrollsystem abgesichert werden (AFGBV Anlage 1 Teil 1 Nr. 6) (j) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gegen unerlaubten Zugriff geschützt werden, zB durch Verschlüsselung (AFGBV Anlage 1 Teil 5 Nr. 16) (k) Datenspeicherung und Datenübermittlung müssen gemäß Stand der Technik vor Manipulation und Missbräuchlicher Verwendung geschützt werden (AFGBV Anlage 1 Teil 5, AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. d) (l) Zur Bewältigung der autonomen Fahraufgabe sollen Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge, Infrastrukturkomponenten) sicher empfangen und verwendet werden können (AFGBV Anlage 1 Teil 1 Nr. 6)
TA02: Integritätsgeschützte Datenverarbeitung	Gespeicherte, verarbeitete und/oder übertragene rechtlich geschützte Daten dürfen nur durch berechtigte Personen/Prozesse modifizierbar sein.	(a) Datenspeicherung und Datenübermittlung müssen gemäß dem Stand der Technik vor Manipulation [und missbräuchlicher Verwendung] geschützt werden (AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. d) (b) Datenübertragungen müssen die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit, Authentizität und Verantwortlichkeit umfassen (AFGBV Anlage 1 Teil 1 Nr. 6 und Teil 5) (c) Datenschutzziele sind [Datenminimierung, Verfügbarkeit,] Integrität, [Vertraulichkeit, [Nichtverkettung, Transparenz und Intervenierbarkeit] für Daten und datenverarbeitende Systeme (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. a, 32 Abs. 1 lit. b DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2 und Teil 5) (d) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (e) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (f) Durchführbarkeit einer periodisch-technischen Fahrzeugintegritätsüberwachung sicherstellen (§ 12 Abs. 1 Nr. 4 AFGBV) (g) Erkennung, Protokollierung und Reaktion auf mögliche Cyberangriffe (UNECE-Regelung 155 Ziffer 5.1.1., AFGBV Anlage 1 Teil 1 Nr. 7.2.2) (h) Regelmäßige Überprüfung der sicherheitsrelevanten elektronischen Systeme (§ 13 Abs. 1 Nr. 2, Abs. 7 AFGBV) (i) Schutz der Software vor Manipulationen (UNECE-Regelung 156 Ziffer 7.1.3.1.) (j) Integrität von Softwareaktualisierungen schützen, sodass sowohl ihre Beeinträchtigung als auch eine ungültige Aktualisierung ausgeschlossen sind (UNECE-Regelung 156 Ziffer 7.2.1.1.) (k) Die Integrität (von Teilen) der Fahrzeugsoftware muss sichergestellt werden, um zu gewährleisten, dass ein Updateprozess mit genügend Restenergie (Batteriekapazität) durchgeführt werden kann (UNECE-Regelung 156 Ziffer 7.2.2.1.2.–7.2.2.5.) (l) Zur Bewältigung der autonomen Fahraufgabe sollen Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge, Infrastrukturkomponenten) sicher empfangen und verwendet werden können (AFGBV Anlage 1 Teil 1 Nr. 6)

Technische Anforderung (TA)	Beschreibung	Gesetzliche Anforderung [der Teil in eckigen Klammern ist für die jeweilige Technische Anforderung nicht relevant]
TA03: Authentische Datenverarbeitung	Die Echtheit der gespeicherten, verarbeiteten und übertragenen Daten muss gewährleistet werden. Weiterhin muss die Echtheit der Kommunikationsteilnehmer überprüfbar sein.	(a) Datenspeicherung und Datenübermittlung müssen gemäß dem Stand der Technik vor Manipulation [und missbräuchlicher Verwendung] geschützt werden (AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. d) (b) Datenübertragungen müssen die Schutzziele [Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit,] Authentizität [und Verantwortlichkeit] umfassen (AFGBV Anlage 1 Teil 1 Nr. 6) (c) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (d) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (e) Erkennung, Protokollierung und Reaktion auf mögliche Cyberangriffe (UNECE-Regelung 155 Ziffer 5.1.1., AFGBV Anlage 1 Teil 1 Nr. 7.2.2) (f) Authentizität [und Integrität] von Softwareaktualisierungen schützen, sodass sowohl ihre Beeinträchtigung als auch eine ungültige Aktualisierung ausgeschlossen sind (UNECE-Regelung 156 Ziffer 7.2.1.1.) (g) Die Authentizität (von Teilen) der Fahrzeugsoftware muss sichergestellt werden, um zu gewährleisten, dass ein Updateprozess mit genügend Restenergie (Batteriekapazität) durchgeführt werden kann (UNECE-Regelung 156 Ziffer 7.2.2.1.2.–7.2.2.5.) (h) Maßnahmen müssen sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person einem unbestimmten Kreis von Personen zugänglich gemacht werden (Art. 25 Abs. 2 DS-GVO, wird nicht vollumfänglich in § 1g Abs. 3 StVG geregelt) (i) Zur Bewältigung der autonomen Fahraufgabe sollen Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge, Infrastrukturkomponenten) sicher empfangen und verwendet werden können (AFGBV Anlage 1 Teil 1 Nr. 6)
TA04: Datenisolation	Um eine anlassbezogene Speicherung (und (Weiter-)Verarbeitung) der Daten zu ermöglichen, werden diese voneinander isoliert.	(a) Anlassbezogene Speicherung der Daten (§ 1g Abs. 2 StVG, Art. 5 Abs. 1 lit. b DS-GVO) (b) Kategorisierung der kontrollierten Daten (§ 1g Abs. 1 StVG) (c) Hersteller muss durch technische Maßnahmen sicherstellen, dass durch Voreinstellung nur zweckgebundene personenbezogene Daten, unter Sicherstellung der Menge, Umfang, Speicherfrist und Zugänglichkeit, verarbeitet werden (Art. 25 Abs. 2 DS-GVO, Zwecke zB in § 1g Abs. 2, 4, 5, 6 und 7 StVG, § 15 Abs. 2 AFGBV) (d) Daten sind unverzüglich zu löschen, sobald sie für die Zwecke nach Satz 1 nicht mehr erforderlich sind, spätestens aber drei Jahre nach Einstellung des Betriebs des entsprechenden Kraftfahrzeugs (§ 1g Abs. 6 S. 2 StVG, Art. 5 Abs. 1 lit. e DS-GVO) (e) Die Speicherdauer und unverzügliche Löschung nach Wegfall der Erforderlichkeit gilt auch für Daten, die beim KBA gespeichert werden (§ 1g Abs. 4 StVG) (f) Konkret heißt es dazu in der AFGBV, dass der integrierte Datenspeicher „ereignisbasiert und während des Betriebes nach § 9 Abs. 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfasst, speichert und verwendet." (AFGBV Anlage 1 Teil 3 Nr. 13) (g) Verschiedene Anlässe (u.a. Unfallszenario) zur Datenspeicherung (§ 1g Abs. 2 Nr. 1–4 StVG) (h) Zweckgebundene Datenverarbeitung (u.a. Forschung) (§ 1g Abs. 5 StVG) (i) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (j) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (k) Datenschutzziele sind [Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit,] Nichtverkettung, [Transparenz und Intervenierbarkeit] (Art. 5 Abs. 1 lit. b, lit. c DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13, 13.2 und Teil 5)
TA05: Interventionsfähigkeit	Es muss in die Datenverarbeitung eingegriffen werden können.	(a) Datenschutzziele sind [Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und] Intervenierbarkeit (Art. 5 Abs. 1 DS-GVO) (b) Hersteller muss durch technische Maßnahmen sicherstellen, dass durch Voreinstellung nur zweckgebundene personenbezogene Daten, unter Sicherstellung der Menge, Umfang, Speicherfrist und Zugänglichkeit, verarbeitet werden (Art. 25 Abs. 2 DS-GVO, Zwecke zB in § 1g Abs. 2, Abs. 4, Abs. 5, Abs. 6, Abs. 7 StVG, § 15 Abs. 2 AFGBV) (c) Maßnahmen müssen sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person einem unbestimmten Kreis von Personen zugänglich gemacht werden (Art. 25 Abs. 2 DS-GVO, wird nicht vollumfänglich in § 1g Abs. 3 StVG geregelt) (d) Fahrzeughalter muss die „Datenhoheit" über die beim Betrieb der autonomen Fahrfunktion anfallenden Daten, technisch und organisatorisch, ermöglicht werden (§ 1g Abs. 3 StVG) (e) Fahrzeughalter sind Einstellungsmöglichkeiten zur Privatsphäre zu eröffnen (§ 1g Abs. 3 StVG) (f) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (g) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (h) Erkennung, Protokollierung und Reaktion auf mögliche Cyberangriffe (UNECE-Regelung 155, AFGBV Anlage 1 Teil 1 Nr. 7.2.2)

Technische Anforderung (TA)	Beschreibung	Gesetzliche Anforderung [der Teil in eckigen Klammern ist für die jeweilige Technische Anforderung nicht relevant]
TA06: Transparenz	Die Datenverarbeitung muss den Nutzern sichtbar gemacht werden.	(a) Fahrzeughalter werden über die Datenverarbeitung in der autonomen Fahrfunktion informiert (§ 1g Abs. 3 StVG) (b) Datenschutzziele sind [Datenminimierung, Verfügbarkeit, Integrität,] Vertraulichkeit, [Nichtverkettung, Transparenz und Intervenierbarkeit] (Art. 5 Abs. 1 lit. f DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2 und Teil 5) (c) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (d) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16)
TA07: Sicheres Löschen	Gespeicherte Daten müssen, nach dem Wegfall der Erforderlichkeit, so gelöscht werden, dass sie nicht wiederherstellbar sind.	(a) Hersteller muss durch technische Maßnahmen sicherstellen, dass durch Voreinstellung nur zweckgebundene personenbezogene Daten, unter Sicherstellung der Menge, Umfang, Speicherfrist und Zugänglichkeit, verarbeitet werden (Art. 25 Abs. 2 DS-GVO, Zwecke zB in § 1g Abs. 2, Abs. 4, Abs. 5, Abs. 6, Abs. 7 StVG, § 15 Abs. 2 AFGBV) (b) Daten sind unverzüglich zu löschen, sobald sie für die Zwecke nach Satz 1 nicht mehr erforderlich sind, spätestens aber drei Jahre nach Einstellung des Betriebs des entsprechenden Kraftfahrzeugs (§ 1g Abs. 6 S. 2 StVG) (c) Die Speicherdauer und unverzügliche Löschung nach Wegfall der Erforderlichkeit gilt auch für Daten, die beim KBA gespeichert werden (§ 1g Abs. 4 StVG) (d) Speicherbegrenzung personenbezogener Daten (Art. 5 Abs. 1 lit. e DS-GVO) (e) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (f) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16)
TA08: De-Identifikation	Wenn möglich, soll der Personenbezug aus den gespeicherten, verarbeiteten und übermittelten Daten entfernt werden.	(a) Datenschutzziele sind [Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit,] Nichtverkettung [Transparenz und Intervenierbarkeit] (Art. 5 Abs. 1 lit. b, lit. f DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13, 13.2 und Teil 5) (b) Sinnvolle Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2 und Teil 5 Nr. 15 und 16) (c) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (d) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (e) Zur Bewältigung der autonomen Fahraufgabe sollen Nachrichten von externen technischen Einheiten (zB Backends, externe Sensoren, Smartphones, andere Kraftfahrzeuge, Infrastrukturkomponenten) sicher empfangen und verwendet werden können (AFGBV Anlage 1 Teil 1 Nr. 6)
TA09: Verfügbarkeit	Der fortwährende Zugriff auf notwendig zu verarbeitende personenbezogene Daten muss sichergestellt werden.	(a) Der Datenspeicher darf nicht flüchtig sein und die Daten sollen auch im stromlosen Zustand erhalten bleiben (AFGBV Anlage 1 Teil 3 Nr. 13) (b) Verfügbarkeit der datenverarbeitenden Systeme, Dienste und Daten muss sichergestellt werden (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. b, lit. c DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2, Teil 5) (c) Datenübertragungen müssen die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit, Authentizität und Verantwortlichkeit umfassen (AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13, 13.2 und Teil 5) (d) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (e) Protokollierung möglicher Cyberangriffe (UNECE-Regelung 155 Ziffer 5.1.1., AFGBV Anlage 1 Teil 1 Nr. 7.2.2)
TA10: Resilienz	Sowohl die Funktion der datenverarbeitenden Systeme als auch die Daten selbst müssen nach einem Ausfall, zB technisch bedingt oder durch einen Cyberangriff, wiederherstellbar sein.	(a) Belastbarkeit der Systeme und Dienste, Wiederherstellbarkeit der Daten und des Datenzugriffs (Art. 32 Abs. 1 lit. b DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2, Teil 5) (b) Wiederherstellbarkeit der Daten und des Datenzugriffs (nach physischem oder technischem Zwischenfall) (Art. 32 Abs. 1 lit. c DS-GVO, AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13.2, Teil 5) (c) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5) (d) Protokollierung möglicher Cyberangriffe (UNECE-Regelung 155 Ziffer 5.1.1., AFGBV Anlage 1 Teil 1 Nr. 7.2.2) (e) Im Fall einer fehlgeschlagenen oder abgebrochenen Aktualisierung muss das System in der Lage sein, eine Vorversion des Systems wiederherzustellen bzw. das Kraftfahrzeug in einen sicheren Zustand zu versetzen (UNECE-Regelung 156 Ziffer 7.2.2.1.1.–7.2.2.5.)
TA11: Nachweisbarkeit	Sowohl Absender als auch Empfänger von Nachrichten sollen das Absenden bzw. das Empfangen einer Nachricht im Nachhinein nicht abstreiten können.	(a) Datenübertragungen müssen die Schutzziele [Vertraulichkeit, Integrität, Verfügbarkeit] Nachweisbarkeit [Authentizität und Verantwortlichkeit] umfassen (AFGBV Anlage 1 Teil 1 Nr. 6, Teil 3 Nr. 13, 13.2, Teil 5) (b) Der Datenspeicher soll durch kryptografische Schutzmaßnahmen nach BSI-TR abgesichert werden (AFGBV Anlage 1 Teil 3 Nr. 13) (c) Datenkanäle der Funkverbindungen müssen nach Stand der Technik mit offenen und etablierten Standards gesichert werden (AFGBV Anlage 1 Teil 5 Nr. 16) (d) Erkennung, Protokollierung und Reaktion auf mögliche Cyberangriffe (UNECE-Regelung 155 Ziffer 5.1.1., AFGBV Anlage 1 Teil 1 Nr. 7.2.2.)

2. Abgeleitete Technische Maßnahmen

Die Tabelle am Ende dieses Abschnitts gibt einen nicht abschließenden Überblick über potenzielle technische Maßnahmen, mit denen die oben abgeleiteten Anforderungen umgesetzt werden können.

Diese sind teilweise auch aus anderen Arbeiten übernommen.[101] Generell sind unterschiedliche Methoden geeignet, um die Anforderungen umzusetzen, je nachdem, ob die Daten gespeichert, verarbeitet oder übertragen werden.

a) TA01: Vertrauliche Datenverarbeitung

Für die Datenspeicherung und -verarbeitung können Zugriffskontrollmöglichkeiten über verschlüsselte Container, Software oder Hardwareisolation umgesetzt werden. Bei verschlüsselten Containern werden die sicherheitskritischen Daten verschlüsselt auf einem Datenträger abgelegt und bei Bedarf, zB zur Verarbeitung, temporär entschlüsselt.

Diese Operation sollte nach Möglichkeit in abgeschirmten Umgebungen durchgeführt werden. In der einfachsten Form können dabei Isolationsverfahren auf Softwareebene genutzt werden. Dazu gehören einfache Mechanismen wie Access Control Lists (ACLs), Mandatory Access Control (MAC) oder Discretionary Access Control (DAC). Weiterhin kann man einzelne Bereiche gegeneinander abschirmen, etwa über Hypervisor-Ansätze (Virtuelle Maschinen) oder leichtgewichtige Virtualisierungstechniken auf Betriebssystemebene (Docker, LXD, NSpawn). State-of-the-Art-Verfahren lagern sicherheitskritische Daten und Operationen in Hardware-isolierte Umgebungen aus. Diese können zB über Memory Protection/Management Units (MPUs/MMUs), dedizierte Hardware-Sicherheitschips, wie ein Trusted Platform Module (TPM) oder ein Hardware Security Module (HSM), oder Prozessorerweiterungen wie ARM TrustZone oder Intel TXT/SGX umgesetzt werden.

Für den Übertragungsweg können physikalisch, logisch oder kryptografisch getrennte Kanäle genutzt werden, um die Vertraulichkeit der übertragenen Daten sicherzustellen. State-of-the-Art sind hier kryptografisch getrennte Kanäle, bei denen zB auf Transport oder Datenebene verschlüsselt wird, um die Daten vor dem Zugriff durch Unbefugte zu schützen.

b) TA02: Integritätsgeschützte Datenverarbeitung

Um die Daten integritätsgeschützt zu speichern, können die Daten mit Cyclic Redundancy Checks (CRCs) erweitert werden. Diese bieten allerdings keinen Schutz gegen absichtliche Manipulation. Dazu können integritätsgeschützte Container genutzt werden, die zB über kryptografisch-gestützte Integritätsmaßnahmen, wie Message Authentication Codes (MACs) oder digitale Signaturen, gegen unbemerkte Manipulation geschützt werden können.

Weiterhin eignen sich auch die Maßnahmen aus TA01 (Datenspeicher), wie Software(SW)-Isolation oder Hardware-gestützte Abschirmung, um die Integrität der gespeicherten Daten sicherzustellen. Dazu können Integritätsmess- und -feststellungsverfahren aus dem Bereich Trusted Computing genutzt werden, um die Integrität des Systems und der darauf gespeicherten Daten zu gewährleisten. Auch können Redundanzkonzepte auf Datenebene geeignet sein, um Datenspeicher durch Abgleich auf ihre Integrität hin zu überprüfen.

Um die Integrität der Datenverarbeitung zu wahren, können zum einen wieder die technischen Maßnahmen aus TA01 (Datenverarbeitung), wie SW-Isolation oder Hardware-gestützte Abschirmung, genutzt werden und zum anderen die bereits erwähnten Redundanzkonzepte, diesmal auf Prozessebene.

Ein Beispiel dieser Prozessredundanzkonzepte können sog. Lockstep-Verfahren sein, bei denen dieselbe datenverarbeitende Operation parallel durchgeführt wird und unterschiedliche Ergebnisse auf eine Integritätsverletzung schließen lassen. Auch lassen sich hier erneut Integritätsmess- und -feststellungsverfahren aus dem Bereich Trusted Computing nutzen, um die Integrität der Datenverarbeitung sicherzustellen.

Bezüglich der Datenübertragung können ebenfalls CRCs an die Daten angehängt werden, um die Integrität der Daten zu schützen, wobei auch hier wieder kein Schutz gegen beabsichtigte Manipulation besteht. Eine gängige Methode ist die kryptografische Absicherung der Kanäle oder der Daten selbst. Dazu können wieder MACs oder digitale Signaturen genutzt werden.

c) TA03: Authentische Datenverarbeitung

Um die Authentizität der gespeicherten Daten sowie die Datenverarbeitung sicherzustellen, können die technischen Maßnahmen aus TA01 (Datenspeicher/-verarbeitung) genutzt werden.

Darüber hinaus kann bei gespeicherten Daten zusätzlich über kryptografische Maßnahmen wie MACs oder digitale Signaturen die Authentizität sichergestellt werden. Auch die Authentizität der Datenübertragung kann mittels kryptografischer Maßnahmen wie MACs oder digitale Signaturen sichergestellt werden.

d) TA04: Datenisolation

Für die Isolation von Daten können für die Speicherung, Verarbeitung und Übertragung die technischen Maßnahmen aus TA01 (Datenspeicher/-verarbeitung/-übertragung) genutzt werden. Insbesondere für die Verarbeitung und Speicherung können die SW-Isolations- und Hardware-gestützten Abschirmungstechniken verwendet werden, um die Daten während der Speicherung und Verarbeitung voneinander zu isolieren.

e) TA05: Interventionsfähigkeit

Um die Interventionsfähigkeit der Nutzer in den Datenverarbeitungsprozess sicherzustellen, können zB Zugriffs- und Datenflusskontrollsysteme umgesetzt werden, um schon im Kraftfahrzeug zum Zeitpunkt der Erhebung Einfluss nehmen zu können.[102]

Über diese Technik können zB Datenflüsse eingeschränkt, umgeleitet oder so modifiziert werden, dass identifizierende Merkmale aus den Daten entfernt werden (vgl. TA08: De-Identifikation). Abhängig von der Implementierung können zB die in TA01 (Datenspeicher/-verarbeitung) vorgeschlagenen Maßnahmen bezüglich Isolation und Abschirmung genutzt werden, um den Zugriff auf zu verarbeitende Daten und/oder den Verarbeitungsprozess zu verhindern.

f) TA06: Transparenz

Ähnlich wie auch bei TA05 können, um die Transparenz der Datenerhebung und -verarbeitung sicherzustellen, Zugriffs- und Datenflusskontrollsysteme zum Einsatz kommen, um die Nutzer über die jeweiligen Prozesse zu informieren. Gespeicherte, verarbeitete und übermittelte Daten können über verschiedene rein software-basierte Techniken wie Tagging oder Sticky Policies unterstützt, oder durch kryptografische Verfahren wie MACs oder digitale Signaturen markiert werden, um zB den

101 Plappert/Stancke/Jäger, Towards a Privacy-Aware Electric Vehicle Architecture, 30th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2022.

102 S. dazu die vorgeschlagenen Systeme in: Plappert/Zelle/Krauß et al., A Privacy-aware Data Access System for Automotive Applications, 15th Conference on Embedded Security in Cars (ESCAR) Europe, 2017, abrufbar unter: http://publica.fraunhofer.de/documents/N-645954.html.

Zweck der Datenerhebung auch über mehrere Komponenten hinweg nachverfolgbar zu machen.

Auch hier ist es möglich, über die in TA01 (Datenspeicher/-verarbeitung) vorgeschlagenen Maßnahmen zu Isolation und Abschirmung zweckgebundene voneinander isolierte Umgebungen zu erzeugen, die Daten eines Zwecks verarbeiten.

g) TA07: Sicheres Löschen

Maßnahmen zur Umsetzung eines sicheren Löschvorgangs resultieren aus der mit der Zweckbindung verbundenen maximalen Speicherdauer bzw. dem Nutzerrecht der Datenverarbeitung. Um auszuschließen, dass Daten nach dem Löschen wiederhergestellt werden können, eignen sich als Datenspeicher verschlüsselte Container oder die in TA01 (Datenspeicher/-verarbeitung) vorgeschlagenen Maßnahmen zur Isolation und Abschirmung.

h) TA08: De-Identifikation

Maßnahmen zur De-Identifikation entfernen identifizierende Merkmale aus Daten und erzeugen Pseudonymität oder Anonymität. Die Wirksamkeit der einzelnen Verfahren richtet sich stark nach dem jeweiligen Anwendungsfall und muss genau analysiert werden, um die Funktionsweise des Anwendungsfalls beizubehalten. Je nach Umsetzung kann es schon genügen, Daten mit den in TA01 (Datenspeicher/-verarbeitung/-übertragung) vorgeschlagenen Maßnahmen voneinander isoliert zu speichern, zu verarbeiten oder zu übertragen. Daneben kann es wirksam sein, je nach Anwendungsfall, Daten zu aggregieren, generalisieren, statistisch zu durchmischen oder Datenübertragungen zu verzögern.

i) TA09: Verfügbarkeit

Die Verfügbarkeit der Daten und datenverarbeitenden Prozesse kann primär über Redundanzmaßnahmen sichergestellt werden. Für die Datenspeicherung bedeutet dies ein Vorhalten von redundanten Daten in verteilten Datenbanken, während bei der Verarbeitung gesamte Prozesse redundant auf verschiedenen Komponenten vorgehalten werden müssen. Bei der Übertragung können je nach Anwendungsfall entweder redundante Kanäle oder verschiedene Übertragungsmedien (Bluetooth, NFC, Internet, Wifi) genutzt werden, um einen Totalausfall zu vermeiden.

Generell kann es auch möglich sein, zB über leichtgewichtige kryptografische Verfahren den Aufwand für Denial-of-Service-Angriffe zu erhöhen, sodass diese nicht mehr rentabel für den Angreifer sind. Weiterhin können auch die in TA02 (Datenspeicher/-verarbeitung) vorgeschlagenen Maßnahmen genutzt werden, um Daten und Prozesse gegen Manipulation oder Löschen zu sichern.

j) TA10: Resilienz

Resilienzmaßnahmen können unterschiedlichen Zwecken dienen: Zur Verhinderung von Cyberangriffen, zur Bereitstellung von Handlungsalternativen bei erfolgreichen Cyberangriffen, zur Aufrechterhaltung von Systemfunktionalität während Cyberangriffen, zur Begrenzung des Schadens durch Cyberangriffe sowie zur Wiederherstellung der Systemfunktionalität nach Cyberangriffen.[103]

Zur Verhinderung von Cyberangriffen können die in TA02 und TA03 aufgeführten Maßnahmen zum Schutz der Integrität und Authentizität beitragen. Des Weiteren können auch einige der bereits in TA01 aufgeführten Maßnahmen zur Beschränkung von Berechtigungen wie zB ACLs, MAC oder DAC basierend auf Attributen von Benutzern, Systemkontext oder Sensorinformationen eingesetzt werden. Zur Bereitstellung von Handlungsalternativen bei erfolgreichen Cyberangriffen müssen im Vorfeld alle möglichen Angriffssituationen analysiert werden und Gegenmaßnahmen geplant und implementiert werden. Zur Aufrechterhaltung von Systemfunktionalität während Cyberangriffen kann eine adaptive Reaktion erfolgen, welche die vorgeplanten Handlungsalternativen sinnvoll nutzt. Ein Intrusion Detection System (IDS) kann bekannte Angriffe in einer Komponente oder im Datenverkehr des Bordnetzes eines Fahrzeugs erkennen. Ein Anomalieerkennungssystem kann darüber hinaus auch nicht erwartetes Verhalten erkennen, welches auf mögliche neue Angriffe hinweist und damit zu einer Einschätzung der aktuellen Situation beitragen. Anschließend können mit diesem Wissen vorgeplante Maßnahmen eingeleitet werden. Ggf. müssen basierend auf der Analyse der Situation Funktionen oder Übertragungskanäle eingeschränkt werden, um den Angreifer nicht weiter in das System vordringen zu lassen.

Weiterhin können die in TA09 beschriebenen Redundanzmechanismen genutzt werden, welche mehrere geschützte Instanzen kritischer Ressourcen und Übertragungskanäle bereitstellen. Im Idealfall sollten die redundanten Funktionen auf unterschiedliche Art realisiert werden, damit nicht alle von demselben Cyberangriff betroffen sind. Zur Begrenzung des Schadens durch Cyberangriffe können zB die in TA04 aufgeführten Maßnahmen zur Datenisolation durch Segmentierung genutzt werden. Zur Wiederherstellung der Systemfunktionalität nach Cyberangriffen können die in TA09 beschriebenen Redundanzmechanismen genutzt werden, um den Wiederherstellungsprozess zu vereinfachen. Daneben gibt es aus Prozesssicht Containerisierungs- und Hot/Cold-Failover-Konzepte, die einen Wiederherstellungsprozess vereinfachen.

Zwischen den Resilienzmaßnahmen können Synergien aber auch Konflikte bestehen. Maßnahmen können zB zur Verbesserung der Resilienz negative Effekte auf die Verfügbarkeit haben oder die Komplexität des Systems erhöhen, wodurch ggf. auch neue Angriffe möglich werden. Der Einsatz von Anomalieerkennungssystemen kann durch Fehleinschätzungen der Situation Reaktionen auslösen, welche das Systemverhalten möglicherweise unnötig einschränken. Daher müssen beim Einsatz von Resilienzmaßnahmen oft systemtechnische Kompromisse eingegangen werden, welche meist auf Risiko- und Kostenabwägungen beruhen.

k) TA11: Nachweisbarkeit

Nachweisbarkeit lässt sich dadurch erreichen, dass zB die Vertrauenswürdigkeit der Systeme mit Integritätsmess- und -verifikationsverfahren wie Secure Boot, Measured Boot und/oder Attestierung so sichergestellt wird, dass eine Manipulation ausgeschlossen werden kann. Darüber hinaus lassen sich auch die in TA01 (Datenspeicher/-verarbeitung) vorgeschlagenen Maßnahmen zur Isolation und Abschirmung nutzen, um vertrauenswürdige Umgebungen zur Datenverarbeitung zu erzeugen. Bei der Datenübertragung können kryptografisch gesicherte Kanäle aufgebaut oder die Daten an sich gesichert werden. Dazu können wieder MACs und digitale Signaturen zum Einsatz kommen.

103 S.a.: Ross/Pillitteri/Graubart/Bodeau/McQuaid, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach U.S. Department of Commerce, U.S. Department of Commerce, 2021.

Tabelle 2

TA01: Vertrauliche Datenverarbeitung	
Datenspeicher/-verarbeitung	• Verschlüsselte Container • SW-Isolation – Softwaremechanismen wie ACLs, MAC, DAC – Hypervisor-Ansätze, – OS-Level Virtualisierung (Container wie Docker, NSpawn, LXD, ...) • Hardware-gestützte Abschirmung – Technologien wie MPUs/MMUs – Dedizierte Sicherheitschips (TPM, HSM) – Prozessor Isolationstechniken (ARM TrustZone, Intel TXT/SGX)
Datenübertragung	• Getrennte physikalische Kanäle (extra Kabel, andere Übertragungsmedien) • Getrennte logische Kanäle (VLANs) • Kryptografisch gesicherte Kanäle/Daten (Verschlüsselung)
TA02: Integritätsgeschützte Datenverarbeitung	
Datenspeicher	• CRC[103], integritätsgeschützte Container, kryptografisch-gestützte Integritätsmaßnahmen (MACs, Signaturen), technische Maßnahmen aus TA01 (Datenspeicher), Redundanzkonzepte auf Datenebene, Integritätsmess- und -feststellungsverfahren (Secure Boot, Measured Boot, Attestierung)
Datenverarbeitung	• Technische Maßnahmen aus TA01 (Datenverarbeitung), Redundanzkonzepte auf Prozessebene, Lockstep, Integritätsmess- und -verifikationsverfahren (Secure Boot, Measured Boot, Attestierung)
Datenübertragung	• CRC, kryptografisch gesicherte Kanäle/Daten (MACs, Signaturen)
TA03: Authentische Datenverarbeitung	
Datenspeicher	• MACs, Signaturen, Technische Maßnahmen aus TA01 (Datenspeicher)
Datenverarbeitung	• Technische Maßnahmen aus TA01 (Datenverarbeitung)
Datenübertragung	• Kryptografisch gesicherte Kanäle/Daten (MACs, Signaturen)
TA04: Datenisolation	
Datenspeicher	• Tagging, Sticky Policies • Technische Maßnahmen aus TA01–TA03 (Datenspeicher)
Datenverarbeitung	• Technische Maßnahmen aus TA01–TA03 (Datenverarbeitung)
Datenübertragung	• Technische Maßnahmen aus TA01–TA03 (Datenübertragung)
TA05: Interventionsfähigkeit	
Datenverarbeitung/ Datenübertragung	• Data Flow/Access Control[104] • Technische Maßnahmen aus TA01 (Datenspeicher/-verarbeitung)
TA06: Transparenz	
Datenverarbeitung/-übertragung	• Data Flow/Access Control, Tagging, Sticky Policies • MACs/Signaturen • Technische Maßnahmen aus TA01 (Datenspeicher/-verarbeitung)
TA07: Sicheres Löschen	
Datenspeicher	• Verschlüsselte Container • Isolierte Umgebungen (zB MPU, dedizierter Sicherheitschip)
TA08: De-Identifikation	
Datenspeicher	• Maßnahmen aus TA01: Datenspeicher/-verarbeitung, Aggregation, Generalisierung, statistische Durchmischung, Übertragungsverzögerungen
Datenverarbeitung	• Maßnahmen aus TA01: Datenspeicher/-verarbeitung
Datenübertragung	• Aggregation, Generalisierung, statistische Durchmischung, Übertragungsverzögerung[105]
TA09: Verfügbarkeit	
Daten	• Redundante Speicherung, Maßnahmen aus TA02 (Datenspeicher) um Daten gegen Manipulation oder Löschen zu sichern
Prozesse	• Redundante Prozessverteilung, Maßnahmen aus TA02 (Datenverarbeitung) um Prozesse gegen Manipulation oder Löschen zu sichern, leichtgewichtige Kryptografie
Datenübertragung	• Redundante Kanäle/Übertragungsmedien, Leichtgewichtige Kryptografie
TA10: Resilienz	
Daten	• Maßnahmen aus TA01: Zugriffskontrolle, aus TA02, TA03: Integrität und Authentizität und aus TA04: Datenisolation TA09: Verfügbarkeit (Daten)
Prozesse	• Vorabplanung von Handlungsalternativen; Anomalieerkennung zur Bewertung der Situation Maßnahmen aus TA09: Verfügbarkeit (Prozesse), Containerisierung, Hot/Cold Failover Konzepte
Datenübertragung	• Maßnahmen aus TA09: Verfügbarkeit (Datenübertragung)
TA11: Nachweisbarkeit	
Datenspeicher/-verarbeitung/ -übertragung	• Integritätsmess- und -verifikationsverfahren (Secure Boot, Measured Boot, Attestierung), kryptografisch gesicherte Kanäle/Daten (MACs, Signaturen), Maßnahmen aus TA01: Datenspeicher/-verarbeitung

103 Maßnahme eignet sich nicht zum Schutz gegen absichtliche Manipulation.
104 Wie zB vorgeschlagen in: Plappert/Zelle/Krauß et al., A privacy-aware data access system for automotive applications, in 15th ESCAR Europe, Conference on Embedded Security in Cars, 2017.
105 Wie zB vorgeschlagen in: Plappert/Zelle/Krauß et al., A Privacy-aware Data Access System for Automotive Applications, in 15th ESCAR Europe, Conference on Embedded Security in Cars, 2017.

Auch in der UNECE-Regelung 155 werden Maßnahmen zur Absicherung des Kraftfahrzeugs vorgeschlagen. Im nachfolgenden Abschnitt werden diese Maßnahmen analysiert und mit den von uns erarbeiteten TA abgeglichen:

3. Minderungsmaßnahmen nach UNECE-Regelung 155

Die UNECE-Regelung 155 listet im Anhang Maßnahmen (M1-M24) zur Minderung von Bedrohungen auf.[104] Diese Maßnahmen werden im Folgenden vorgestellt und im Anschluss gegen die rechtlichen Anforderungen abgeglichen.

Die Maßnahmen umfassen zunächst Empfehlungen für Server und Cloud-Umgebungen (M1-M5). Dies umfasst die Anforderungen Maßnahmen gegen innere Angreifer (M1), gegen unautorisierte Zugriffe (M2), zur Wiederherstellung von Systemen im Falle eines Ausfalls (M3), zur Minimierung der Risiken durch Cloudcomputing (M4) und gegen Datenverlust (M5) zu ergreifen. Hinzu kommen Maßnahmen zur Anwendung von Sicherheitsrichtlinien nach dem Stand der Technik. So sollen Systeme mit dem „Security by Design"-Ansatz entwickelt werden. IT-Sicherheit soll also bereits bei der Konzeptphase ein zentraler Bestandteil des Entwicklungsprozesses sein (M6). Weiterhin sollen „Best Practices" bei der Soft- und Hardwareentwicklung (M23) wie auch beim Schutz der Integrität und Vertraulichkeit bei der Speicherung personenbezogener Daten (M24) angewendet werden.

Weiterhin werden Maßnahmen zur Zugriffskontrolle gefordert. Diese Maßnahmen sind aufgeteilt in Zugriffskontrollen, die angewendet werden sollen, um Systemdaten und -code zu schützen (M7). Ebenfalls soll ein Systemdesign und eine Zugriffskontrolle, die es unautorisierten Personen nicht möglich macht auf personenbezogene und systemkritische Daten zuzugreifen, etabliert werden (M8). Außerdem sollen unautorisierte Zugriffe erkannt und verhindert werden (M9). Ebenso soll ein Rollen- und Rechtemanagement implementiert werden, bei dem nur die nötigsten Berechtigungen vergeben werden (M18). Organisatorisch soll sichergestellt werden, dass IT-sicherheitsrelevante Prozesse definiert und befolgt werden. Dies umfasst das Erfassen von Aktionen und Zugriffen, die mit der Verwaltung von IT-Sicherheitsfunktionen im Zusammenhang stehen.

Außerdem sollen Nachrichten auf Integrität und Authentizität geprüft werden (M10) und die Übertragung vertraulich erfolgen (M12). Kryptografische Schlüssel sollten dabei sicher gespeichert werden (M11). Eine weitere Maßnahme umfasst den Einsatz von Intrusion Detection Systemen (IDS). Angriffserkennung und Abwehr bei „denial of service"-Angriffen soll als Maßnahme implementiert werden (M13). Außerdem soll in Betracht gezogen werden Maßnahmen zu ergreifen, um bösartige Datenübertragungen oder Abläufe zu erkennen (M15).

Weitere Maßnahmen betreffen den Schutz der Software auf Steuergeräten des Kraftfahrzeugs. Hierfür sollen Maßnahmen in Betracht gezogen werden, die vor Schadsoftware und Viren für eingebettete Systeme schützen (M14). Weiterhin soll ein sicherer Softwareupdateprozess vorhanden sein (M16); dieser wird noch einmal ausführlich in der UNECE-Regelung 156 beschrieben. Generell soll die Software auf IT-Sicherheit geprüft, authentisch und ihre Integrität geschützt sein (M21). Sicherheitsmaßnahmen sollen dabei das Risiko beim Einsatz von Drittanbietersoftware minimieren (M21). Besonders geschützt werden sollen Systeme mit Fernzugriff (M20) und externe Schnittstellen (M22).

Fraglich ist, weshalb in der UNECE-Regelung 155 die Minderungsmaßnahme M17 nicht beschrieben ist. Hier besteht eine Lücke hinsichtlich der zu treffenden Maßnahmen.

Tabelle 3 gleicht die im vorherigen Abschnitt abgeleiteten Schutzziele mit den vorgeschlagenen Maßnahmen der UNECE-

104 UNECE-Regelung 155, Anhang Teil B Minderungsmaßnahmen, Tabelle B1-C3.

Tabelle 3

	TA01	TA02	TA03	TA04	TA05	TA06	TA07	TA08	TA09	TA10	TA11
M1	+	+	+	+		(+)				+	+
M2	+	+	+	+						+	
M3	+	+	+	+		(+)			+	+	
M4	+	+	+	+		(+)			+	+	
M5	+		+				+	+		+	
M6	+	+	+	+	+	(+)			+	+	
M7	+		+							+	
M8	+	+	+	+				+		+	
M9			+			(+)				+	
M10		+	+							+	
M11	+			+						+	
M12	+									+	
M13					+	(+)			+	+	
M14		+		+					+	+	
M15					+	(+)				+	
M16		+	+			(+)			+	+	
M17	–	–	–	–	–	–	–	–	–	–	–
M18						(+)				+	
M19						(+)					
M20			+							+	
M21	+	+		+	+					+	
M22			+							+	
M23	+	+	+	+					+	+	
M24	+	+									

Regelung 155 ab, um mögliche Lücken aufzudecken. Dabei stellen die Zeilen die Minderungsmaßnahmen aus der UNECE-Regelung und die Spalten die vorgeschlagenen Kategorien des vorherigen Kapitels dar.

Beim Abgleich der technischen Maßnahmen, die aus dem Rechtsrahmen abgeleitet wurden, mit den Maßnahmen, die im Anhang der UNECE-Regelung 155 erläutert werden, fällt auf, dass die UNECE-Regelung vorrangig beschreibt, welche Entitäten geschützt werden sollen (zB Backend Systeme (M1-3 und M5), Cloudsysteme (M4), externe Schnittstellen (M22) und Systeme mit Fernzugriff (M20)). Oder die Art des Angriffs ist aufgeführt, vor der geschützt werden soll (zB Maßnahmen gegen Innere Angreifer (M1), Angriffserkennung und Abwehr bei „denial of service"-Angriffen (M13), unautorisierte Zugriffe (M2), Schadsoftware und Viren (M14)). Auch variiert das Level der Detailierung zwischen den Maßnahmen zur Minderung von Bedrohungen. M23 empfiehlt etwa den Einsatz von „best practices" für die sichere Entwicklung von Hard- und Software, was sehr viele Gegenmaßnahmen beinhaltet und teilweise weitere Maßnahmen, die aufgelistet werden, umschließt. M13 hingegen richtet sich ausschließlich auf das Erkennen und Ergreifen von Gegenmaßnahmen im Falle eines „denial of service"-Angriffs.

Da die UNECE-Regelung 155 ausschließlich Cybersicherheitsbedrohungen adressiert, sind technische Maßnahmen nur teilweise abgedeckt. So werden zwar Maßnahmen zur vertraulichen Übertragung und Speicherung von personenbezogenen Daten berücksichtigt, doch Transparenz, Intervenierbarkeit, das Verschleiern der Identität oder das sichere Löschen in Verbindung mit personenbezogenen Daten und damit Anforderungen, die sich aus der DS-GVO ableiten lassen, werden nicht betrachtet. Transparenz ist nicht gegenüber der fahrzeugführenden Person, sondern nur gegenüber dem Betreiber der IT-Infrastruktur (Kraftfahrzeughersteller) wichtig, um etwa Zugriffe zu dokumentieren oder Softwareänderungen zu protokollieren. Datenschutz wird nur in M5 betrachtet, wenn es um den Schutz vor Datenpannen geht. Diese Maßnahme kann jedoch sehr weit ausgelegt werden und umfasst nicht zwangsläufig die Anonymisierung von Daten oder den Schutz gegenüber dem Kraftfahrzeughersteller. Hingegen legt die UNECE-Regelung einen Fokus auf organisatorische Maßnahmen wie die Nachverfolgbarkeit und Dokumentation von Aktionen und ein Rechte- und Rollenmanagement. Die Absicherung des Zugriffskontrollsystems und der Zugriffskontrolle wird mehrmals aufgeführt (M2, M7, M9, M18, M19, M20). Insbesondere bei Zugriffen durch verschiedene Entitäten spielt das Zugriffskontrollsystem eine entscheidende Rolle, etwa bei Zugriffen durch freie Werkstätten, Drittanbieter von Infotainment-Anwendungen oder Fahrzeugvermietungen (vgl. unter V. 3.). Zudem fällt auf, dass Schutzmaßnahmen zur aktiven Überwachung der Sicherheit (Intrusion Detection Systeme) nur zurückhaltend angesprochen werden: „Maßnahmen zur Erkennung schädlicher interner Nachrichten oder Aktivitäten sind zu erwägen" (M15).

VI. Fazit und Ausblick

Automatisierte und vernetzte Kraftfahrzeuge drängen immer weiter in unseren Alltag vor. Autonome Kraftfahrzeuge stellen indes noch immer eher eine Vision denn Realität dar und die Euphorie früherer Jahre hat sich deutlich abgekühlt. Die technische Entwicklung schreitet jedoch mit schnellen Schritten voran und auch die rechtliche Entwicklung versucht hier Schritt zu halten oder sogar erst Technikentwicklungen zu ermöglichen. Mit Blick auf die gesellschaftliche Relevanz des Themas ist es notwendig, dass Recht und Technik nicht nebeneinander und womöglich gegeneinander laufen, sondern sich ergänzen und wenn nötig auch begrenzen oder aber Raum für Weiterentwicklung bieten. Unter II. und III. dieses Beitrags wurden die aktuellen rechtlichen Entwicklungen für Kraftfahrzeuge mit autonomer Fahrfunktion mit einem Fokus auf die Regelungen zur Datenverarbeitung (§ 1g StVG) und zur Cybersicherheit dargestellt. Insbesondere die Anforderungen aus der AFGBV sowie der UNECE-Regelung 155 und UNECE-Regelung 156 wurden herausgearbeitet. Dabei wurden die Neuregelungen dahingehend untersucht, welche Auswirkungen diese für Kraftfahrzeughersteller und kraftfahrzeughaltende Personen haben und welche datenschutzrechtlichen Anforderungen primär aus der DS-GVO in diesem Zusammenhang beachtet werden müssen.

Darauf aufbauend konnten unter V. konkrete technische Anforderungen und auch Maßnahmen zum Schutz personenbezogener Daten und zur Gewährleistung der Cybersicherheit definiert werden. Durch die Darstellung der rechtlichen und technischen Anforderungen für eine vertrauenswürdige IT, die Datenschutz und security Aspekte gleichermaßen berücksichtigt, ergibt sich ein – die neue Rechtslage und den Stand der Technik umfassendes – Gesamtbild für den Bereich der Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung.

Bezüglich der einzelnen neuen Vorgaben und Regelungen, welche sich aus der Novellierung des StVG, der AFGBV und den UNECE-Regelungen ergeben, sollte indes im Detail geprüft werden, wie und ob diese in der Praxis umsetzbar sind. Die Pflichten aus UNECE-Regelung 155 sollten zB die gesamte Lieferkette umfassen und dementsprechend auch Zulieferfirmen mitberücksichtigen. Da für die Cybersicherheit eines Kraftfahrzeugs dessen Gesamtsystem betrachtet werden muss, gehören hier auch Cloud-Services mit eingeschlossen. Inwiefern die Neuerungen hier ausreichend klar und praktisch umsetzbar sind, erscheint bisher noch wenig detailliert geklärt. Die Vorgaben in der UNECE-Regelung 156 bezüglich des Zurücksetzens auf einen vorherigen Softwarestand stellen darüber hinaus auch technische Vorgaben dar, welche, entgegen der sonst eher dynamisch wirkenden Regelung, relativ detaillierte Pfade vorgeben.

Im technischen Teil des Beitrags (s. unter V.) wurden die technische Anforderungen (TA) aus der rechtlichen Analyse der deutschen Rechtsnormen zum autonomen Fahren, insbesondere aus § 1g StVG und AFGBV, abgeleitet und diese den rechtlichen Anforderungen tabellarisch zugeordnet. In einem umfassenden Maßnahmenkatalog zur Absicherung im vernetzten und automatisierten Fahren wurden anwendungsnahe Umsetzungsvorschläge vorgestellt, die die abgeleiteten TA adressieren. Dabei ist jedoch festzuhalten, dass diese Vorschläge bewusst generisch gehalten sind, um sie in möglichst vielseitigen Szenarien und Fahrzeugarchitekturen einsetzen zu können und durch ihre Abstraktion eine gewisse Zukunftstauglichkeit aufweisen. Sie sind zudem nur beispielhaft und keineswegs als umfassend zu verstehen, um hier die Hersteller nicht in ihrer Umsetzung einzuschränken. Unter V.3. sind dann die abgeleiteten TA noch den Maßnahmen der UNECE-Regelung 155 gegenübergestellt worden. Der Abgleich mit der UNECE-Regelung 155 zeigt auf, dass die hier vorgeschlagenen Maßnahmen nicht allein die Anforderungen an die IT-Sicherheit von Kraftfahrzeugen abbilden.

Zur umfangreichen Analyse der Thematik bedarf es einer holistischen Betrachtung der Kraftfahrzeugarchitektur, die, wie im vorliegenden Beitrag, Datenschutzaspekte und Informationssicherheit (security) berücksichtigt, aber zusätzlich auch die Betriebssicherheit (safety) einbezieht. Hier bestehen Anknüpfungspunkte für weiter notwendige Forschung.

Schnell gelesen ...

- Die StVG-Novelle im Juli 2021 hat u.a. das Recht der Datenverarbeitung in automatisierten und autonomen Fahrzeugen fachspezifisch angepackt.
- Die Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften (AFGBV) soll diese abstrakten Maßgaben im Detail umsetzen.
- Der Ansatz ist zu begrüßen, lässt aber nicht wenige Fragen und Probleme im Detail offen.
- Der neue Rechtsrahmen erlaubt die Ableitung umfangreicher technischer Anforderungen und eines beispielhaften Maßnahmenkatalogs.
- Die technischen Anforderungen können von den in durch UNECE-Regelungen vorgeschlagenen Maßnahmen nur teilweise abgedeckt werden und zeigen insbesondere im Hinblick auf den geforderten Datenschutz Lücken auf.
- Der vorliegende Beitrag versucht, aus technischer wie rechtlicher Sicht einen Beitrag zur weiteren Fortentwicklung zu leisten.

Professor Dr. Clemens Arzt
ist Professor für Staats- und Verwaltungsrecht und Recht der Fahrzeugautomatisierung an der HWR Berlin und Gründungsdirektor des Forschungsinstituts für öffentliche und private Sicherheit (FÖPS Berlin).

Steven Kleemann, LL.M.,
ist Wissenschaftlicher Mitarbeiter am Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) und Doktorand an der Universität Potsdam.

Christian Plappert, M.Sc.,
ist Wissenschaftler am Fraunhofer Institut für Sichere Informationstechnologie (SIT) und forscht an neuen Sicherheitskonzepten von Fahrzeugen mit Hilfe von Trusted Computing Technologien.

Dr. Roland Rieke
ist Wissenschaftler am Fraunhofer Institut für Sichere Informationstechnologie (SIT) mit seinem Forschungsschwerpunkt Entwurfsprinzipien für sichere, skalierbare Systeme sowie modellgestützte prädiktive Sicherheitsanalysen in vernetzten Fahrzeugen.

Daniel Zelle, M.Sc.,
ist Wissenschaftler am Fraunhofer Institut für Sichere Informationstechnologie (SIT) und forscht an der Analyse und dem Entwurf neuer Sicherheitsprotokolle für die Kommunikation innerhalb von Fahrzeugen als auch mit deren Infrastruktur.

Die Ausarbeitung geht auf gemeinsame Untersuchungen im Forschungsprojekt VITAF zurück, das vom BMBF bis 2022 gefördert wurde (Förderkennzeichen: 16KIS0839).
Kapitel V wird im Wesentlichen von den Autoren Plappert, Rieke und Zelle (Fraunhofer SIT) verantwortet; Kapitel I bis IV von den Autoren Arzt und Kleemann (HWR/FÖPS Berlin). Der Gesamttext ist in enger Abstimmung aller Autoren entstanden, die Redaktion lag bei Steven Kleemann.

Schnittstelle: IT · Medien
TK · Digitalisierung.

Legal Tech, Smart Contracts, Games, Cybersecurity, Datenschutz u.v.m.

Die MMR ist interdisziplinär wie keine andere Zeitschrift im Recht der neuen und innovativen Medien. Hier finden Sie Informationen zu einschlägigen Themen, die unabdingbar miteinander im Kontext der Digitalisierung verbunden sind. Die MMR bildet die perfekte Schnittstelle zwischen »Recht – IT – KI – Digitalisierung – Medien – TK«. Profitieren Sie vom gesamten Spektrum digitaler Themen, darunter:

- IT- und Softwarerecht
- Big-Data- und Cloud-Anwendungen
- Online-Plattformen und -Handel
- Innovative Beratungs- und Geschäftsmodelle
- Digitalisierung von Behörden und Justiz
- Blockchain, Algorithmen, KI und Robotik
- Plattform-Ökonomie und Intermediäre.

3 Hefte gratis

Kostenloses Schnupperabo:

beck-shop.de/go/MMR

Erhältlich im Buchhandel oder bei:
beck-shop.de | Verlag C.H.BECK oHG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 141405

C.H.BECK

Datenschutz
im Fokus.

ZD – Die Datenschutz-Zeitschrift bei C.H.BECK

Die ZD informiert umfassend über datenschutzrechtliche Aspekte aus allen Rechtsgebieten im nationalen, europäischen und internationalen Kontext. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B.
▪ Datentransfer in Drittstaaten ▪ Konzerndatenschutz ▪ Beschäftigtendatenschutz ▪ Datenschutz-Folgenabschätzung ▪ Compliance ▪ Kundendatenschutz ▪ Soziale Netzwerke ▪ Vorratsdatenspeicherung ▪ Informationsfreiheit ▪ Profiling und Scoring ▪ Tracking ▪ Bußgelder und Sanktionen ▪ Gesundheitsdatenschutz/eHealth ▪ Big-Data-Anwendungen ▪ Datenhandel ▪ ePrivacy.

3 Hefte gratis

Kostenloses Schnupperabo:

beck-shop.de/go/ZD

Erhältlich im Buchhandel oder bei:
beck-shop.de | Verlag C.H.BECK oHG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 158812

C.H.BECK

beck-online
DIE DATENBANK

IT-Recht, Datenschutz- und Informationsfreiheitsrecht

IT-Recht PLUS | PREMIUM

Das **PLUS**-Modul bietet Highlights wie die **MMR, Spindler/Schuster, Recht der Elektronischen Medien** und den **BeckOK Informations- und Medienrecht, Hrsg. Gersdorf/Paal.** Dazu umfassende Rechtsprechung, Gesetzestexte, Prozessformulare, Musterverträge u.v.m.

IT-Recht **PREMIUM** enthält zusätzliche renommierte Werke, darunter **Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Paschke/Berlit/Meyer/Kröner, Hamburger Kommentar Gesamtes Medienrecht** und **Bräutigam/Rücker, E-Commerce** u.v.m.

beck-shop.de/29202 ▸ schon ab **€ 90,–/Monat***

Datenschutz- und Informationsfreiheitsrecht PLUS | PREMIUM

Im **PLUS**-Modul enthalten sind u.a. **ZD – Zeitschrift für Datenschutz, Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, BeckOK Datenschutzrecht, Hrsg. Wolff/Brink.** Inklusive Rechtsprechung, Gesetzestexte, zahlreiche Formulare und Lösungen für die Unternehmenspraxis.

Das **PREMIUM**-Modul bietet zusätzlich weitere Werke wie **Ehmann/Selmayr, Datenschutz-Grundverordnung, Kühling/Buchner, DS-GVO/BDSG** und **Taeger/Gabel, DSGVO – BDSG – TTDSG** u. a.

beck-shop.de/11249239 ▸ schon ab **€ 63,–/Monat***

* Preise für bis zu 3 Nutzer, zzgl. MwSt., 6-Monats-Abo

JETZT
4 Wochen
kostenlos
testen
beck-online.de

facebook.com/verlagchbeck | twitter.com/beckonlinede

C.H.BECK

Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München | 174722