MOBILITÄTSDATENWÄCHTER – DIGITALE PRIVATHEIT BEI VERNETZTEN FAHRZEUGEN FÜR ALLE VERBRAUCHER:INNEN GEWÄHRLEISTEN

Positionspapier des Verbraucherzentrale Bundesverbands (vzbv) zu einem verbrauchergerechten und fairen Zugang zu Fahrzeugdaten

18. November 2022

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Mobilität und Reisen

Rudi-Dutschke-Straße 17
10969 Berlin

mobilitaet@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. ZUSAMMENFASSUNG

Ein fairer, verbraucherfreundlicher und unabhängiger Zugang zu Fahrzeugdaten muss gewährleistet sein, damit neue, innovative Mobilitätsoptionen für Verbraucher:innen entstehen können und dem notwendigen Mobilitätswandel einen Schub verleihen. Gleichzeitig muss die Ausübung der Datenhoheit der Verbraucher:innen gewahrt und unterstützt werden.

In den bisher vorgeschlagenen Maßnahmen zur Digitalisierung der Mobilität kommt dieser Aspekt zu kurz. Wenn Nutzer:innen nicht wissen, an wen ihre Daten fließen und zu welchen Zwecken diese genutzt werden, können sie keine informierte – und damit auch keine souveräne – Entscheidung darüber treffen, ob und unter welchen Bedingungen sie Daten teilen möchten. Verbraucher:innen benötigen daher Transparenz und Kontrolle über den Verbleib und die Verwendung der von ihnen erzeugten Daten.

Daher spricht sich der Verbraucherzentrale Bundesverband (vzbv) für die Etablierung eines **Mobilitätsdatenwächters** aus. Über die bisherigen Vorschläge hinaus sollen mit dem Mobilitätsdatenwächter Regeln für alle Hersteller festgelegt werden, die den Schwerpunkt auf die Kontrolle der Fahrdaten durch den/die Fahrer:in legen sowie auf die Transparenz darüber, warum Unternehmen bestimmte Informationen benötigen, wie lange sie gespeichert werden und welche Dritte auf sie zugreifen dürfen. In Ergänzung zu den Aufgaben des Datentreuhänders nimmt der Mobilitätsdatenwächter konkret die Funktion der Autorisierungsstelle wahr. Diese Aufgabentrennung zwischen Datentreuhänder (Zugang zum Fahrzeug; Datenweiterleitung) und Mobilitätsdatenwächter (Autorisierung) gewährleistet die Neutralität beim Umgang mit den Mobilitätsdaten.

Der Betrieb eines Personal Information Management Systems (**PIMS**) soll den Nutzer:innen dabei helfen, die Datenverarbeitungen besser anweisen, kontrollieren und steuern zu können. Ein standardisierter Datenschutzmodus sollte den Verbraucher:innen ermöglichen, ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten durch den Hersteller oder zur Weitergabe an Dritte beliebig (oft) zu erteilen und zu widerrufen. Die erfolgreiche Implementierung eines PIMS setzt, neben Organisation und Finanzierung, standardisierte technische Voraussetzungen sowie vor allem eine Kooperationspflicht der Datenverarbeiter mit dem PIMS voraus. Die nur freiwillige Nutzung eines PIMS dürfte wegen fehlender Akzeptanz auch auf der Betroffenenseite zum Misserfolg führen. Der Mobilitätsdatenwächter stellt den Verbraucher:innen eine individuelle Konfiguration des Datenschutzes zur Verfügung.

Der vzbv fordert den Gesetzgeber auf:

- der faktischen Datenhoheit durch die Fahrzeughersteller mit einem fairen und verbraucherfreundlichen Zugang zu Fahrzeugdaten zu begegnen,
- den Fahrzeugnutzer:innen organisatorisch und technisch die Datenhoheit über fahrzeuggenerierte Daten zurückzugeben,
- in Ergänzung zu einem Datentreuhändermodell die Etablierung eines Mobilitätsdatenwächters voranzutreiben.

II. AKTUELLE SITUATION

Fahrzeuge werden immer stärker miteinander digital vernetzt und können untereinander und mit der Verkehrsinfrastruktur (zum Beispiel Ampeln (Lichtzeichenanlage) oder Straßenschilder) kommunizieren. So wissen diese Fahrzeuge zum Beispiel, wann eine Ampel grün wird.[1] Andere Verkehrszeichen „sagen“ einem Fahrzeug, wo es sich befindet.[2] Autos, die andere Fahrzeuge oder Verkehrsteilnehmende zum Beispiel über Straßenverhältnisse, Wetter, Verkehrssituation und Baustellen in Echtzeit informieren, sind nicht mehr Zukunftsmusik. Vernetzt fährt es sich sicherer, effizienter und komfortabler. Denn die intelligente Vernetzung von Fahrzeugen kann die Effizienz der Verkehrssysteme erhöhen, Unfälle vermeiden und allen Verbraucher:innen von Nutzen sein. Die Technik kann nicht nur das Fahrerlebnis verbessern, sondern beispielweise zu Fuß gehende und Rad fahrende Personen besser schützen.

Diese Entwicklungen haben allerdings auch eine Kehrseite. Mit der zunehmenden Vernetzung werden immer mehr Daten verarbeitet (zum Beispiel erfasst, gespeichert und ausgewertet). Die Vorteile der Technologie lassen sich aber nur realisieren, wenn die Skepsis der Verbraucher:innen hinsichtlich der Zuverlässigkeit, der Datensicherheit und des Datenschutzes verringert werden kann. Laut einer Umfrage im Auftrag des vzbv sind 35 Prozent der Befragten skeptisch und wollen ihre Mobilitätsdaten nicht teilen. 23 Prozent der Befragten würden unter der Bedingung, selbst von der Datenweitergabe zu profitieren, Daten weitergeben. Gut jeder Dritte (36 Prozent) der Befragten sogar, wenn sie der Allgemeinheit nutzt.[3] Transparenz und Vertrauenswürdigkeit sind die Schlüsselfaktoren der Digitalisierung im Fahrzeug.

Entscheidend wird dabei die Frage sein, inwieweit die Nutzer:innen Kontrolle über die Daten ihres Fahrzeugs haben und diese ausüben können. Der faire Zugang zu Fahrzeugdaten ist Voraussetzung, um Innovationen und Mobilitätsmehrwerte zu generieren. Der vzbv legt mit dem Konzept für einen Mobilitätsdatenwächter ein verbraucherfreundliches und faires Rollenmodell für den Datenzugang im Auto vor, der den Anspruch „mein Auto, meine Daten“ Wirklichkeit werden lässt. In einem Gutachten der Baum · Reiter & Collegen Rechtsanwaltsgesellschaft mbH im Auftrag des vzbv werden das Modell, die Notwendigkeit und die gesetzlichen Grundlagen für die Einführung eines Mobilitätsdatenwächters vertieft dargestellt.[4] In weiten Teilen beziehen sich diesbezügliche Aussagen in diesem Papier auf dieses Gutachten.

---

[1] Mag, Hans-Joachim: Wenn die Ampel mit dem Auto spricht, 2020, https://www.dmt-puls.de/news/wenn-die-ampel-mit-dem-auto-spricht/, 17.11.2022; Grundhoff, Stefan: Car-to-X-Kommunikation. Sprecht miteinander, 2020, https://www.walter-magazin.de/auto/car-to-x-kommunikation-sprecht-miteinander/, 17.11.2022.

[2] Dietze, Carina: Schon entdeckt? Das steckt hinter den schwarz-weißen Schildern auf der Autobahn, 2022, https://efahrer.chip.de/news/schon-entdeckt-das-steckt-hinter-den-schwarz-weissen-schildern-auf-der-autobahn_107861, 17.11.2022.

[3] Verbraucherzentrale Bundesverband e.V.: Intelligente Mobilität: 35 Prozent sehen das Teilen von Daten skeptisch, 2021, https://www.vzbv.de/publikationen/intelligente-mobilitaet-35-prozent-sehen-das-teilen-von-daten-skeptisch, 15.11.2022; Kantar Public Germany: Verbraucherbefragung zu den Themen Schuhe und Autonomes Fahren, 2021, Seite 61, https://www.vzbv.de/sites/default/files/2021-10/vzbv%20-%20Schuhe%20und%20Autonomes%20Fahren%20-%20Tabellen%20inkl.%20Methode%20%28003%29.pdf, 17.11.2022.

[4] Reiter, Julius; Methner, Olaf; Schenkel, Bénédict in Kooperation mit Bönninger, Jürgen: Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, Düsseldorf, m. w. N.

1. POLITISCHER RAHMEN

Nur wenn es der Gesetzgeber durch entsprechende Gesetze schafft, den vertrauenswürdigen Umgang mit Mobilitätsdaten überzeugend sicherzustellen, werden Verbraucher:innen rundum vernetzt fahren. Im Koalitionsvertrag für die 20. Legislaturperiode hat sich die Ampel-Koalition einige wichtige Vorhaben vorgenommen, die Mobilitätsdaten besser nutzbar machen sollen:

- „Wir schaffen ein Mobilitätsdatengesetz und stellen freie Zugänglichkeit von Verkehrsdaten sicher.“[5]
- „Den Datenraum Mobilität entwickeln wir weiter.“[6]
- „Im Gesetz zum autonomen Fahren werden wir die Regelungen verbessern, Haftungsfragen klären und die Datenhoheit der Nutzer sicherstellen.“[7]
- „Die Potenziale von Daten für alle heben wir, indem wir den Aufbau von Dateninfrastrukturen unterstützen[8] […]“ **und**
- **„**Zur wettbewerbsneutralen Nutzung von Fahrzeugdaten streben wir ein Treuhänder-Modell an, das Zugriffsbedürfnisse der Nutzer, privater Anbieter und staatlicher Organe sowie die Interessen betroffener Unternehmen und Entwickler angemessen berücksichtigt.“[9]

Im Ergebnis wird eine Dateninfrastruktur angestrebt, mit der nicht nur Fahrzeughersteller über einen direkten Zugang zu fahrzeugerfassten Mobilitätsdaten verfügen, sondern auch eine neutrale dritte Stelle – ein Datentreuhänder. Bisher steht aber eine konkrete Positionierung der Bundesregierung – zum Beispiel gegenüber der EU-Kommission – aus.

Seit einigen Jahren läuft auf europäischer Ebene eine Diskussion über den Zugang zu Daten, Funktionen und Ressourcen zur Entwicklung innovativer datengesteuerter Mobilitätsdienste. Die Kommission arbeitet daran, die EU-Rechtsvorschriften über die Typgenehmigung von Fahrzeugen im Hinblick auf einige technische Fragen und dem Zugang zu Fahrzeugdaten, -funktionen und -ressourcen unter Berücksichtigung des technischen Fortschritts zu aktualisieren.[10] Ein Vorschlag ist für das zweite Quartal 2023 angekündigt.

---

[5] Sozialdemokratische Partei Deutschlands (SPD); BÜNDNIS 90/DIE GRÜNEN; Freie Demokratische Partei (FDP): Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025, S. 52, https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1, 17.11.2022.

[6] Siehe Fußnote 5, dort S. 50.

[7] Siehe Fußnote 5, dort S. 52.

[8] Siehe Fußnote 5, dort S. 17.

[9] Siehe Fußnote 5, dort S. 52.

[10] Initiative der Europäischen Kommission: Zugang zu Fahrzeugdaten, -funktionen und ressourcen, Ref. Ares(2022)2302201, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Zugang-zu-Fahrzeugdaten-funktionen-und-ressourcen_de, 15.11.2022.

2. PROBLEM: FAKTISCHE DATENHOHEIT DER AUTOHERSTELLER

Der Zugang zu Mobilitätsdaten wird derzeit technisch und damit faktisch im Wesentlichen von dem jeweiligen Fahrzeughersteller kontrolliert. Die Zugangsmöglichkeiten des/r Fahrzeugnutzer:in oder sonstiger Dritter ist begrenzt. Soweit das Fahrzeug über eine Mobilfunkschnittstelle verfügt, werden die Daten ausschließlich auf einen herstellereigenen Server übertragen. Dritte sind für einen Zugang in der Hauptsache auf die Weiterleitung durch den Fahrzeughersteller angewiesen oder sind auf einen (begrenzten) Datenzugang über die OBD II-Schnittstelle beschränkt.

Gemäß Werkseinstellung und aufgrund fehlender Schnittstellen sehen vernetzte Fahrzeuge auch für den Fahrzeugnutzer (in der Regel ein/eine Verbraucher:in) selbst keinen Zugriff auf die im Fahrzeug generierten Daten vor. Neben der fehlenden Schnittstelle wiegt zudem schwer, dass für den/die durchschnittlichen Fahrzeugnutzer:in nicht ersichtlich ist, welche Daten überhaupt durch das Fahrzeug generiert, im Fahrzeug gespeichert oder extern übermittelt werden. Unmittelbare Datenzugangsmöglichkeiten zugunsten des Fahrzeugnutzers beziehungsweise der Fahrzeugnutzerin sind nicht vorhanden, das heißt es besteht aktuell keine Möglichkeit, per Anzeige oder gar Download einen Überblick zu den verarbeiteten Mobilitätsdaten zu erhalten. Insoweit besteht für die Verbraucher:innen keine Transparenz, was zu Folgeproblemen zum Beispiel bei der Wahrnehmung der eigenen Datenschutzrechte führt. Ein zweckmäßiger und durchsetzbarer Anspruch auf Datenzugang und/oder Datenweitergabe zugunsten des Fahrzeugnutzers lässt sich nach aktuellem Stand auch nur bedingt aus gesetzlichen Vorschriften herleiten. [11]

Auch Dritte, wie Werkstätten, Versicherungen oder Pannendienste, die im Auftrag des/r Fahrzeughalter:in auf die Verarbeitung personenbezogener Daten zur Vertragserfüllung angewiesen sind, können mangels geeigneter Schnittstelle nicht selbst unmittelbar auf Mobilitätsdaten im Fahrzeug zugreifen, sondern sind auf einen Zugang zu den entsprechenden Daten über den Fahrzeughersteller angewiesen. Der Verband der Automobilindustrie e.V. (VDA) legt mit seinem NEVADA-Konzept und der Erweiterung ADAXO fest, dass die im Fahrzeug generierten Daten ausnahmslos zunächst auf den jeweiligen Herstellerserver übertragen werden. Vertragliche Konditionen zur Ausgestaltung des Datenzugangs werden von jedem Fahrzeughersteller nach eigenem Ermessen geregelt. Die Fahrzeughersteller entscheiden über Qualität (zum Beispiel Zeitpunkt der Datenweitergabe und Datenformat), Quantität (zum Beispiel Arten von Fahrzeugdaten, einzeln oder nur im Paket) und Preis der Daten. Die Wahlfreiheit der Verbraucher:innen wird dadurch beschränkt, denn im Wettbewerb um Mobilitätsdienste, die auf der Ressource Mobilitätsdaten basieren, stehen sich derzeit Fahrzeughersteller und die mit ihnen verbundenen Unternehmen auf der einen Seite und sonstige Dienstleister auf der anderen Seite gegenüber. Der Fahrzeughersteller ist dabei nicht nur als Fahrzeugproduzent und -verkäufer tätig, sondern bietet darüber hinaus auch Komplementärdienstleistungen an. Der beschränkte Datenzugang kann für dritte Dienstleister im Hinblick auf Märkte für digitale, mobilitätsdatenbasierte Dienstleistungen als Eintrittsbarriere wirken. Dies birgt das Risiko für ein

[11] Artt. 12, 15, 20 DSGVO (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG).

Marktversagen, was sich zum Nachteil der Fahrzeugnutzer:innen auswirkt und sogar dazu führen kann, dass keine neuen, innovativen Technologien entwickelt werden.

> Die faktische Datenhoheit der Autohersteller schränkt die Wahlfreiheit für Verbraucher:innen ein, verhindert Wettbewerb und Innovationen.

3. RISIKO: INFORMATIONSÜBERLASTUNG DER NUTZER:INNEN UND OFT EINE FEHLENDE KENNTNISNAHME

Ein weiteres Machtungleichgewicht zwischen Fahrzeughersteller(n) und Kund:innen besteht insbesondere, weil es für die Mehrheit der Fahrzeugnutzer:innen kaum möglich ist, zwischen den verschiedenen Datenverarbeitungszwecken zu differenzieren oder aber nachzuvollziehen, welche Fahrzeugfunktionen oder digitalen Dienste von welchen Verarbeitungsvorgängen abhängen. Besonderer Bedeutung kommt deshalb der Informationserteilung gegenüber dem/r Fahrzeugnutzer:in zu. Informationen über die Datenverarbeitungsvorgänge werden seitens der Fahrzeughersteller in umfangreichen Datenschutzhinweisen bereitgestellt. Dabei wird in erster Linie auf eine Verlinkung auf hinterlegte PDF-Dokumente zurückgegriffen, wobei die Dokumente mitunter nur tief im Menü zu finden sind und einen Umfang von rund 30 Seiten haben.[12] Aus den Datenschutzhinweisen ergeben sich die verschiedenen, datenbasierten Dienstleistungen, die dort im Einzelnen mit Hinweis auf die Datenverarbeitungsvorgänge erläutert werden. Nur selten wird ein/e Fahrzeugnutzer:in die umfangreichen Datenschutzinformationen tatsächlich zur Kenntnis nehmen. Vielen Autokäufer:innen dürfte nicht einmal bewusst sein, dass sie mit dem neuen Fahrzeug nicht nur ein Fortbewegungsmittel, sondern einen Datenspeicher erwerben.

Neben der Fülle an Informationen ist auch der Informationskanal herausfordernd. Nicht nur, weil dieser darauf abgestimmt sein muss, ob der/die Fahrzeugnutzer:in die Informationen in Papierform, über den Bildschirm im Fahrzeug (wobei es hier dann auch auf die jeweilige Bildschirmgröße ankommt) oder sein Smartphone erhält. Die Informationserteilung wird den flexiblen und dynamischen Datenverarbeitungsprozessen nur schwer gerecht werden können. Herausfordernd sind zudem das Hinzutreten neuer Verarbeitungszwecke (im Hinblick derer regelmäßig eine neue Einwilligung erforderlich wäre), der Widerruf bestehender Einwilligungen sowie erneut der Umstand, dass Fahrzeuge von unterschiedlichen Personen genutzt werden, die alle betroffene Personen im Sinne des Datenschutzrechts sein können, nicht jedoch zwingend einzeln ihre Einwilligung zur Datenverarbeitung erklärt haben („Dual-Use-Konstellationen“). Damit in der Praxis personenbezogene Mobilitätsdaten nicht auch ohne gesetzliche Rechtfertigung verarbeitet werden, ist demnach jedenfalls ein angemessenes Einwilligungsmanagement erforderlich. In Frage steht, ob ein solches seitens der Fahrzeughersteller zufriedenstellend angeboten werden kann.

> Einer Informationsüberlastung des Betroffenen ist vorzubeugen, damit diese ihre Datenschutzrechte angemessen ausüben können.

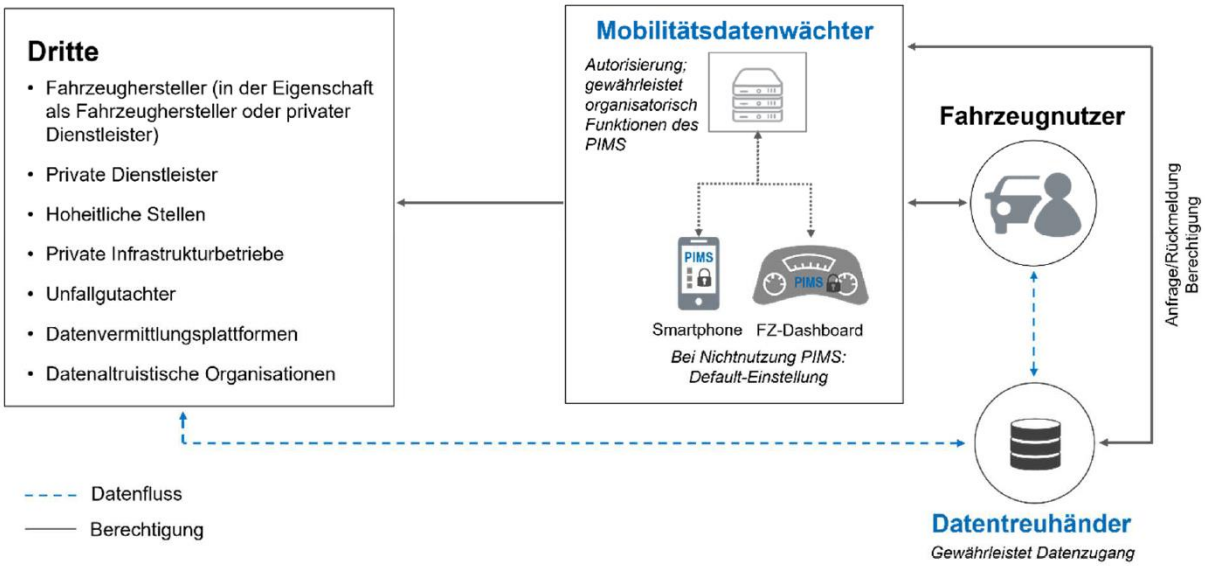
[12] Reiter, Julius; Methner, Olaf; Schenkel, Bénédict in Kooperation mit Bönninger, Jürgen: Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, Seite 20, Düsseldorf.

III. MOBILITÄTSDATENWÄCHTER

Bisherige Regulierungsbemühungen, wie die staatliche Förderung des Mobility Data Space (MDS - Mobilitätsdatenraum), konzentrieren sich auf das Verhältnis zwischen verschiedenen Unternehmen und darauf, gegenseitiges Vertrauen durch Regelungstreue aufzubauen. Damit soll die Bereitschaft, Daten zwischen Unternehmen zu teilen, steigen. Vernachlässigt wird dabei die Schnittstelle zu den Nutzer:innen. Damit aber Verbraucher:innen die Kontrolle und Transparenz über die von ihnen generierten Mobilitätsdaten nicht entgleitet, schlägt der vzbv die Etablierung eines Mobilitätsdatenwächters vor. Dieser soll zum einen den datenschutzkonformen Umgang mit Mobilitätsdaten gewährleisten und zum anderen einen fairen und diskriminierungsfreien Zugang zu Mobilitätsdaten ermöglichen.

Zur Veranschaulichung die folgende Grafik, die in Zusammenarbeit mit unseren Gutachtern entstand (vergleiche Fußnote 4).

Mobilitätsdatenwächtermodell



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, also einen sicheren Automotiv-Telematik-Gateway im Fahrzeug, können von Drittanbietern bereitgestellte Applikationen ausgeführt werden. Sollte darüber hinaus eine Auslagerung der Daten notwendig sein, sollte dies an unabhängige treuhänderische Dritte erfolgen. Wie in Kapitel II.1 dargestellt, hat sich die Regierungskoalition auf ein „Treuhänder-Modell“ festgelegt.

Um an dieser Stelle der beschriebenen Datenhoheit der Fahrzeughersteller zu begegnen, soll zukünftig einem Mobilitätsdatentreuhänder technisch der unmittelbare Datenzugang gewährt werden. Der Mobilitätsdatentreuhänder erhält den Datenzugang aus dem Fahrzeug und kann diesen, je nach Anwendungsfall und Bedarf, zwischenspeichern und/oder direkt an den Datenempfänger („Dritte“) weiterleiten. Über die Information, ob, inwieweit und an wen Mobilitätsdaten weitergegeben werden dürfen/sollen, verfügt nicht der Datentreuhänder, sondern der Mobilitätsdatenwächter

nach den Vorgaben des/der Fahrzeugnutzer:in sowie nach gesetzlichen Legitimationsgründen. Dieser betreibt dafür ein Personal Information Management System (PIMS), in dem der/die Fahrzeugnutzer:in seine/ihre Datenverarbeitungspräferenzen hinterlegt, Einwilligungen erteilt und sämtliche Datenverarbeitungsvorgänge transparent nachverfolgen kann. Soweit nun ein „Dritter“ beim Mobilitätsdatentreuhänder um Überlassung bestimmter Mobilitätsdaten bittet, fragt der Datentreuhänder beim „Mobilitätsdatenwächter“ an, ob seitens des/r dispositionsbefugten Fahrzeugnutzer:in eine Autorisierung vorliegt. Ist dies der Fall oder liegt ein gesetzlicher Legitimationsgrund vor, erteilt der Wächter die Freigabe und der Datentreuhänder führt den gewünschten Datentransfer durch. In Betracht kommt nicht nur die Datenübermittlung aus dem Fahrzeug in Richtung Dritte. Auch auf dem umgekehrten Wege können – soweit auch hier eine Autorisierung oder Legitimierung vorliegt – über den Mobilitätsdatentreuhänder Informationen (zum Beispiel auch Updates) in das Fahrzeug übermittelt werden.

Der Mobilitätsdatenwächter hat dabei zu keinem Zeitpunkt physischen Zugriff auf die Daten. Darüber verfügt nur der Datentreuhänder, der aber seinerseits selbst nicht über die Art oder den Umfang der Datenweiterleitung entscheidet. Die Aufgabentrennung zwischen Datentreuhänder (Zugang zum Fahrzeug, Datenweiterleitung) und Mobilitätsdatenwächter (Autorisierung) gewährleistet die Neutralität beim Umgang mit Mobilitätsdaten und verhindert Interessenkonflikte.

1. BETRIEB EINES PERSONAL INFORMATION MANAGEMENT SYSTEMS (PIMS)

1.1 Definition und Funktionen

PIMS sind technische Hilfsmittel, die Nutzer:innen dabei helfen sollen, Datenverarbeitungen besser anweisen, kontrollieren und steuern zu können. Bei einem PIMS handelt es sich um kein fertiges oder starres System. Vielmehr sind zahlreiche Funktionen denkbar, deren Implementierung vom konkreten Anwendungsfall abhängt. Künftig könnten über so einem PIMS auch die neuen Zugangsrechte, die voraussichtlich mit dem Data Act kommen, geltend gemacht werden.

Zentrale Funktionalitäten von PIMS sind die konsequente Beachtung und Durchsetzung von Datenschutzrecht, die Integration eines Einwilligungsmanagements sowie die Gewährleistung von Transparenz und Nachvollziehbarkeit aller Datenverarbeitungsvorgänge (gegebenenfalls im Hinblick auf personenbezogene sowie auch auf nicht-personenbezogene Daten).[13] Indem betroffene Nutzer:innen eines PIMS ihre digitalen Aktivitäten nachvollziehen und kontrollieren können, wird gleichzeitig rechtswidrigen Datenverarbeitungen vorgebeugt. Verbraucher:innen müssen ebenso einen Überblick über bereits erteilte oder bereits widerrufene Einwilligungen erhalten. Dies würde das Vertrauen des/der Einzelnen in die Nutzung digitaler vernetzter Systeme stärken. Vertrauen ist eine Voraussetzung, die auch für die Weiterentwicklung

[13] Vgl. auch Krämer, Jan: Digitale Selbstbestimmung durch Personal Information Management Systems?, 2022, S. 4 f., https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-4-kraemer-digitale-selbstbestimmung-durch-personal-information-management-systems.pdf, 15.11.2022; Stellungnahme des Verbraucherzentrale Bundesverband e.V.: Neue Datenintermediäre – Anforderungen des vzbv an Personal Information Management Systeme (PIMS) und Datentreuhänder, 2020, S. 6, https://www.vzbv.de/publikationen/datenintermediaere-gesetzlich-regeln, 15.11.2022.

der Ökosysteme vernetzter Fahrzeuge sowie Mobilitätsplattformen grundlegend ist. Über die Basisfunktionen hinaus sind Identitätsmanagement, also die Identifizierung des Nutzers bei verschiedenen Onlinediensten sowie die Auswertung und Monetarisierung von nicht personenbezogenen Daten weitere Funktionen von PIMS. Die Funktion Datenmanagement, also ein möglicher persönlicherer Datenspeicher, Zusammenführung verschiedener Datenquellen, Datenkonvertierung wären aber eher Aufgabe des Datentreuhänders, siehe auch Grafik.

1.2 Voraussetzungen

Die erfolgreiche Implementierung eines PIMS setzt, neben Organisation und Finanzierung, standardisierte technische Voraussetzungen[14] sowie vor allem eine Kooperationspflicht der Datenverarbeiter mit dem PIMS voraus. Letztgenannter Punkt mündet in eine rechtliche Verpflichtung aller datenverarbeitenden Stellen, den betroffenen Personen zum Beispiel die Vornahme der gewünschten Datendispositionen (Einwilligungsmanagement), die Kenntnisnahme datenschutzrechtlicher Informationen, die Nachvollziehbarkeit sämtlicher Verarbeitungsvorgänge oder die Wahrnehmung der sonstigen Datenschutzrechte über das PIMS zu ermöglichen.[15] Dem Datenverarbeiter soll es in der Folge verboten sein, mit der betreffenden Person am PIMS vorbei zu interagieren.[16]

Eine freiwillige Nutzung eines PIMS durch Dritte und Fahrzeughersteller dürfte dagegen mit hoher Wahrscheinlichkeit wegen fehlender Akzeptanz auch auf Betroffenenseite zum Misserfolg führen. Datendispositionen, Datenschutzinformationen sowie Verarbeitungsvorgänge wären auch bei teilweiser Nutzung des PIMS weiterhin nicht zentralisiert zugänglich. Das Interesse der Nutzer:innen, das PIMS (als ein weiteres System unter vielen) zu nutzen, ginge verloren.

1.3 Anforderungen in Bezug auf Mobilitätsdaten

Im Rahmen des Mobilitätsdatenwächtermodells geht es um die Einführung eines PIMS, das nicht allgemeingültig, sondern speziell im Hinblick auf die Verarbeitung von Mobilitätsdaten entwickelt und genutzt werden soll. In Entsprechung dazu sind passende, sektorspezifische Mindestfunktionalitäten des PIMS auszuwählen. In Anbetracht der datenschutzrechtlichen Herausforderungen, die sich bei der Verarbeitung von Mobilitätsdaten stellen, sowie unter Berücksichtigung der zugewiesenen Aufgaben des „Datentreuhänders“ kommen in erster Linie nachstehende PIMS-Funktionen in Betracht:

- Ein wirksames und nutzerfreundliches Einwilligungsmanagement, das auch nicht-personenbezogene Daten einbezieht. Zwar betrifft dies nicht mehr die datenschutzrechtliche Ebene. Jedoch sollte bei der Gestaltung und der Einführung eines PIMS innerhalb des speziellen Kontextes „Mobilitätsdaten“ gleichzeitig dafür

[14] Specht-Riemenschneider, Louisa; Kerber, Wolfgang, Designing Data Trustees – A Purpose-Based Approach (Datent reuhänder – Ein problemlösungsorientierter Ansatz), 2022, S. 34, Berlin, Konrad-Adenauer-Stiftung e. V.
[15] Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission“, 2019, S. 134, https://www.bundesregierung.de/breg-de/service/publikationen/gutachten-der-datenethikkommission-langfassung-1685238, 15.11.2022.
[16] Siehe Fußnote 14, dort S. 33.

Sorge getragen werden, dass dem/der Fahrzeugnutzer:in, der/die häufig auch Eigentümer:in des Fahrzeugs ist, die vollständige Datenhoheit in seinem Fahrzeug generierten Daten übertragen wird.

- Eine transparente und nachvollziehbare Darstellung aller Verarbeitungsvorgänge, die im PIMS durch verständliche Datenschutzinformationen erfolgt, angepasst an das Kommunikationsmittel (Smartphone, Fahrzeugdisplay und so weiter) und zur Durchsetzung von Datenschutzrechten dargestellt wird, welche datenschutzrechtliche Ansprüche (insbesondere Recht auf Auskunft, Recht auf Berichtung, Recht auf Löschung, Recht auf Datenübertragbarkeit) wie durchgesetzt werden können. Bestehende Diskrepanzen zwischen mithilfe des Einwilligungsmanagements erteilten Einwilligungen und tatsächlichen Verarbeitungsvorgängen, die auf einer Einwilligung beruhen sollen, würden (automatisiert) sichtbar.

1.4 Ausgestaltung

Neben den passenden PIMS-Funktionen kommt es für den Erfolg des Systems des Mobilitätsdatenwächters maßgeblich auf eine nutzergerechte Bedienoberfläche an. Durch ein strukturiertes Menü, selbsterklärende (beziehungsweise kurz erläuterte) Symbolleisten (zum Beispiel Toolbars), Schaltflächen (zum Beispiel Buttons), Schalter und Regler oder sonstige Auswahllisten muss es dem/r Nutzer:in ohne Weiteres möglich sein, seine/ihre bevorzugten Einstellungen vorzunehmen oder die gesuchten Informationen abzurufen. Dabei muss die Oberfläche neutral gestaltet sein, damit eine Systemnutzung ohne Beeinflussung durch die Interessen einer datenverarbeitenden Stelle gewährleistet ist. Die Bedienung des PIMS sollte von verschiedener Stelle aus möglich sein. In Betracht kommt zunächst eine Bedienung im Fahrzeug selbst über das Fahrzeugdisplay („Daten-Cockpit“). Gleichzeitig sollte jedoch auch eine Bedienbarkeit über den Computer oder das Smartphone ermöglicht werden. Die Bedienbarkeit über eine Smartphone App hätte im Rahmen einer erweiterten Funktionalität den Vorteil, dass die auf dem Smartphone gespeicherten Einstellungen in jedes (kompatible) vernetzte Fahrzeug mitgenommen werden können.[17] Das für den/die Nutzer:in fremde Fahrzeug kann sich dann mit dem Smartphone verbinden. Die PIMS-Einstellungen werden berücksichtigt. Auf diese Weise könnte auch dem Problem, dass ein Fahrzeug durch verschiedene datenschutzrechtlich betroffene Personen (dass heißt Fahrer:in, Beifahrer:in, Halter:in, Käufer:in, Eigentümer:in) genutzt werden kann, begegnet werden.

1.5 Institutionelle Ausgestaltung, Qualitätssicherung und Finanzierung

Die konkreten Aufgaben des Mobilitätsdatenwächters werden aktuell in Gänze noch von keiner Stelle wahrgenommen. Es stellt sich daher im Rahmen einer institutionellen Ausgestaltung, Qualitätssicherung und Finanzierung des Mobilitätsdatenwächtermodells die Frage, welche bestehenden oder neu zu schaffenden Organisationen die beschriebenen Aufgaben übernehmen könnten beziehungsweise sollten. In Betracht kommen zunächst Unternehmen aus der

[17] Verbraucherzentrale Bundesverband e.V.: Fahrerlos alle mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht, 2021, S. 15, https://www.vzbv.de/pressemitteilungen/gesetz-zum-autonomen-fahren-muss-alle-mitnehmen, 15.11.2022.

Privatwirtschaft. Alternativ könnte sich der Staat dieser Aufgaben annehmen. Bei der Auswahl ist zu berücksichtigen, dass der Staat mit der Umsetzung des Mobilitätsdatenwächtermodells regulierend tätig wird, und zwar zum einen gegen ein Versagen mobilitätsdatenbasierter Märkte und zum anderen zur konsequenten Beachtung und Durchsetzung von Datenschutzrecht. Unter Beachtung des Grundsatzes der Marktfreiheit wird der Staat zur Vermeidung von Marktversagen nur soweit als nötig eingreifen, solange sich die Märkte im Übrigen von selbst regulieren. Vor allem muss der Staat bei seiner Regulierungstätigkeit das Verhältnismäßigkeitsprinzip beachten. Soweit bestehendes Regulierungsrecht nicht ausreicht, um die bezweckten Ziele zu erreichen, wird der Staat nur insoweit nachbessern, als dies zwingend erforderlich und angemessen ist.

Der Mobilitätsdatenwächter fungiert als Autorisierungsstelle gegenüber dem Mobilitätsdatentreuhänder. Für diese Aufgabe ist vor allem die Einrichtung von Schnittstellen erforderlich, damit Mobilitätsdatenwächter und Datentreuhänder miteinander kommunizieren können. Im Schwerpunkt betreibt der Mobilitätsdatenwächter allerdings ein PIMS, dessen Aufbau und Betrieb, verglichen mit dem Autorisierungsprozess, die deutlich umfangreichere Aufgabe darstellt. Maßgeblich muss sich die Auswahl einer passenden Institution zur Wahrnehmung der Aufgaben des Mobilitätsdatenwächters also daran orientieren, wer zum Aufbau und Betrieb eines PIMS geeignet ist.

Zur Erbringung der Aufgaben des Mobilitätsdatenwächters kommen sowohl private Unternehmen als auch staatliche Stellen in Betracht. Für ein privates Unternehmen spricht, dass der staatliche Eingriff weniger intensiv ausfällt und sich auf die zwingende Einbindung eines Mobilitätsdatenwächters beschränkt. Hierzu kommt, dass private Unternehmen grundsätzlich gute Investoren sind und das Potenzial haben, auf komplexen Märkten der Datenwirtschaft innovativ tätig zu sein. Gegen die Überlassung der Aufgaben an ein privates Unternehmen spricht allerdings die perspektivische Finanzierbarkeit, die zudem wirtschaftlich dem zwingenden Gebot der Vermeidung von Interessenkollisionen entgegenstehen könnte. Auch wenn PIMS bereits seit einigen Jahren als geeignetes Mittel zur Umsetzung von Datenschutzrecht angesehen werden, hat sich bislang kein wirtschaftlich tragfähiges Geschäftsmodell etablieren können.[18] Vorerst sind es zunächst nur die Fahrzeughersteller und Dritte, die das spezielle mobilitätsdatenbasierte PIMS vorschalten müssten. Die Fahrzeugnutzer:innen werden voraussichtlich nicht dazu bereit sein, für die Nutzung des PIMS ein Entgelt zu bezahlen. Aufgrund der verhältnismäßig geringen Anzahl von Fahrzeugherstellern und Dritten ist eine Finanzierung von dieser Seite aus mangels Skalierbarkeit kaum denkbar. Soweit ein „Datentreuhänder“ später die Autorisierung beim „Mobilitätsdatenwächter“ anfragt, könnte für diesen Vorgang ein Entgelt vom Dritten verlangt werden. Die potenzielle Häufigkeit von Autorisierungsanfragen ließe wohl auch eine Skalierung zu. Bis es dazu kommt, bedürfte es allerdings einer nicht unerheblichen Vorfinanzierung, die private Investoren abschrecken könnte. Zwar wäre es denkbar, dem Finanzierungsproblem durch staatliche Subventionierung bereits anerkannter oder zertifizierter PIMS privater Betreiber zu begegnen.[19] Zu beachten ist

[18] Vgl. auch Krämer, Jan: Digitale Selbstbestimmung durch Personal Information Management Systems?, 2022, S. 16, https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-4-kraemer-digitale-selbstbestimmung-durch-personal-information-management-systems.pdf , 15.11.2022.

[19] Specht-Riemenschneider, Louisa; Kerber, Wolfgang, Designing Data Trustees – A Purpose-Based Approach (Datentreuhänder – Ein problemlösungsorientierter Ansatz), 2022, S. 41, Berlin, Konrad-Adenauer-Stiftung e.V.

jedoch, dass private Unternehmen in der Regel kein Interesse an Neutralität haben, sondern wirtschaftliche Eigeninteressen verfolgen, wohingegen der Staat Aufgaben ohne Gewinnerzielungsabsicht wahrnehmen kann. Allerdings soll gerade ein neutrales Auftreten gegenüber Fahrzeugnutzer:in, Fahrzeughersteller und sonstigen Dritten grundlegende Eigenschaft des Mobilitätsdatenwächters sein. Durch die Neutralität soll insbesondere vermieden werden, dass die Nutzer:innen des PIMS durch dessen Ausgestaltung unbewusst fremdbestimmt entscheiden („Dark Patterns“). Das PIMS muss ein Hilfsmittel sein, das ausschließlich die selbstbestimmte Entscheidungshoheit unterstützt.[20] Dies ist bei Unternehmen, die wirtschaftliche Eigeninteressen verfolgen, gewöhnlich nicht gewährleistet.

Im Falle des Mobilitätsdatenwächters wäre alternativ die Gründung einer Gesellschaft im Eigentum des Bundes möglich. Diese Stelle könnte die Aufgaben des Mobilitätsdatenwächters wahrnehmen. Wegen des Betriebs eines PIMS und des datenschutzrechtlichen Schwerpunkts könnte die Rechts- und Fachaufsicht des Mobilitätsdatenwächters nach einer entsprechenden Gesetzesänderung zur Zuständigkeit beim Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) angesiedelt sein.[21] Die Begründung des staatlichen Mobilitätsdatenwächters würde dabei nicht ausschließen, dass private Unternehmen parallel eine entsprechende Stelle gründen. Mehrere Mobilitätsdatenwächter könnten in wettbewerblicher Hinsicht nebeneinander betrieben werden, was den Vorteil hätte, dass die Verbraucher:innen entscheiden könnten, mit welchem Wächter sie zusammenarbeiten wollen. Zulassung und Betrieb weiterer Mobilitätsdatenwächter sollten zur Einhaltung der Qualitäts- und Neutralitätsstandards allerdings einem angemessenen Zertifizierungs- und einer angemessenen Aufsicht unterworfen werden.[22]

[20] Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission“, 2019, S. 133, https://www.bundesregierung.de/breg-de/service/publikationen/gutachten-der-datenethikkommission-langfassung-1685238, 15.11.2022.

[21] Entsprechende Tendenz: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): Vernetzte Fahrzeuge – Datenschutz im Auto, 2020, S. 19, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/VernetzteFahrzeuge.html, 15.11.2022.

[22] Siehe Fußnote 20.

IV. GESETZLICHE UMSETZUNG

1. NATIONALE GESETZGEBUNG

Soweit der europäische Gesetzgeber Regelungen im Sinne des hier vorgestellten Mobilitätsdatenwächtermodells nicht vorantreibt, kann und sollte der deutsche Gesetzgeber auf nationaler Ebene tätig werden und eine Vorreiterrolle übernehmen. Dabei muss er den Schutz von Mobilitätsdaten und deren Verarbeitung beachten. Als passender Regelungsbereich bietet sich das von der Regierung für das Jahr 2024 angekündigte „Mobilitätsdatengesetz“ an. Schwerpunktmäßig würde es dort auf die folgenden Regelungsbereiche ankommen:

- Die Definition des Mobilitätsdatenwächters und seiner Aufgaben
- Eine Kooperationspflicht der Datenverarbeiter (Verantwortliche im Sinne der DSGVO) mit dem Mobilitätsdatenwächter (dass heißt insbesondere mit dem PIMS)
- Die Interoperabilität bei der Zusammenarbeit zwischen (verschiedenen) „Mobilitätsdatenwächter(n) und Datentreuhänder(n)
- Ein Zertifizierungs- und Überwachungssystem im Falle der Gründung weitere „Mobilitätsdatenwächter“
- Finanzielle Förderung von privatwirtschaftlichen Mobilitätsdatenwächter oder Einrichtung einer beliehenen Stelle mit dem Auftrag des Aufbaus und Betriebs eines Mobilitätsdatenwächters.

2. SEKTORSPEZIFISCHE REGELUNG

In Ergänzung des geplanten Regelungsrahmens des Data Acts ist eine sektorspezifische Regelung für einen Zugang zu Mobilitätsdaten auf europäischer Ebene möglich. Aktuell hat sich der europäische Gesetzgeber dieser Frage angenommen und strebt eine sektorspezifische Regulierung durch Änderung der Typengenehmigungsverordnung an.[23] Ob neben einer solchen europäischen Regelung andere oder weitergehende Datenzugangsmöglichkeiten durch nationale Gesetzgebung vorgeschrieben werden können, hängt davon ab, ob und inwieweit der europäische Gesetzgeber mit der Änderung der Typengenehmigungsverordnung eine Vollharmonisierung vornehmen wird. Im europäischen Gesetzgebungsprozess für eine sektorspezifische Regulierung sollte sich die Bundesregierung dafür einsetzen, dass dort die Einführung eines PIMS mitgeregelt wird. Falls die Bemühungen hier nicht erfolgreich sind, käme jedenfalls hinsichtlich der Einführung eines PIMS weiterhin eine nationale Regelung in Betracht.

[23] VERORDNUNG (EU) 2018/858 DES EUROPÄISCHEN PARLAMENTS UND DES RATES, 2018, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32018R0858, 15.11.2022; siehe auch Fußnote 10.