

FAHRERLOS ALLE MITNEHMEN – AUTOMATISIERTE UND VERNETZTE MOBILITÄT AUS VERBRAUCHER- SICHT

aktualisiertes Positionspapier des Verbraucherzentrale Bundes-
verbands e.V. (vzbv)
12. Oktober 2021

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Mobilität und Reisen

Rudi-Dutschke-Straße 17
10969 Berlin

mobilitaet@vzbv.de

INHALT

I. ZUSAMMENFASSUNG	3
II. DIALOG- UND BETEILIGUNGSSTRATEGIE	5
III. ETHIKGRUNDSÄTZE	6
IV. HAFTUNG BEIM AUTONOMEN FAHREN	8
V. MOBILITÄTSDATENGESETZ	9
1. Mobilitätsdaten zum Gemeinwohl	11
2. Zugang zu Fahrzeugdaten.....	12
3. Nutzung anonymisierter Daten	13
4. Kontrolle über personenbezogene Daten.....	13
4.1 Personal Identity Management System (PIMS).....	13
4.2 Datentreuhänder.....	15
5. Datenraum Mobilität.....	16

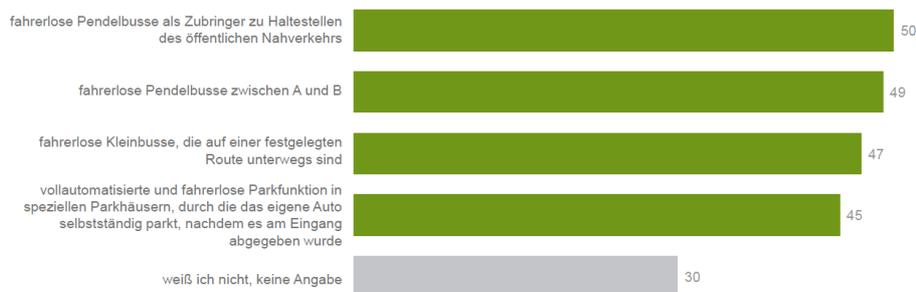
I. ZUSAMMENFASSUNG

Fahrerlose Fahrzeuge, App-basierte intermodale Mobilität sowie miteinander und/oder mit der Infrastruktur vernetzte Verkehrsmittel haben das Potenzial, den mobilen Alltag für Verbraucher:innen grundlegend zu verändern. Die Digitalisierung der Mobilität kann ein wichtiger Treiber für den aus Klimaschutzgründen notwendigen Mobilitätswandel¹ sein. Die Herausforderungen, die durch die Veränderung ihrer Mobilität auf die Verbraucher:innen zukommen, sind enorm. Routinen können aufbrechen, aber auch Sicherheiten. Neue Optionen können entstehen, aber auch neue Risiken.

Eine repräsentative Umfrage im Auftrag des Verbraucherzentrale Bundesverbands (vzbv) hat ergeben, dass sich eine große Mehrheit der Menschen sehr gut vorstellen kann, Angebote mit fahrerlosen Fahrzeugen zu nutzen.

Gewünschte Nutzung von Angeboten mit autonomen Fahrzeugen

Jeweils etwa jeder Zweite würde fahrerlose Pendel- bzw. Kleinbusse oder eine vollautomatisierte Parkfunktion in speziellen Parkhäusern nutzen. Drei von zehn würden allerdings keine dieser Angebote nutzen bzw. sind sich unschlüssig.



Frage: Welche der folgenden Angebote mit selbststeuernden, also fahrerlosen Fahrzeugen würden Sie nutzen wollen?
Darstellung: Angaben in Prozent, Mehrfachnennungen möglich

Die Vergangenheit hat gezeigt, dass grundlegende Veränderungen nicht im bekannten Modus gelöst werden können, sondern gesamtgesellschaftlich verantwortet werden müssen. Deshalb ist der Zeitpunkt gekommen, um **mehr Mitsprache bei der Gestaltung von Mobilitätsszukünften**² zu wagen. Die Einführung autonomer Fahrzeuge in den Verkehr muss mit einer Dialog- und Beteiligungsstrategie, wie sie die Nationale Plattform Zukunft der Mobilität vorgeschlagen hat³, begleitet werden. Anderenfalls gehen grundlegende Neuerungen in jeder Hinsicht an den Menschen vorbei.

Die Bundesregierung hat bereits im Jahr 2016 und in diesem Jahr gesetzliche Regelungen zum automatisierten und autonomen Fahren erlassen. Deutschland ist damit weltweit das erste Land, das sein Verkehrsrecht auf automatisierte und autonome Fahrzeuge anpasst und den Fahrzeugführenden durch ein automatisiertes System ersetzt. Die Ausgestaltung dieser gesetzlichen Regelungen sind stark industriegetrieben und

¹ In diesem Papier wird von Mobilitätswandel gesprochen, um deutlich zu machen, dass es sich um einen umfassenden Wandel auf mehreren Ebenen und entlang unterschiedlicher Pfade handelt.

² Konzepte zukünftiger Mobilität werden nicht nur individuell, sondern auch lokal stärker differenzieren und auf die Bedürfnisse der Nutzer:innen angepasst.

³ NPM: Zwischenbericht AG3: Gesellschaftliche Dialog- und Beteiligungsstrategie zur Gestaltung digitalisierter Mobilität, 2020, <https://www.plattform-zukunft-mobilitaet.de/wp-content/uploads/2020/12/20201210-NPM-Bericht-AG3-GD-final.pdf>, 29.04.2021.

vernachlässigen in weiten Teilen die Verbraucherperspektive. Besonders vom neuesten Gesetz zum „**autonomen Fahren in bestimmten Betriebsbereichen**“ haben fast zwei Drittel der Bevölkerung nicht mitbekommen, dass es überhaupt beschlossen wurde.⁴ Darüber hinaus lässt es viele Fragen offen, zum Beispiel hinsichtlich etwaiger privater Fahrzeughalter:innen und Nutzer:innen, insbesondere wenn es um die Rolle der Technischen Aufsicht sowie um Abgrenzungsfragen bei der Benutzung von Fahrzeugen geht, die sowohl hochautomatisiert mit Fahrzeugführer als auch autonom (in bestimmten Betriebsbereichen) mit Passagieren unterwegs sein können.⁵ Der **Anwendungsbereich** der Regelungen zum autonomen Fahren hätte sich nach Auffassung des vzbv zunächst ausdrücklich **nur auf gewerbliche Fahrzeughalter beschränken sollen, also zum Beispiel auf Unternehmen, die mit fahrerlosen Shuttles Personen befördern**. Es sollte eine Kommission eingerichtet werden, die die **Überarbeitung der Haftungsregeln** bei automatisierten, autonomen und vernetzten Fahrzeugen zur Aufgabe hat.

Der **faire Zugang zu Fahrzeug- und Mobilitätsdaten (Vernetzung)** ist entscheidend, um Verbraucher:innen Mobilitätsmehrwerte (zum Beispiel einfache intermodale Buchungen) zu bieten sowie die Verkehrseffizienz zu steigern und den Verkehr intelligenter zu steuern. Fahrzeughersteller sollten verpflichtet werden, Fahrzeughalter:innen sämtliche Fahrzeugdaten zur Verfügung zu stellen, die relevant für den sicheren Betrieb, die effiziente Nutzung der Fahrzeuge oder auch die Erbringung von Mobilitätsdienstleistungen sind. Dies sollte auf eine möglichst transparente und für Fahrzeughalter:innen vollständig kontrollierbare Weise geschehen. Fahrzeughersteller und Beförderungsunternehmen sollten keinesfalls darüber entscheiden dürfen, welche Daten sie zu teilen bereit sind und welche nicht („Gatekeeper“-Funktion). Sämtliche Daten, die während des autonomen Fahrens verarbeitet werden, sollten in standardisierten Formaten und über standardisierte Schnittstellen verfügbar gemacht werden. Dafür müssen sich nicht nur die EU-Kommission, sondern auch die Bundesregierung auf europäischer Ebene stark machen.⁶

Mobilitätsdaten müssen grundsätzlich **anonymisiert** werden und an den Anonymisierungsprozess müssen klare Anforderungen formuliert sowie weiterführende Schutzkonzepte, die das Risiko einer De-Anonymisierung verringern, entwickelt werden. Hierbei können neue Datenintermediäre, wie „Datentreuhänder“ oder „Personal Information Management Systems“ (PIMS), helfen. Für diese braucht es einen gesetzlichen Rahmen, der sicherstellt, dass sie unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse an der Verwertung der im Auftrag der Verbraucher:innen verwalteten Daten agieren und somit Interessenkonflikte ausgeschlossen werden. Hierfür sollte sich die Bundesregierung im Rahmen der Verhandlungen zum europäischen Data Governance Act⁷ einsetzen.

⁴ 63 Prozent der Befragten, so eine repräsentative Umfrage im Auftrag des vzbv durch Kantar zum Thema Autonomes Fahren im September 2021. Abrufbar unter: <https://www.vzbv.de/sites/default/files/2021-10/vzbv%20-%20Autonomes%20Fahren%20-%20Infografiken.pdf>

⁵ Vgl. vzbv: Stellungnahme: Fahrerlose Mobilität, aber sicher und nutzerfreundlich, 2021, S. 6 f., <https://www.vzbv.de/dokument/fahrerlose-mobilitaet-aber-sicher>, 29.04.2021.

⁶ Im Rahmen des Delegierten Rechtsakts für „Cooperative Intelligent Transport Systems“ (C-ITS).

⁷ Vorschlag für eine Verordnung des Europäischen Parlaments und Rates über europäische Daten-Governance (Daten-Governance-Gesetz), 2020/0340/COD.

Die Nutzung von öffentlich-rechtlich und privatwirtschaftlich bereitgestellten Daten setzt ein hohes Vertrauen der Nutzer:innen voraus. Nur bei einer entsprechend hohen Akzeptanz in der Bevölkerung können neue Verkehrsformen etabliert werden. Es kommt daher entscheidend auf die Nutzerperspektive an. Vor diesem Hintergrund sollte der **Datenraum Mobilität** einen **Verbraucherbeirat** erhalten, der bei allen verbraucherrelevanten Vorhaben konsultiert werden muss.

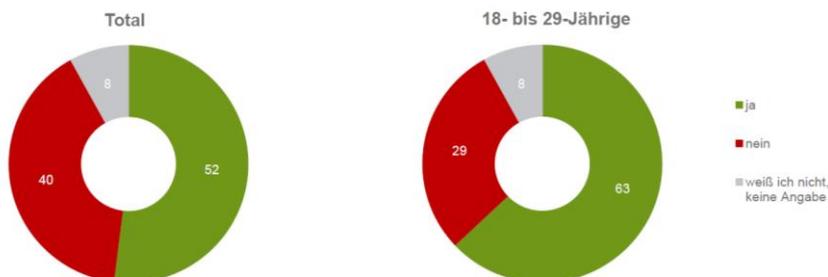
II. DIALOG- UND BETEILIGUNGSSTRATEGIE

Innovationen, die sich so unmittelbar auf die Lebensbedingungen auswirken, wie Automatisierung von Fahrzeugen und Verkehrssystemen und die Vernetzung zwischen Verkehrsträgern, benötigen eine starke Unterstützung seitens der Bürgerinnen und Bürger. Das Gelingen der Mobilitätstransformation ist von dermaßen großer Bedeutung, dass es an der Zeit ist, die bekannten Verfahren der politischen Entscheidungsfindung (Anhörungen, Stellungnahmen, Plattformen usw.) durch **innovative und zukunftsweisende Beteiligungsformate** auf nationaler und auf lokaler Ebene zu ergänzen.

Eine knappe Mehrheit der Verbraucher:innen wünscht sich, dass die Bundesregierung die Bevölkerung stärker an den politischen Maßnahmen im Bereich Autonomes Fahren beteiligt. Dieser Wunsch ist mit 63 Prozent gerade bei den Befragten unter 30 Jahren besonders hoch. Das ist nicht verwunderlich, sind das doch die zukünftigen Nutzer:innen solcher Fahrzeuge.

Stärkere Beteiligung der Bevölkerung an den politischen Maßnahmen im Bereich autonomes Fahren

Gut die Hälfte der Befragten würde eine stärkere Beteiligung der Bevölkerung an den politischen Maßnahmen im Bereich autonomes Fahren begrüßen. Bei den Jüngeren sind sogar fast zwei von drei Befragten dafür.



Frage: Würden Sie es begrüßen, wenn die Bundesregierung die Bevölkerung stärker an den politischen Maßnahmen im Bereich „selbststeuernde, also fahrerlose Fahrzeuge“ beteiligt?
Darstellung: Angaben in Prozent
Basis: Alle Befragten (n = 1.033)

Die Gestaltung zukünftiger Mobilität ist ein Thema mit einer starken Dynamik und hohen Komplexität. Einzelne können nur schwer den Überblick behalten und geraten zunehmend in eine passive Rolle, bei denen oftmals Unverständnis aufbricht, wenn sie mit Veränderungen konfrontiert werden. Durch die Möglichkeit, von Anfang an bei der Gestaltung ihrer Mobilitätsoptionen beteiligt zu werden und alle wichtigen Fakten zu kennen, kann zunehmend sichergestellt werden, dass neue Konzepte und Produkte den Bedürfnissen und Anforderungen der Verbraucher:innen entsprechen. Neue Beteiligungsformate, die die Bürgerinnen und Bürger in den Mittelpunkt stellen, können dank ihrer Vielschichtigkeit von Perspektiven hochwertige und kokreative Lösungen produzieren. Dabei sollen Bürgerbeteiligungen in keinem Fall andere demokratische Prozesse ersetzen, sondern ergänzen. Sie sollen Empfehlungen aus Sicht der Bürgerinnen und Bürger geben und den öffentlichen Diskurs bereichern.

Komplexe gesellschaftliche Herausforderungen können nur durch übergreifende Kooperationen gelöst werden. Gesellschaftlicher Dialog kann nur mit einer breiten Beteiligung aller Stakeholder funktionieren. Deshalb soll die Dialog- und Beteiligungsstrategie von einem breiten Bündnis von Zivilgesellschaft, Wirtschaft, Wissenschaft und Politik – der **Dialoginitiative** – getragen und begleitet werden. Mit der Dialoginitiative soll sowohl sichergestellt werden, dass das vorhandene Expertenwissen in die gesellschaftlichen Diskurse eingebracht wird als auch eigene aktive Beiträge zur Verbreitung beigetragen werden.

Als innovatives partizipatives Format bietet sich für die Debatte um Mobilitätsszukünfte ein **Bürgerrat für Mobilität** auf nationaler Ebene an. Dabei erhalten zufällig ausgewählte Personen die Gelegenheit, sich intensiv mit einer konkreten Frage auseinanderzusetzen. Der Mobilitätsrat ermöglicht das Zusammenkommen verschiedener Menschen, die unterschiedliche Erfahrungen und Einstellungen in den Rat hineinbringen. Durch die persönliche Ansprache der ausgelosten Personen können auch jene erreicht werden, die noch nicht an Beteiligungsprozessen mitgewirkt oder sich mit dem Thema noch nicht auseinandergesetzt haben. Mit der Übergabe der erarbeiteten Empfehlungen an die Bundesregierung wird die Verantwortung wieder an die politischen Entscheidungsträger zurückgegeben. Diese müssen zu den Empfehlungen Stellung nehmen.

Es braucht unterschiedliche Partizipationselemente auf unterschiedlichen politischen Ebenen, um die komplexe Herausforderung der Mobilitätstransformation bewältigen zu können. Kaskadierte Verfahren, die Beteiligung auf mehreren Ebenen integrieren, erhöhen die Wirksamkeit. Gerade die Gestaltung von Mobilitätsszukünften verlangt nach einer Übersetzung von nationalen Belangen auf die lokale Ebene sowie andersherum. Zusätzlich zu dem **nationalen Bürgerrat für Mobilität** sollten sich auf **lokaler Ebene Mobilitätsräte** mit der Gestaltung des Mobilitätssystems vor Ort auseinandersetzen und dazu konkrete Handlungsempfehlungen entwickeln.

Der vzbv fordert die Bundesregierung und die EU-Kommission auf, einen Dialog- und Beteiligungsprozess zur „Digitalisierung des Mobilitätssektors“ mit Bürgern einzuleiten. So können die Potenziale der Automatisierung und Vernetzung in der Mobilität zum Nutzen der Verbraucher:innen ausgelotet und genutzt werden.

III. ETHIKGRUNDSÄTZE

Die Medienberichterstattung ist von Bildern über fahrerlose Fahrzeuge geprägt, die auf der einen Seite das Auto als rollenden Raum für Arbeit, Spiel, Spaß und Entspannung beschreiben, auf der anderen Seite von spektakulären Unfällen mit angeschalteten Autopiloten. Gerade die ethische und rechtliche Bewältigung von so genannten Dilemma-Situationen⁸ erregt besondere Aufmerksamkeit. Dies ist keineswegs überraschend, da grundlegende Fragen, ob Maschinen statt Menschen über Schicksale entscheiden und welcher Unterschied in der gesellschaftlichen und individuellen Bewertung bei von Maschinen verursachten Unfällen bestehen sowie wie man die Maschinen programmieren sollte, angesprochen werden.

⁸ Dilemma-Situationen bei automatisierten Fahrzeugen sind dadurch gekennzeichnet, dass das System vor der Entscheidung zwischen zwei Übeln steht. Die Grundvoraussetzung für eine Dilemma-Situation ist, dass es in jedem Fall zu einem Unfall kommt, ein Ausgang ohne eine Unfallsituation kann nicht erreicht werden.

Die 2016 eingesetzte Ethik-Kommission zum automatisierten Fahren hatte zum Ziel, Antworten auf die ethischen Herausforderungen in so genannten Dilemma-Situationen zu finden sowie Leitlinien für die Programmierung automatisierter Fahrsysteme zu entwickeln. Die Kommission, unter der Leitung des früheren Bundesverfassungsrichters und jetzigen Bonner Universitätsprofessors Dr. Dr. Udo Di Fabio, setzte sich aus insgesamt 14 Vertretern der Philosophie, der Rechts- und Sozialwissenschaften, der Technikfolgenabschätzung, des Verbraucherschutzes sowie Vertretern der Automobilbranche und der Softwareentwicklung zusammen. Im Abschlussbericht formulierte die Kommission 20 ethische Regeln.⁹ Der Bericht führt einige rote Linien auf, wie die, dass autonom fahrende Fahrzeuge nicht zu einer Totalüberwachung der Menschen führen dürfen. Für die Programmierung von Algorithmen in Dilemma-Situationen hat die Ethik-Kommission Grundsätze formuliert. Während das Gremium jegliche Einbeziehung qualifizierender Informationen, wie Alter, Geschlecht, körperliche oder geistige Konstitution, in die Entscheidungsfindung ablehnte, konnte die Ethik-Kommission die Frage nach Quantifizierung „nicht in jeder Hinsicht konsensual zu Ende führen...“.¹⁰ Deshalb beinhalten die Regeln in gewissem Maße einen Widerspruch. Denn auf die Feststellung, dass eine Aufrechnung von Opfern untersagt ist, folgt die Einschränkung, dass Programmierungen, welche die Zahl von Personenschäden vermindern, vertretbar sein können. Die Uneinigkeit schon in der Ethik-Kommission weist darauf hin, dass diese Fragen einer weiteren Diskussion bedürfen.

Zwar hat die Bundesregierung auf Basis der ethischen Regeln einen Maßnahmenplan zum automatisierten Fahren verabschiedet¹¹ und auf EU-Ebene beschäftigt man sich im Rahmen des Hochrangigen Strukturierten Dialogs zum automatisierten und vernetzten Fahren („High Level Structural Dialogue“) mit ethischen Fragenstellungen, um einen einheitlichen, europaweiten Rahmen zu entwickeln. Aber die Konkretisierung von ethischen Prinzipien in der Normung und Standardisierung und verbindliche ethische Standards für die technische Gestaltung und Protokollierung sind bisher nicht festgelegt. Transparenz über den Einsatz und die Arbeitsweise von automatisierten und vernetzten Fahrsystemen herstellen - zum einen gegenüber individuell Betroffenen und zum anderen gegenüber der Öffentlichkeit – ist eine Grundvoraussetzung für Akzeptanz für den digital-getriebenen Mobilitätswandel.

Der vzbv fordert eine Neuauflage der Ethik-Kommission zum automatisierten und vernetzten Fahren, möglichst auf europäischer Ebene im Rahmen des Hochrangigen Strukturierten Dialogs zum automatisierten und vernetzten Fahren („High Level Structural Dialogue“), um ethische Grundsätze weiter zu präzisieren und Vorschläge für verbindliche ethische Standards sowie deren Kontrolle zu erarbeiten.

⁹ BMVI: Ethik-Kommission Automatisiertes und Vernetztes Fahren, Bericht Juni 2017, 2017, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile, 29.04.2021.

¹⁰ Ebenda, S. 18.

¹¹ BMVI: Maßnahmenplan der Bundesregierung zum Bericht der Ethik-Kommission, 2017, <https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/massnahmenplan-zum-bericht-der-ethikkommission-avf.pdf>, 29.04.2021.

IV. HAFTUNG BEIM AUTONOMEN FAHREN

Die Sicherheit von Autos ist zunehmend nicht mehr nur eine Frage der Hardware – also der Karosserie, Bremsen und ähnlichem – sondern auch der damit verbundenen Software in Kombination mit Updates, durch die das Sicherheitsniveau ständig angepasst werden kann. Mit steigender Automatisierung müssen deshalb Fahrzeughalter:innen, die keinerlei Einfluss auf die herstellerseitige Programmierung haben, sukzessive aus der Haftung entlassen werden. Diesem Grundsatz werden die neuesten Regelungen zum autonomen Fahren nicht gerecht, obwohl nicht nur der vzbv, sondern auch der Bundesrat bei der letzten Novelle des Straßenverkehrsgesetzes (StVG) im Jahr 2017 eine spezielle Herstellerhaftung dergestalt eingefordert hatte, in Anknüpfung an § 7 StVG „die Gefährdungshaftung proportional zum Grad der Automatisierung des Fahrsystems auf den Hersteller auszudehnen“¹². Die Halterhaftung wurde im Gegenteil ausgeweitet statt reduziert, nämlich um die Haftung für die Technische Aufsicht¹³. Denn Fahrzeughalter:innen haften in erster Linie verschuldensunabhängig im Rahmen der Gefährdungshaftung für sämtliche Schäden, unabhängig davon, ob die Technische Aufsicht oder der Autopilot den Schaden verursacht hat. Sie müssen sich deren Verschulden beziehungsweise Fehler zurechnen lassen. Dies ist ein krasser Gegensatz zum Haftungsregime des StVG, wonach die Person mit der größten Nähe zum Fahrbetrieb besonders aus dem StVG haftet.

Absurd ist außerdem, dass Fahrzeughalter:innen die Pflicht aufgedrückt wird, durch die Technische Aufsicht etwaige Unzulänglichkeiten der Hersteller aufzufangen.

Zwar regelt § 1f StVG-E die grundsätzlichen Pflichten der Halter:innen, der Technischen Aufsicht und des Herstellers eines Kraftfahrzeugs mit autonomer Fahrfunktion, die Aufteilung der Verantwortlichkeiten und der damit zusammenhängenden Haftung muss aber trennschärfer vorgenommen werden. Um die Akzeptanz der Fahrzeughalter:innen und den daraus erst resultierenden Einsatz autonom fahrender Kraftfahrzeuge sowie die gesellschaftliche Akzeptanz zu gewährleisten, sollten diejenigen in den Fokus der Haftung genommen werden, die einen maßgeblichen Einfluss auf die Sicherheit der autonomen Systeme haben. Das sind die Hersteller. Sie dürfen sich nicht ihrer Haftung entziehen, indem Fahrzeughalter:innen letztlich im Rahmen der Gefährdungshaftung für alles haften müssen. Auch der Bundesrat hat in seiner Stellungnahme völlig zu Recht angemerkt, dass die Haftung der Technischen Aufsicht oder von Hacker:innen gleich mit geregelt werden muss.¹⁴

Das Haftungsregime sollte daher auf drei Säulen basieren: **Die größte Verantwortlichkeit sollte beim Hersteller liegen**, gefolgt von der Technischen Aufsicht, die immer dann einspringt, wenn der Autopilot an seine Grenzen stößt. Subsidiär sollten Halter:innen verantwortlich sein. Die Haftung von automatisierten oder gar autonomen (Fahr-

¹² Vgl. Bundestag Drucksache 18/11534, Bundesregierung: Unterrichtung durch die Bundesregierung, Stellungnahme des Bundesrates, 2017, S. 5, <http://dipbt.bundestag.de/doc/btd/18/115/1811534.pdf>, 27.04.2021.

¹³ Fahrzeuge mit autonomer Fahrfunktion müssen nach § 1d Absatz 3 StVG-E von der Technischen Aufsicht überwacht werden. Darunter ist eine natürliche Person zu verstehen, die das Fahrzeug während des autonomen Betriebs deaktivieren und Fahrmanöver freigeben kann. Der Technischen Aufsicht kommt mithin eine grundlegende Verantwortung zu, wenn es um den sicheren Betrieb von Fahrzeugen mit autonomer Fahrfunktion geht.

¹⁴ Vgl. Bundestag Drucksache 19/28178, Bundesregierung: Unterrichtung durch die Bundesregierung, 2021, S. 17 ff., 22, <https://dserver.bundestag.de/btd/19/281/1928178.pdf>, 29.04.2021.

)Systemen darf nicht erst an der Abwicklung von Unfällen ansetzen. Das Festhalten allein an der Halterhaftung ist im Hinblick auf einen effektiven Opferschutz unzureichend. Will man Unfälle von vorneherein weitgehend ausschließen, sollte die **Gefährdungshaftung nicht mehr Halter:innen treffen, sondern die Hersteller**.¹⁵ Ein Hersteller muss im Sinne einer Gefährdungshaftung stets haften, wenn sein Produkt bei bestimmungsgemäßer Verwendung einen Schaden anrichtet.¹⁶

Außerdem sollten die Hersteller autonomer und automatisierter Fahrsysteme nicht nur verpflichtet werden, sicherheitsrelevante Updates anzubieten (so sieht es § 1f Absatz 3 StVG-E vor). Um einen möglichst gründlichen Ressourcenschutz gewährleisten zu können, sollten Hersteller auch dazu verpflichtet werden, die Fahrsysteme über die Lebensdauer des Fahrzeugs hinweg ständig umfassend zu aktualisieren (**Update-Pflicht**). Die Herstellung von Kraftfahrzeugen verbraucht zu viele Ressourcen, als dass die Autos nach wenigen Jahren verschrottet werden sollten.

Der vzbv fordert, zeitnah eine Kommission einzurichten, die die **Überarbeitung der Haftungsregeln** bei automatisierten, autonomen und vernetzten Fahrzeugen zur Aufgabe hat. Darüberhinaus muss die EU-Kommission die Produkthaftungsrichtlinie dahingehend erneuern, dass diese Art Fahrzeuge ausdrücklich erfasst werden.

V. MOBILITÄTSDATENGESETZ

Die (Unmengen von) Daten, die beim automatisierten Fahren anfallen, sind sowohl personenbezogen oder –beziehbar¹⁷ und darüber hinaus äußerst sensibel. Der Europäische Datenschutzausschuss (EDSA) hat bereits 2020 einen Entwurf von Leitlinien zur Verarbeitung personenbezogener Daten bei vernetzten Fahrzeugen und Mobilitätsanwendungen vorgelegt und weist darin auf die besondere Schutzbedürftigkeit bestimmter Datenarten hin, wie beispielsweise Standortdaten, biometrische Daten und Daten, die zu staatlichen Sanktionen führen können.¹⁸

Was Fragen des Datenschutzes betrifft, muss zum Beispiel beim neuesten Gesetz zum autonomen Fahren in bestimmten Betriebsbereichen noch geprüft werden, ob dieses nicht maßgeblich nachgebessert werden muss.¹⁹ Das gilt vor allem vor dem Hintergrund, dass das Gesetz (ohne jede Not) auch private Fahrzeughalter:innen in den Anwendungsbereich mit einbezieht. Denn insoweit sind auch die personenbezogenen Daten von privaten Fahrzeughalter:innen betroffen.

¹⁵ Zum Hintergrund und Einzelheiten dieser Forderung vgl. vzbv: Positionspapier: Fahrerlose Mobilität, aber sicher und nutzerfreundlich, 2021, S. 7 ff., <https://www.vzbv.de/dokument/fahrerlose-mobilitaet-aber-sicher>, 29.04.2021.

¹⁶ Vgl. vzbv: Positionspapier: Produkthaftung im digitalen Zeitalter, S. 4 f, https://www.vzbv.de/sites/default/files/2021-06/21-06-07_vzbv_Positionspapier%20Produkthaftung_neu.pdf.

¹⁷ Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie: Gemeinsame Erklärung der DSK und des VDA: Datenschutz bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, 2016, https://www.bfdi.bund.de/DE/Datenschutz/Themen/Reisen_Verkehr/VerkehrArtikel/Erkl%C3%A4rungDSK_VDA_NutzungVernetzterKfz.html?cms_submit=Senden&cms_templateQueryString=gemeinsame+erkl%C3%A4rung, 29.04.2021.

¹⁸ Vgl. EDPB: Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_de, 29.04.2021.

¹⁹ So auch die Stellungnahme des Bundesrates, vgl. Bundestag Drucksache 19/28178, Bundesregierung: Unterrichtung durch die Bundesregierung, 2021, S. 21, <https://dserver.bundestag.de/btd/19/281/1928178.pdf>, 29.04.2021.

Nicht-personenbezogene Daten, die aufgrund der Automatisierung der Fahrzeuge, aber auch durch die Vernetzung der Verkehrsträger generiert werden, können einen echten Mehrwert für das Gemeinwohl darstellen und sollten deshalb grundsätzlich besser verfügbar gemacht werden. Ein Vorteil des vernetzten Fahrens liegt darin, dass mittels car-to-car- und car-to-Infrastruktur-Vernetzung Verkehrssicherheit und Verkehrsfluss verbessert werden. Nicht-personenbezogene Mobilitätsdaten können darüber hinaus wertvolle Hinweise zur Infrastrukturplanung, Reduktion von Sicherheitsrisiken sowie Umweltauswirkungen, Auslastungs- und Verkehrssteuerung, aber auch für die intermodale Routeninformation bieten.

Bereits heute gibt es im Mobilitätsbereich eine Reihe von Gesetzen, die schon jetzt das Erheben, Speichern und Weiterleiten von Daten regeln, wie etwa die europäische e-Call-Verordnung²⁰, die delegierte Verordnung der EU-Kommission zur Bereitstellung EU-weiter multimodaler Reiseinformationsdienste²¹ oder die Regelungen im Straßenverkehrsgesetz (StVG), die für das automatisierte Fahren (Level 3) gelten.²² Weitere erst kürzlich erlassene Gesetze betreffen zum Beispiel die Novellierung des Personenbeförderungsgesetzes (PBefG) oder das StVG hinsichtlich des autonomen Fahrens (Level 4). Beide Gesetze warten mit umfangreichen Regelungen zur Speicherung und Weitergabe von Mobilitätsdaten auf.

Ein Rechtsrahmen, der aus vielen versprengten Einzelgesetzen besteht, kommt schnell an seine Grenzen. Diese Fragmentierung verhindert übergreifende Regelungen zur Koordination grundsätzlicher Ziele, wie etwa die der oben genannten ethischen Grundsätze. Um Verbraucher:innen in Zukunft die Möglichkeit zu geben, ihre Reisekette möglichst aus einer Hand buchen zu können, braucht es hingegen ein einheitliches Gesetz, das allgemeingültige Regeln zur Datensicherheit, zur Datennutzung sowie die Beziehungen der Unternehmen untereinander und ihre grundsätzliche Berechtigung auf den Zugriff der Daten (open-data-Ansatz) regelt und Schnittstellen und Standards definiert.

Ein umfassender Regulierungsrahmen ist notwendig, der den Zugang zu den Mobilitätsdaten, deren Anonymisierung und die Kontrolle über personenbezogene Daten regelt. Dies gilt nicht nur für den Bereich des automatisierten und autonomen Fahrens, sondern für alle Mobilitätsbereiche, in denen Daten gespeichert und weitergeleitet werden.

Ein **sektorales Datengesetz** im Bereich der Mobilität (**Mobilitätsdatengesetz**) könnte dann aus einem **allgemeinen** und einem **besonderen Teil** bestehen. Der allgemeine Teil sollte übergreifende und grundlegende Gesichtspunkte regeln, wie etwa Ethikgrundsätze, open-data-Ansatz, Pflicht zur Anonymisierung von Daten, Haftungsverteilung etc. Im besonderen Teil des Mobilitätsdatengesetzes können dann spezielle Fragen geklärt werden, etwa wie genau eine Anonymisierung zu erfolgen hat, welche konkreten Standards und Schnittstellen zum Datenteilen bei unterschiedlichen Daten (sicherheitsrelevante, fahrssystemrelevante, kommerzielle etc.) gelten sollen.

Da vernetzte Mobilität nicht vor Grenzen haltmacht und daher europaweit gedacht werden muss, fordert der vzbv die EU-Kommission auf, sich mit diesem Thema zu befassen.

²⁰ Verordnung (EU) 2015/758.

²¹ Delegierte Verordnung (EU) 2017/1926.

²² § 63a StVG.

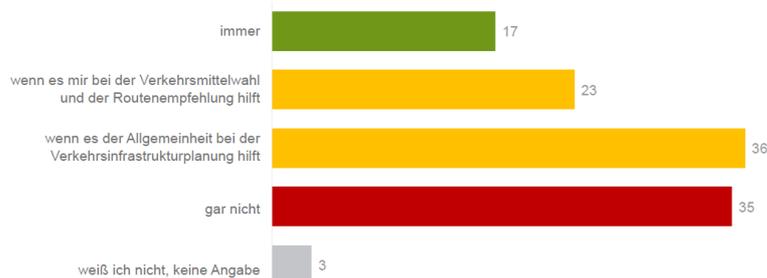
Die nachfolgend aufgeführten Aspekte sollten dabei auf jeden Fall mitberücksichtigt werden:

1. MOBILITÄTSDATEN ZUM GEMEINWOHL

Die Menschen in Deutschland sind noch am ehesten bereit, ihre Mobilitätsdaten weiterzugeben, wenn es der Allgemeinheit bei der Verkehrsinfrastrukturplanung hilft. Ein gutes Drittel ist hingegen gar nicht bereit, Mobilitätsdaten zu teilen.

Bedingungen für die Weitergabe von Mobilitätsdaten

Nur jeder Sechste ist generell dazu bereit, seine Mobilitätsdaten weiterzugeben, knapp jeder Vierte hingegen nur unter der Bedingung, dass man selbst von der Datenweitergabe profitiert, und gut jeder Dritte, wenn sie der Allgemeinheit nutzt. Ein weiteres Drittel ist generell nicht dazu bereit.



Frage: Unter welchen der folgenden Bedingungen wären Sie persönlich bereit, Ihre Mobilitätsdaten, also Daten darüber, wann Sie sich von A nach B mit welchem Verkehrsmittel bewegen, weiterzugeben?

Darstellung: Angaben in Prozent, Mehrfachnennungen möglich
Basis: Alle Befragten (n = 1.033)

Die Vorteile des automatisierten und vernetzten Fahrens in Verbindung mit der vom PBefG regulierten öffentlichen Personenbeförderung können nur ausgeschöpft werden, wenn die Mobilitätsdaten²³, unter strikter Beachtung der bestehenden datenschutzrechtlichen Vorgaben möglichst frei und schnell zwischen den beteiligten Stellen, Unternehmen wie Behörden, ausgetauscht werden können. Diesen Datenaustausch zwischen Kraftfahrzeugen, Automobilherstellern, Beförderungsunternehmen, Infrastruktur, Mobilitätsplattformen und Nutzer:innen transparent und standardisiert zu gestalten, muss Hauptaufgabe gesetzlicher Regelungen sein. Hier gilt es, einen umfassenden und vor allem einheitlichen Standard zu schaffen. Die Gesetze zum autonomen Fahren und zur Novellierung des PBefG regeln indes lediglich den Zugang zu Daten für **Gemeinwohlzwecke** (autonomes Fahren) oder **wesentlichen statischen und dynamischen Daten zu Beförderungsdienstleistungen** (PBefG). Sie sparen die Regulierung des wichtigsten Teils aus, nämlich der Daten für **kommerzielle Zwecke**. So wird ein fairer und transparenter Zugang zu Mobilitätsdaten nicht gelingen.

Indem Fahrzeughalter:innen ihre Fahrzeuge mit autonomer Fahrfunktion oder Nutzer:innen ein Personenbeförderungsmittel benutzen, fallen die begehrten Mobilitätsdaten an. Sie sollten daher auch den Fahrzeughalter:innen oder Nutzer:innen zur Verfügung stehen. Sie sollten diese Daten jedenfalls nicht etwa vom Fahrzeughersteller oder Verkehrsunternehmen zurückkaufen oder vor Gericht erstreiten müssen.

Vielmehr sollten Fahrzeughersteller verpflichtet werden, den Fahrzeughalter:innen **sämtliche** Fahrzeugdaten zur Verfügung zu stellen. Dies sollte auf eine möglichst

²³ Mobilitätsdaten umfassen Fahrzeugdaten sowie alle weiteren durch Mobilität anfallende Daten und Daten der Infrastruktur.

transparente und für die Fahrzeughalter:innen vollständig kontrollierbare Weise geschehen.²⁴ Fahrzeughersteller und Beförderungsunternehmen dürfen keinesfalls darüber entscheiden, welche Daten sie zu teilen bereit sind und welche nicht („Gatekeeper“-Funktion). Die beim autonomen (aber auch beim automatisierten) Fahren anfallenden Daten sollten lokal im Fahrzeug gespeichert oder wenn zur Förderung des Gemeinwohls notwendig (im gegenseitigen Einverständnis mit allen beteiligten Stellen) an einen bereits in der politischen Entwicklung befindlichen, für alle zugänglichen „Datenraum Mobilität“ gesendet werden.²⁵

Der vzbv fordert, dass Mobilitätsdaten nicht einzelnen Unternehmen, sondern dem **Gemeinwohl** zugutekommen müssen.

2. ZUGANG ZU FAHRZEUGDATEN

Zur Stärkung des Vertrauens in die datengetriebene Automatisierung und Vernetzung von Fahrzeugen ist ein Rechtsrahmen notwendig, der einen fairen Zugang zu Fahrzeugdaten regelt und Datenschutz sowie Datensicherheit gewährleistet. Dies gilt vor allem, wenn in Zukunft Privatpersonen Fahrzeuge mit hochautomatisierter oder autonomen Fahrfunktionen kaufen und zulassen werden. Aus Verbrauchersicht sollten **personenbezogene Daten vorzugsweise im Fahrzeug selbst gespeichert** und soweit möglich im Fahrzeug unter Kontrolle der Betroffenen verarbeitet werden. Durch eine standardisierte Softwareumgebung und einer Hardwareplattform im Fahrzeug können von Drittanbietern bereitgestellte Applikationen ausgeführt werden. Der Zugang zu Fahrzeugdaten sollte über eine so genannte Offene Telematik-Plattform (OTP), die der Verband der TÜV e.V. (VdTÜV) Anfang 2017 und Ende 2019 ins Gespräch gebracht hat²⁶, also ein sicheres Automotiv-Telematik-Gateway im Fahrzeug gewährleistet werden, die darüber hinaus gegen Angriffe und Manipulationen geschützt sein muss. Über solche Applikationen können die für die jeweiligen Dienste notwendigen Daten direkt (drahtlos) auf die Server des Drittanbieters übermittelt werden. Dabei ist keine weitere Zwischenebene in Form eines Trust Centers oder des OEM-Backends für den Datenabruf notwendig. Auch die mit § 63a StVG Absatz 3 im Fall eines Unfalls obligatorische Übermittlung von relevanten Einträgen aus dem Fahrmodusspeicher an berechnete Stellen kann auf diese Art realisiert werden.

Sollte darüber hinaus eine Auslagerung der Daten notwendig sein, sollte dies an unabhängige treuhänderische Dritte, sogenannte „Trust-Center“²⁷ erfolgen, die die Fahrzeug- und Verkehrsdaten verwalten und eine Vermittlerrolle zwischen Dateninhabern und berechtigten Dritten übernehmen. Das Konzept des Verbands der Automobilindustrie (VDA)²⁸, das einen exklusiven Zugang zu in Fahrzeugen generierten Daten über ein Hersteller-Backend ermöglicht und für Dritte über einen der Extended-Vehicle-

²⁴ Vgl. Ausführungen zu Ziff. 3. (s.u.).

²⁵ Vgl. Ausführungen zu Ziff. 4 (s.u.).

²⁶ Verband der TÜV e.V.: Remote-Zugang zu Fahrzeugdaten für hoheitliche Aufgaben zur Gewährleistung von Verkehrssicherheit und Umweltschutz im Straßenverkehr. 2019, und Anforderungen an die Telematikchnittstelle im Fahrzeug - Vertrauenswürdiger Zugang zu Fahrzeugdaten und zu von Fahrzeugen generierten Daten, 2017.

²⁷ Zur erstmaligen Forderung eines „Trust Centers“ vgl. vzbv: Positionspapier: Rechtssicher Fahren mit automatisierten Fahrzeugen, 2017, S. 14 ff., https://www.vzbv.de/sites/default/files/2016-12-30_stn_zum_gesetzentwurf_aend_stvg_final.pdf, 29.04.2021.

²⁸ VDA: NEVADA Share & Secure, <https://www.vda.de/de/themen/innovation-und-technik/datensicherheit/was-ist.html>, 29.04.2021.

Schnittstelle nachgelagerten „neutralen Server“ bereitstellt, lehnt der vzbv ab. Verbraucher:innen sollten die Möglichkeit haben, maximale Kontrolle über ihre Mobilitätsdaten ausüben zu können und frei über Datenintermediäre entscheiden zu können. Die Hersteller müssten sich dann dem Wettbewerb um das Vertrauen der Verbraucher:innen stellen.

Nach langen Verhandlungen wird die EU-Kommission im Rahmen eines delegierten Rechtsakts für „Cooperative Intelligent Transport Systems“ (**C-ITS**) zeitnah unter anderem einen EU-weiten Standard für den Fahrzeugdatenzugang vorschlagen. Die Chance den Zugang zu Daten in Fahrzeugen direkt im Fahrzeug unter Kontrolle der Verbraucher:innen zu regeln und damit Datenschutz durch Technik zu erreichen, darf nicht verpasst werden.

Sowohl die EU-Kommission als auch die Bundesregierung müssen sich auf europäischer Ebene für einen verbraucherfreundlichen, standardisierten Datenzugang bei automatisierten und vernetzten Fahrzeugen stark machen.

3. KONTROLLE ÜBER PERSONENBEZOGENE DATEN

Bei im Fahrzeug generierten Daten ist quasi immer von einem Personenbezug auszugehen, da diese durch das Fahr- und Nutzungsverhalten der Verbraucher:innen stark beeinflusst werden. Zur Durchsetzung der Anforderungen zum Schutz der personenbezogenen Daten bei automatisierter und vernetzter Mobilität ist ein umfassendes Konzept erforderlich, dass Verbraucher:innen eine informierte und selbstbestimmte Ausübung ihrer Datenhoheit ermöglicht sowie einzelnen Missbrauch bis hin zu professionell organisiertem Betrug verhindert.

Aus Verbrauchersicht müssen die **Transparenzpflichten** der Datenschutz-Grundverordnung strikt beachtet werden. Betroffene (Fahrzeughalter:innen, Nutzer:innen von Beförderungsleistungen) müssen einen leicht zugänglichen und verständlichen Überblick über die Daten erlangen können, die verarbeitet werden, bestenfalls im Fahrzeug. Über diesen umfassenden Einblick muss Verbraucher:innen die **vollständige Kontrolle** über die Daten ermöglicht werden.

4. NUTZUNG ANONYMISierter DATEN

Neben der Automatisierung ist die Vernetzung der Schlüssel zu Mobilitätsmehrwerten wie die Steigerung der Verkehrseffizienz und Verkehrssteuerung, aber auch Informationen und Buchungsmöglichkeiten für Verbraucher:innen, die intermodale Verknüpfungen von Verkehrsmitteln vereinfachen. Straßeninfrastruktur und Fahrzeuge werden durch die Vernetzung Informationen austauschen. Neue Technologien führen zu geänderten Rollenverteilungen und neuen Geschäfts- und Betreibermodellen. Diese bauen auf den Daten auf, die mit Hilfe von öffentlichen Infrastrukturen gesammelt werden. Folgerichtig muss der Begriff „öffentliches Gut“ neu definiert werden und die Daten, die im öffentlichen Raum generiert werden, zum Allgemeinwohl nutzbar gemacht werden. Keinesfalls darf dieser Datenschatz nur einer eingeschränkten Nutzergruppe zur Verfügung stehen.

Bei der Vernetzung von Fahrzeugen beziehungsweise Infrastruktur im Straßenverkehr werden neben einer stabilen Kommunikationsinfrastruktur sogenannte digitale Zwillinge (digital twins), also digitale Abbilder verkehrsrelevanter Elemente, gefordert. Digitale Abbilder der physischen Straßenverkehrsinfrastruktur können statische (zum Beispiel

Standort) und/oder dynamische Informationen (zum Beispiel Signalzustand bei Ampeln) beinhalten.²⁹ Während statische und dynamische Daten von Ampeln, Verkehrszeichen etc. zum Zwecke des Verkehrsmanagements und der Verkehrssicherheit im datenschutzrechtlichen Sinne als unkritisch anzusehen sind und möglichst in standardisierter Form allgemein verfügbar gemacht werden sollten, sind digitale Abbilder von Verkehrsteilnehmern (Autos, Fahrräder, Fußgänger:innen oder ÖV-Nutzer:innen) kritisch zu sehen. Zwar können diese Informationen gerade für die Planung und Steuerung von Verkehrsinfrastruktur herangezogen werden und damit besser nachfrageorientiert ausgerichtet werden, aber „digital twins“ von Menschen bergen ein hohes Risiko der Nachverfolgung von Routen oder der Profilerstellung von Fahrverhalten durch Dritte. Die Verfügbarmachung von diesen Daten muss deshalb an zwei Bedingungen geknüpft werden: Zum einen müssen diese Daten anonymisiert übertragen werden und an die Anonymisierung strenge Anforderungen gestellt werden; zum anderen muss die Übertragung dieser anonymisierten Daten immer freiwillig erfolgen und jederzeit widerrufbar sein.

§ 1g Absatz 1 Nr. 1 StVG-E sieht zum Beispiel vor, dass Fahrzeughalter:innen eines Kraftfahrzeugs mit autonomer Fahrfunktion verpflichtet sind, unter anderem die Fahrzeugidentifikationsnummer (FIN) beim Betrieb des Kraftfahrzeugs anlassbezogen zu speichern und unter den im Gesetz angegebenen Umständen weiterzuleiten. Alle Daten, die mit der FIN oder dem Kfz-Kennzeichen verknüpft oder verknüpfbar sind, sind jedoch bei der Nutzung von Fahrzeugen als personenbezogen und damit datenschutzrechtlich relevant anzusehen.³⁰ Um rechtliche Klarheit in dem zentralen Punkt „Datenschutz“ zu schaffen fordert der vzbv, dass – wie bereits in anderen Mobilitätsgesetzen deutschland- und EU-weit etabliert³¹ – auch beim autonomen Fahren ausdrücklich klar gestellt wird, dass **Daten mit Personenbezug** vor der Verarbeitung **anonymisiert** werden müssen, es sei denn, es dient zur Aufklärung von Unfällen. Das gilt auch für personenbezogene Daten, die nach dem Kauf bei der Inanspruchnahme von Beförderungsdienstleistungen gespeichert werden.³²

Eine solche Klarstellung dient nicht nur dem Datenschutz, sondern in erster Linie den datenverarbeitenden Unternehmen. Indem Daten anonymisiert werden, beziehungsweise von vornherein nicht personenbezogen sind, werden sie erst richtig verkehrsfähig, sodass sie mit möglichst wenig Verzögerung in Echtzeit abgebildet werden können. Erst wenn Mobilitätsdaten derart verkehrsfähig sind, kann aus deren Zusammenführung und zentraler Verarbeitung ein echter Vorteil für Verkehrssicherheit und Verkehrsfluss geschaffen und somit für das Gemeinwohl genutzt werden. Müsste bei der

²⁹ NPM: Maßnahmen zur Digitalisierung der Verkehrsinfrastruktur, 2020, <https://www.plattform-zukunft-mobilitaet.de/wp-content/uploads/2020/12/20201210-NPM-Bericht-AG3-DVI-final.pdf>, 29.04.2021.

³⁰ Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie: Gemeinsame Erklärung der DSK und des VDA: Datenschutz bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, 2016, https://www.bfdi.bund.de/DE/Datenschutz/Themen/Reisen_Verkehr/VerkehrArtikel/Erkl%C3%A4rungDSK_VDA_NutzungVernetzterKfz.html?cms_submit=Senden&cms_templateQueryString=gemeinsame+erkl%C3%A4rung, 29.04.2021.

³¹ Vgl. § 2 Nr. 12 S. 2 Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG): „Für den Fall, dass auch Daten mit Personenbezug verarbeitet werden, sollten diese anonymisiert werden.“; vgl. Erwägungsgrund 5 u. 6 zur Delegierten VO (EU) 2017/1926 der Kommission vom 31.05.2017 (zur Ergänzung der Richtlinie 2010/40/EU hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienste), wonach der EU-Gesetzgeber davon ausgeht, dass die Übermittlung personenbezogener Daten in der Regel nicht notwendig ist, um verkehrsträgerübergreifende Dienste anzubieten.

³² Vgl. vzbv: Positionspapier: Für eine Personenmobilität auf der Höhe der Zeit, S. 17 f., https://www.vzbv.de/sites/default/files/downloads/2020/12/04/21-02-22_stellungnahme_oea_pbefg_vzbv_final.pdf, 29.04.2021.

Verarbeitung jedes personenbezogenen Datums zunächst geprüft werden, ob dies datenschutzrechtlich zulässig ist, würde der Sinn und Zweck der Bereitstellung konterkariert werden.

Der vzbv fordert, dass **Mobilitätsdaten** grundsätzlich **anonymisiert** und an den Anonymisierungsprozess klare **Anforderungen formuliert** sowie weiterführende Schutzkonzepte, die das Risiko einer De-Anonymisierung verringern, entwickelt werden.

4.1 Personal Identity Management System (PIMS)

Da als personenbezogen alle Daten zu betrachten sind, die mit der Fahrzeugidentifikationsnummer (FIN) oder dem Kfz-Kennzeichen verknüpft sind, ist es aus Verbrauchersicht sinnvoll, dass Fahrzeugnutzende technische Mittel an die Hand zu bekommen, mit welchen sie zuverlässig kontrollieren können, welche öffentlichen oder kommerziellen Stellen welche Daten für welchen Zweck für welchen Zeitraum zur Nutzung erhalten. Dies kann zum Beispiel durch ein Personal Identity Management System (PIMS)³³ geschehen. Bei PIMS handelt es sich um eine Technik, mit der Betroffene in die Lage versetzt werden, über die Erhebung und Weitergabe ihrer personenbezogenen Daten Kontrolle auszuüben. Kerngedanke dieses Konzeptes ist, einzelne Verbraucher:innen in das Zentrum des Datenmanagements zu stellen, ohne dass diese bei jedem Fahrtantritt erneut eine komplizierte Datenschutzeinstellung vornehmen müssen. Sie geben ihre Datenschutzpräferenzen vielmehr einmalig beispielsweise in eine App auf seinem Smartphone ein. Das datengetriebene, autonome respektive vernetzte Fahrzeug ruft diese Datenschutzeinstellung vor der Fahrt vom Smartphone ab (beispielsweise per Bluetooth/Near Field Communication) oder die App des Beförderungsunternehmens beziehungsweise der Mobilitätsplattform übernimmt die Datenschutzeinstellungen.

4.2 Datentreuhänder

Darüber hinaus sollten **Regelungen für treuhänderische Datenmittler** geschaffen werden. Nur so kann das Ziel erreicht werden, mithilfe dieser Datenmittler die Verarbeitung beziehungsweise den Austausch von notwendigerweise zu erhebenden persönlichen Daten zu erleichtern, ohne dabei Abstriche beim Schutz der personenbezogenen Daten der Betroffenen machen zu müssen. Um die Risiken zu begrenzen, die mit der zentralen Rolle der Datenmittler einhergehen, und gleichzeitig das Vertrauen in diese Organisationen zu erhöhen, sollte ein obligatorisches Zertifizierungssystem für diese Dienste geschaffen werden.³⁴

Ferner sollten bei einer gesetzlichen Regelung nicht nur Daten aus Kraftfahrzeugen mit autonomen Fahrfunktionen berücksichtigt werden, sondern aus allen Neufahrzeugen (Pkw, Lkw, Bussen, usw.), um die Verkehrsanalyse auf eine möglichst breite Basis stellen und die Verkehrssicherheit damit um ein Maximum erhöhen zu können.

Der vzbv fordert einen gesetzlichen Rahmen, der sicherstellt, dass neue Datenintermediäre, wie „Datentreuhänder“ oder „Personal Information Management Systems“

³³ Zu den Anforderungen an PIMS vgl. vzbv: Positionspapier: Neue Datenintermediäre - Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder, 2020, https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf, 29.04.2021.

³⁴ Zu den Anforderungen an Datenmittler vgl. vzbv: Positionspapier: Neue Datenintermediäre - Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder, 2020, a.a.O.

(PIMS), **unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse** an der Verwertung der im Auftrag der Verbraucher:innen verwalteten Daten agieren und somit Interessenkonflikte ausgeschlossen werden.³⁵ Hierfür sollte sich die Bundesregierung im Rahmen der Verhandlungen zum europäischen Data Governance Act einsetzen.³⁶

5. DATENRAUM MOBILITÄT

Ein Mobilitätsdatengesetz würde die rechtlichen Voraussetzungen, Konkretisierungen und damit Rechtssicherheit für alle Beteiligten schaffen. Für die Umsetzung dieses rechtlichen Rahmens ist aber eine Institution erforderlich, in der zum einen Mobilitätsdaten zusammenlaufen und ihrer Bestimmung gemäß verarbeitet und zum anderen Regeln für den Datenaustausch zwischen Unternehmen, Behörden, Wissenschaft und Verbraucher:innen vereinbart, umgesetzt und deren Einhaltung überprüft werden. Im Auftrag des Bundesverkehrsministeriums ist in diesem Jahr ein Datenraum Mobilität (Mobility Data Space (MDS)) entwickelt und geschaffen worden, in dem alle Anbieter im Mobilitätsmarkt, öffentliche und private Gesellschaften für Mobilität auf Straße, Schiene und in der Luft Daten auf Augenhöhe teilen können, um Mehrwert für ihre Kunden zu schaffen. Darüber hinaus muss der Datenraum genutzt werden, um den Datenaustausch zur Förderung von Gemeinwohlinteressen voranzubringen. Maßstab aus Verbrauchersicht ist die Möglichkeit, Mobilität mit wenigen Klicks organisieren zu können. Der Übergang zur digital getriebenen intermodalen und energieeffizienten Mobilität muss für Verbraucher:innen einfach gestaltet werden, das heißt: Zugangshürden müssen abgebaut und Alternativen überzeugend attraktiv werden. Erst wenn sich Verbraucher:innen über die Mobilitätsplattform ihrer Wahl umfassend über das Angebot an Mobilitätsdienstleistungen informieren und das für den Anlass geeignete oder in Kombination beste Verkehrsmittel bequem buchen und bezahlen können, kann der notwendige Mentalitätswandel und die Erosion der engen Beziehung vieler Verbraucher:innen zum Auto vorangebracht werden.

Private Mobilitätsanbieter beispielsweise, die auf die Sammlung großer Datensätze für die Fortentwicklung ihres Produkts angewiesen sind, geben die von ihnen gesammelten Daten nur ungern ab, da sie fürchten, den selbst erarbeiteten Vorteil und die direkte Zusammenarbeit mit Kund:innen aufgeben zu müssen. Öffentliche Mobilitätsanbieter wiederum, die bereits jetzt ihre Daten für die Zusammenarbeit mit Kommunen zugänglich machen müssen, müssen somit auch nicht um ihre Stellung im Wettbewerb bangen. Und Kommunen, die ihr Mobilitätskonzept stetig weiterentwickeln wollen und sollen, sind auf die Daten von Mobilitätsanbietern angewiesen.

Nur auf Basis einer erfolgreichen Zusammenarbeit kann der Datenraum Mobilität Fortschritte erreichen. Der Expertenbeirat des MDS sollten einen Verbraucherbeirat zur Seite gestellt bekommen, der bei allen verbraucherrelevanten Vorhaben konsultiert werden muss. Der Verbraucherbeirat sollte anlassbezogen mündliche und schriftliche Rechenschaftsberichte des MDS zu speziellen Themen einfordern und zu speziellen

³⁵ Zu den Kernpositionen des vzbv bezüglich der Anforderungen an PIMS und Datenmittler vgl. vzbv: Positionspapier: Neue Datenintermediäre - Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder, 2020, S. 3, a.a.O.

³⁶ Vgl. auch Stellungnahme des vzbv: Vertrauen stärken durch verbraucherfreundliche Daten-Governance (2021). S. 8ff. URL: https://www.vzbv.de/sites/default/files/downloads/2021/01/13/21-01-12_vzbv-stellungnahme_data-governance-act.pdf [Zugriff: 20.04.2021]

Fragestellungen Studien und Gutachten in Auftrag geben können. Der Beirat muss hierfür mit einem entsprechenden Budget ausgestattet werden.

Die Nutzung von öffentlich-rechtlich und privatwirtschaftlich bereitgestellten Daten setzt ein hohes Vertrauen der Nutzer:innen voraus. Nur bei einer entsprechend hohen Akzeptanz in der Bevölkerung können neue Verkehrsformen etabliert werden. Es kommt daher entscheidend auf die Nutzerperspektive an.

Sollte der freiwillige Ansatz des Datenraums Mobilität mit Unterstützung des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) scheitern, sollten alle Anbieter per Gesetz dazu verpflichtet werden, ihre Daten zur Verfügung zu stellen, um durch das Zusammenfügen aller Daten ein optimales Mobilitätsangebot in Stadt und Land zu gewährleisten