iKoPA Integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge

Deliverable 3.2

Datenschutz bei vernetzten, automatisierten und kooperativen Fahrzeugen nach der Datenschutzgrundverordnung

Version number	1.0
Dissemination level	Public
Project Coordination	htw saar
Due date	2018-12-31
Date of preparation	2018-12-21, 2019-03-25

Funded by the

Federal Ministry
of Education
and Research

Project Coordination

Prof. Dr. Horst Wieker

Head of ITS Research Group (FGVT) at the
htw saar – Hochschule für Technik und Wirtschaft des Saarlandes,
University of Applied Sciences
Department of Telecommunications
Campus Alt-Saarbrücken
Goebenstr. 40
D-66117 Saarbrücken
Germany

Phone +49 681 5867 195
Fax +49 681 5867 122
E-mail wieker@htwsaar.de

Author:

Gundula Gagzow – Unabhängiges Landeszentrum für Datenschutz

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 EINLEITUNG UND ZUSAMMENFASSUNG

Vernetzte und in naher Zukunft automatisiert fahrende Fahrzeuge stehen mit dem kombinierten Einsatz von Informations- und Kommunikationstechnologie beispielhaft für die fortschreitende Digitalisierung zahlreicher Lebensbereiche.

Bereits heute steht die entsprechende Technik zur Verfügung oder wird entwickelt, mit deren Hilfe das Fahrzeug über entsprechende Sensoren und Prozessoren das Umfeld und den Fahrzeuginnenraum in Echtzeit wahrnehmen, den eigenen Standort bestimmen und den Fahrweg dynamisch an die Verkehrslage anpassen kann.[1] Mit dem multiplen Kommunikationsansatz vernetzter und automatisierter Fahrzeuge entstehen darüber hinaus auch neue Schnittstellen und neuen Technologien für den Datenaustausch.

Moderne Fahrzeuge werden in Zukunft mit anderen Systemen kooperieren und hierfür automatisiert mit anderen Gegenständen oder Systemen von „Maschine zu Maschine" kommunizieren. Diese Fähigkeit ist zum einen wesentliche Grundbedingung für hoch- und vollautomatisierte Fahrfunktionen. Zum anderen wird das moderne Fahrzeug dadurch zum Bestandteil des Internet of Things und ermöglicht neue, insbesondere datengetriebene und ortsbasierte Geschäftsmodelle.[2] Die Nutzung moderner Fahrzeuge verspricht insoweit zahlreiche Vorteile, die von erhöhter Fahrsicherheit über Ressourcenschonung durch effizientere Fahrweisen bis zur Zunahme des Komforts reichen.

Bei dem Betrieb der „rollenden Kommunikationszentren"[3] fallen daher auch enorme Datenmengen an, die zum Teil für den Betrieb benötigt werden, teilweise aber auch als Nebenfolge der Nutzung der neuen Technologien entstehen, und an denen unterschiedliche Begehrlichkeiten bestehen. Der enorme Datenumfang dieser digitalen Datenspuren ermöglicht mit entsprechenden Big-Data-Analysewerkzeugen die Ableitung aussagekräftiger Informationen über die Fahrweise, Aufenthaltsorte, den Zustand des Fahrzeugs und der Insassen sowie die Fahrzeugumgebung und damit die Erstellung präziser Bewegungs- und Verhaltensprofile.

Die Fahrzeugdaten gestatten damit tiefe Einblicke in die private Lebensgestaltung des Einzelnen und fallen als personenbezogen in den Schutzbereich der Grundrechte auf Datenschutz der Artikel 8 und 7 der Charta der Grundrechte der EU sowie der Artikel 2 Abs. 1, 1 Abs. 1 des Grundgesetzes. Nach dem Rechtsgrundsatz des Vorbehalts des Gesetzes ist daher für die Verarbeitung dieser Daten eine ausdrückliche gesetzliche

---

1 Vgl. Ethik–Kommission, S. 6.

2 Allgemein zu Location Based Services vgl. Hansen et al., Verkettung digitaler Identitäten, 195 ff.

3 Hansen, DuD 2015, 367 (367).

Erlaubnis erforderlich, die seit dem 25.05.2018 primär in der Datenschutzgrundverordnung (DSGVO) zu suchen ist.

Die vorliegende Untersuchung beinhaltet vor diesem Hintergrund eine umfassende Analyse der datenschutzrechtlichen Rahmenbedingungen am Maßstab der DSGVO. Das vernetzte, automatisierte und kooperative Fahren wirft eine Vielzahl von Problemen auf, die von der Klärung des Personenbezugs in einem kooperativen System mit zahlreichen Technologien und Beteiligten über die transparente und eindeutige Klärung und Festlegung der Verantwortlichkeiten und die Anforderungen der in Betracht kommenden Rechtsgrundlagen bis hin zur Auswahl risikoadäquater technischer und organisatorischer Maßnahmen reichen. Darüber hinaus sind die neuen Formen der Datenverarbeitung, die automatisiert im Hintergrund ablaufen, für den Nutzer weitgehend unsichtbar, so dass auch die Gewährleistung von Transparenz und Betroffenenrechten vor besonderen Herausforderungen steht.

Die Analyse umfasst auch die für die spezifischen Fragestellungen relevanten grundsätzlichen Auslegungsfragen der neuen Rechtslage, wie zum Beispiel der Auslegungsmaßstab der DSGVO im Mehrebenensystem zwischen der EU und den Mitgliedstaaten. Die Untersuchung zeigt zudem auf, dass viele der mit der DSGVO einhergehenden Änderungen inhaltlich nicht so revolutionär sind, wie es in der öffentlichen Diskussion den Anschein hat. Im Kern wurden die Regelungen der bislang geltenden Datenschutzrichtlinie 95/46 EG[4] in eine unmittelbar geltende Verordnung überführt und an bestimmten Stellen wurde im Interesse einer verbesserten Rechtsdurchsetzung nachjustiert. Die Kernprinzipien der Datenschutzrichtlinie, von denen sich viele bereits in der Datenschutzkonvention des Europarats aus dem Jahr 1981 finden, gelten auch unter Geltung der DSGVO weiter fort. In der DSGVO werden zudem die Betroffenenrechte gestärkt, die Sanktionsbefugnisse der Aufsichtsbehörden ausgeweitet und die Pflichten der für die Verarbeitung Verantwortlichen intensiviert. Die Verarbeitungsgrundsätze, zu denen auch die Grundsätze der Datenminimierung und der Zweckbindung gehören, sind nunmehr für alle verarbeitenden Stellen in Art. 5 Abs. 1 DSGVO verbindlich und sanktionsbewährt festgeschrieben und gemäß den Artt. 24, 25 und 32 DSGVO durch Ergreifen technischer und organisatorischer Maßnahmen umzusetzen. Zu nennen sind ferner die Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO sowie die Pflichten zu datenschutzfreundlicher Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen in Art. 25 DSGVO.[5]

---

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[5] Vgl. ErwG 11 DSGVO.

In technischer Hinsicht richten sich die Vorgaben der DSGVO nach dem Risiko für die Grundrechte und Grundfreiheiten der betroffenen Personen. Die DSGVO verlangt risikoadäquate technische und organisatorische Maßnahmen und nennt insoweit beispielhaft Pseudonymisierungslösungen. Eine wirksame Pseudonymisierung kann das Risiko für die Grundrechte der betroffenen Personen minimieren und eine ursprünglich unzulässige Datenverarbeitung legitimieren. Der risikobasierte Ansatz der DSGVO eröffnet damit Gestaltungsmöglichkeiten für risikomindernde, datenschutzfreundliche Innovationen.

In kooperativen Systemen besteht dabei die besondere Herausforderung, dass die Wirksamkeit der Pseudonymisierung nicht durch andere Identifikationsmöglichkeiten (beispielsweise durch Daten, die in gekoppelten IT-Systemen vorhanden sind oder im Zuge der Vernetzung anfallen, z.B. bei der Abrechnung von Ladevorgängen eines E-Fahrzeuges) aufgehoben werden darf. Eng mit dieser Frage verknüpft ist die Zuweisung der jeweiligen Verantwortungsbeiträge und die Erforderlichkeit und Grenzen spezialgesetzlicher Ausgestaltung in Fachgesetzen.

Herausforderungen bestehen auch im Bereich der Kommunikation zwischen Geräten (machine-to-machine, M2M), bei der die Fahrzeuge automatisiert ihre Daten mit anderen Fahrzeugen, Infrastrukturanbietern und weiteren Diensten austauschen, ohne dass hierzu eine Nutzeraktion erforderlich ist. Die Herstellung informationeller Waffengleichheit erfordert insoweit technische Lösungen, die Transparenz und Kontrolle der betroffenen Person über die auf ihre Person beziehbaren Informationen im Fahrzeug selbst gewährleisten.

Die Freiheit des Einzelnen, sich unerkannt, unbeobachtet und frei von A nach B bewegen zu können, darf nach dem Bericht der vom Bundesministerium für Verkehr und digitale Infrastruktur mit der Erstellung ethischer Leitlinien beauftragte Ethik-Kommission Automatisiertes und Vernetztes Fahren (im Folgenden: Ethik-Kommission) zudem nicht einer auf Effizienz beruhenden, zentralisierten digitalen Verkehrsinfrastruktur geopfert werden; Das könnte zu einer Totalüberwachung der Verkehrsteilnehmer führen.[6] *„Autonomes Fahren ginge zu Lasten autonomen Alltagshandelns. Der Zugewinn an Komfort und Verkehrssicherheit könnte dann nicht den Verlust an Freiheit und Autonomie rechtfertigen. Einer solchen Entwicklung ist daher durch die Förderung datenschutzfreundlicher Innovationen (Privacy by Design) sowie durch normative Ausgestaltungen entgegenzuwirken.“*[7]

[6] Ethik–Kommission, S. 24.

[7] Ethik–Kommission, S. 24.

Im Besonderen werden im vorliegenden Dokument die datenschutzrechtlichen Vorgaben dargestellt, die bei der Einbindung externer Dienstanbieter in die mit hoch- und vollautomatisierten Fahrfunktionen und speziellen Kommunikationstechnologien ausgestatteten Fahrzeugsystemarchitekturen zu beachten sind. Die Ethik-Kommission hat die dabei durch die Grundrechte gesetzten absoluten Grenzen möglicher Gestaltungen deutlich herausgestellt: *„Erlaubte Geschäftsmodelle, die sich die durch automatisiertes und vernetztes Fahren entstehenden, für die Fahrzeugsteuerung erheblichen oder unerheblichen Daten zunutze machen, finden ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer. Fahrzeughalter oder Fahrzeugnutzer entscheiden grundsätzlich selbst über Weitergabe und Verwendung ihrer anfallenden Fahrzeugdaten. Die Freiwilligkeit solcher Datenpreisgabe setzt das Bestehen ernsthafter Alternativen und Praktikabilität voraus. Einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, sollte frühzeitig entgegengewirkt werden."*[8]

Die DSGVO fordert in Art. 25 DSGVO ausdrücklich eine datenschutzfreundliche Produktgestaltung „by Design" und „by Default". Um Fehlentwicklungen zu verhindern, die später kaum noch oder nur unter erschwerten, insbesondere kostenintensiven Bedingungen rückgängig gemacht werden können, trägt hier auch der Gesetzgeber im Rahmen seiner staatlichen Schutzpflichten Verantwortung. Insbesondere bei eingriffsintensiven Verarbeitungen mit hohem Risiko müssen die allgemeinen Grundsätze der DSGVO rechtzeitig durch bereichsspezifische Vorgaben spezifiziert werden, um die notwendigen Impulse für einen effektiven, vorwirkenden Grundrechtsschutz sowie die für den Datenumgang benötigte Rechtssicherheit für alle Beteiligten zu gewährleisten.

[8] Ethik–Kommission, S. 12, ethische Regel Nr. 15.

2 DATENSCHUTZGRUNDVERORDNUNG

Regelungen zum Datenschutz finden sich sowohl auf europäischer als auch auf nationaler Ebene. Seit dem 25.05.2018 ist die Verordnung (EU) 2016/67[9] (Datenschutz – Grundverordnung, DSGVO) in den Mitgliedstaaten der EU unmittelbar anwendbar. Die DSGVO ist zwar bereits am 24.05.2016 und damit vier Jahre nach der Initiative für die Neuordnung des Europäischen Datenschutzrahmens in Kraft getreten. Sie ist allerdings gemäß Artikel 99 Abs. 2 DSGVO erst nach einer zweijährigen Übergangszeit seit dem 25.05.2018 anwendbar.

Die DSGVO ist überwiegend als Verordnung konzipiert. Im Gegensatz zu einer Richtlinie, die nur Zielvorgaben an den nationalen Gesetzgeber enthält, ist eine Verordnung gemäß Art. 288 Abs. 2 AEUV wie ein nationales Gesetz unmittelbar in den Mitgliedstaaten der Europäischen Union anwendbar. Eine Verordnung verfolgt das Ziel einer Vollharmonisierung des europäischen Rechtsraums und beansprucht daher gegenüber nationalen Gesetzen Anwendungsvorrang.

Zum Teil überlässt die DSGVO den Mitgliedstaaten aber auch Gestaltungsspielräume oder enthält keine abschließenden Regelungen. Insoweit strebt die DSGVO keine Vollharmonisierung an und hat nur den Charakter einer Richtlinie mit Zielvorgaben, die von den Mitgliedstaaten auf unterschiedliche Weise in nationales Recht umgesetzt werden können. Daher kann die DSGVO als Hybrid zwischen Verordnung und Richtlinie bezeichnet werden.[10]

Zum besseren Verständnis wird zunächst der für die Auslegung der DSGVO wichtige verfassungsrechtliche Hintergrund dargestellt, bevor eine vertiefte Auseinandersetzung mit den für das vernetzte, automatisierte und kooperative Fahren relevanten Vorgaben der DSGVO erfolgt.

2.1 Verfassungsrechtlicher Hintergrund

Nachfolgend werden die grundrechtlichen Vorgaben für Datenschutz, deren Vorgaben die DSGVO konkretisiert,[11] im Mehrebenensystem der Europäischen Union näher betrachtet und die Bedeutung der Grundrechte für die Auslegung der DSGVO untersucht.

---

[9] 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.

[10] Kühling/Martini et al, 2016, S. 1 f.

[11] Art. 1 Abs. 2 DSGVO, ErwG 1, 2 DSGVO.

2.1.1 Grundrechtliche Vorgaben für Datenschutz im Mehrebenensystem der EU

Grundrechtliche Vorgaben finden sich sowohl in den Artt. 7 und 8 der Charta der Grundrechte der Europäischen Union (GRCh), in Art. 16 Abs. 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) sowie in Art. 8 der europäischen Menschenrechtskonvention (EMRK). Auf nationaler Ebene werden diese Rechte im Grundgesetz (GG) über das Recht auf informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Bestandteile des Allgemeinen Persönlichkeitsrechts in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützt, wenn sie nicht einen spezielleren Schutzbereich beispielweise das Fernmeldegeheimnis in Art. 10 GG berühren.[12]

Das bislang geltende Datenschutzrecht ist sowohl auf europäischer als auch auf nationaler Ebene maßgeblich durch das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) aus dem Jahr 1983 geprägt, in dem die wesentlichen Leitlinien für das Grundrecht auf informationelle Selbstbestimmung herausgearbeitet wurden. Das Recht auf informationelle Selbstbestimmung ist seitdem, ebenso wie das später hinzugetretene Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, als Bestandteil des Allgemeinen Persönlichkeitsrechts anerkannt, das wegen seiner Nähe zur Menschenwürde besonderen Schutz genießt.

Das BVerfG legte in der ausführlichen Urteilsbegründung die Gefährdungen dar, die insbesondere mit immer neuen technologischen Möglichkeiten zur Erfassung personenbezogener Daten einhergehen: *„Auch der Umgang mit Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach seinem Ziel und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben. Insofern gibt es unter den Bedingungen der elektronischen Datenverarbeitung kein schlechthin, also ungeachtet des Verwendungskontexts belangloses personenbezogenes Datum mehr.“*[13]

Das Allgemeine Persönlichkeitsrecht umfasst nach den Urteilsgründen *„auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.“* [14] *„Dieses Recht flankiert und erweitert den*

---

[12] BVerfG, Beschluss v. 22.08.2006, –2 BvR 1345/03–, Rn. 66, (m.w.N.), juris.

[13] BVerfG, Urteil v. 11.03. 2008,–- 1 BvR 2074/05, 1 BvR 1254/07–, NJW 2008, 1505 (1506), Rn. 66 (m.w.N.), juris.

[14] BVerfGE 65, 1 ff., Rn. 170, openjur

grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit; es lässt ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen beginnen."[15]

Die Tragweite des Eingriffs in das allgemeine Persönlichkeitsrecht hängt daher nicht nur von der Art der Information, sondern vor allem von der Nutzbarkeit und den Verwendungsmöglichkeiten des Datums ab, die sich nach dem Zweck der Verarbeitung und den durch die eingesetzten Technologien möglichen Verarbeitungs- und Verknüpfungsmöglichkeiten richten: *„Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen."*[16]

„Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitung – voraus, dass dem Einzelnen Entscheidungsfreiheit […] einschließlich der Möglichkeiten gegeben ist, sich auch entsprechend dieser Möglichkeit zu verhalten."[17]

„Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden. Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist."[18]

Im Kontext des vernetzten und automatisierten Verkehrs entfällt der Schutzbedarf nicht bereits deshalb, weil die betroffene Information im öffentlichen Straßenraum allgemein zugänglich ist: *„Auch wenn der Einzelne sich in die Öffentlichkeit begibt, schützt das Recht auf informationelle Selbstbestimmung dessen Interesse, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatisierter Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwendung erfasst werden".*[19]

---

15 BVerfG, Urteil v. 11.03. 2008,– 1 BvR 2074/05, 1 BvR 1254/07–, NJW 2008, 1505 (1506), Rn. 63.

16 BVerfGE 65, 1, Rn. 176, openjur.

17 BVerfGE 65, 1 ff., Rn. 172, openjur.

18 BVerfG, Beschluss v. 22.08.2006, –2 BvR 1345/03-, Rn. 65 (m.w.N.), juris.

19 BVerfG, Urteil v. 11.03. 2008,– 1 BvR 2074/05, 1 BvR 1254/07–, NJW 2008, 1505 (1506), Rn. 67 (m.w.N.), juris.

Die Grundrechte wirken als objektive Werteordnung in das einfachgesetzliche Recht hinein, indem sie bei der Auslegung der einfachgesetzlichen unbestimmten Rechtsbegriffe oder bei Ermessens- und Handlungsspielräumen beachtet werden müssen und wirken so nicht nur auf die unmittelbar adressierte staatliche Gewalt, sondern auch mittelbar zwischen Privaten.[20] Insoweit entfalten die Grundrechte als staatliche Schutzpflichten ihre Wirkung auch in anderen Rechtsbereichen.[21] *„Die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht gebietet den zuständigen staatlichen Stellen vielmehr, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen.“*[22]

Weitere bereits auf das Volkzählungsurteil zurückgehende Grundsätze sind die Grundsätze der Datenminimierung und der Zweckbindung an konkrete und feststehende Zwecke, die den Grundsatz der Erforderlichkeit und der Verhältnismäßigkeit konkretisieren.[23] Aus den Grundsätzen der Zweckbindung und der Datenminimierung folgt das Gebot der Nichtverkettung. Ferner folgt daraus ein Verbot der Sammlung personenbezogener Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken.[24]

Das BVerfG stellte unmissverständlich klar, das aus den Grundrechten ein grundsätzliches Verbot der Erstellung von Voll- und Teilabbildern der Persönlichkeit folgt.[25] Daraus folgt auch das Gebot der informationellen Datentrennung, da die Zusammenführung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, insbesondere über einheitliche Kennzeichen, ein entscheidender Schritt wäre, den Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.[26]

Ferner besteht bei der Erhebung personenbezogener Daten zu statistischen Zwecken im öffentlichen Interesse, die keinen Personenbezug benötigen, ein Gebot der frühestmöglichen Anonymisierung und frühestmöglichen, vollständigen Löschung der personenbezogenen Erhebungs- bzw. Hilfstatsachen, verbunden mit wirksamen Vorkehrungen zur Verhinderung der De-Anonymisierung, zur Wahrung der strikten Geheimhaltung und zur Sicherung des Nachteilsverbots.[27] Insoweit müssen gesetzlich

---

[20] BVerfGE 7, 198 (206 f.); BVerfG, Urteil v. 11.06.1991, –1 BvR 239/90 –, Rn. 11.

[21] BVerfG, Beschluss v. 17.07.2013 – 1 BvR 3167/08, NJW 2013, 3086 (m.w.N).

[22] BVerfG 2006 –1 BvR 2027/02–, Rn. 33.

[23] BVerfGE 65, 1, Rn. 180, Rn. 185, Rn. 224, openjur.

[24] BVerfGE 65, 1, Rn. 184, openjur.

[25] BVerfGE 65, 1, Rn. 185 f., Rn. 196 f., openjur.

[26] BVerfGE 65, 1, Rn. 210, openjur.

[27] BVerfGE 65, 1, Rn. 187, Rn. 190, Rn. 218, openjur.

klar definierte Verarbeitungsvoraussetzungen geschaffen werden, die sicherstellen, dass der Einzelne nicht zum bloßen Informationsobjekt wird.[28] *„Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist."*[29]

Diese Grundsätze sind seitdem präzisiert worden und prägen auch heute noch sowohl das deutsche, als auch das europäische Datenschutzrecht.

Bereits mit dem Inkrafttreten der vor der DSGVO geltenden Datenschutzrichtlinie 95/46/EG im Jahr 1995 verlagerte sich die Zuständigkeit bei Streitigkeiten um die Auslegung der auf der Richtlinie beruhenden Datenschutzgesetze zum Teil vom BVerfG auf den EuGH, der die Einhaltung der grundrechtlichen Vorgaben nicht am Maßstab des Grundgesetzes, sondern anhand der Bestimmungen der Charta der Grundrechte der EU prüft. Der EuGH hat bei der Auslegung der Datenschutzrichtlinie 95/46 EG anhand dieser Vorgaben aber die Rechtsprechung des Bundesverfassungsgerichts inhaltlich fortgeführt und einen vergleichbaren Schutzmaßstab für die Grundrechte auf Datenschutz auf europäischer Ebene geschaffen.

Durch die mit Geltungserlangung der DSGVO geänderte Struktur in Form einer Verordnung verlagert sich die Zuständigkeit bei ungeklärten Auslegungsfragen weitgehend auf den EuGH, da die Prüfung gemäß Art. 51 GRCh, Art. 6 Abs. 1 EUV nun vorrangig am Maßstab der Charta der Grundrechte der EU, maßgeblich der Art. 7 und Art. 8 GRCh vorzunehmen ist.

Art. 8 GRCh und Art. 16 AEUV enthalten ein eigenständiges europäisches Grundrecht auf Datenschutz, wonach jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Dieses Recht steht nach der Rechtsprechung des EuGH mit dem in Art. 7 GRCh verankerten Recht auf Achtung des Privatlebens in engem Zusammenhang.[30] Danach hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Diese Grundrechte dürfen gemäß Art. 52 Abs. 1 GRCh nur aufgrund eines Gesetzes eingeschränkt werden, dass den Wesensgehalt der Grundrechte achtet und ein von der Union anerkanntes, dem Gemeinwohl oder Schutz gleichwertiger Rechte dienendes Ziel verfolgt. Ferner muss die Einschränkung erforderlich sein und dem Grundsatz der

---

[28] BVerfGE 65, 1, Rn. 185, openjur.

[29] BVerfGE 27, 1 Rn. 24, openjur.

[30] EuGH, Urteil v. 08.04.2014, Digital Rights Ireland und Seitlinger u.a., C– 293/12, EU:C:2014:238, Rn. 53.

Verhältnismäßigkeit genügen. Art. 8 Abs. 2 GRCh stellt zusätzliche Anforderungen auf. Personenbezogene Daten dürfen danach nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Bei der vorzunehmenden Abwägung sind auch die weiteren möglicherweise betroffenen Grundrechte der GRCh in die Betrachtung einzubeziehen und mit dem Recht auf Schutz personenbezogener Daten in einen angemessenen Ausgleich zu bringen.[31] Nur wenn die grundrechtlichen Vorgaben beachtet wurden, ist der mit der Verarbeitung personenbezogener Daten einhergehende Eingriff in den Schutzbereich der Grundrechte gerechtfertigt und der Eingriff ist grundrechtskonform.

Die Vorgaben der DSGVO dienen der Gewährleistung der Grundrechte der von der Verarbeitung ihrer personenbezogenen Daten betroffenen natürlichen Personen.[32] Die Datenschutzgesetze stellen damit Instrumente bereit, um die informationstechnischen Persönlichkeitsrisiken für die Grundrechte zu bewältigen und zielen darauf ab, eine minimalintensive Verarbeitung im Einzelfall zu ermöglichen, die ohne diese Vorgaben mit den Grundrechten nicht vereinbar und daher verboten wäre.

2.1.2 Grundrechtskonforme Anwendung der DSGVO

Um das mögliche Potential bei der Informationsverarbeitung ausschöpfen zu können, müssen – wie bereits dargestellt – bei der Auslegung und Anwendung der DSGVO die in den Grundrechten festgelegten Werte beachtet und in einen angemessenen Ausgleich gebracht werden. Dafür bedarf es einer Abwägung der betroffenen grundrechtlichen Belange.[33]

Die benötigte Flexibilität, um alle denkbaren grundrechtlichen Belange in den Wirkbereich einer Gesetzesnorm einbeziehen zu können, wird durch Einfügung sog. unbestimmter Rechtsbegriffe erreicht. Die DSGVO weist daher einen hohen Abstraktions- und Generalisierungsgrad auf und beinhaltet zahlreiche dieser wertausfüllungsbedürftigen Rechtsbegriffe. Beispiele für solche unbestimmten Rechtsbegriffe sind „Personenbezug“ bzw. „Identifizierbarkeit“, „technische und organisatorische Maßnahmen“ oder „berechtigte Interessen“. Diese Abstraktion und Generalisierung soll eine Anwendung über lange Zeiträume ermöglichen, ohne dass Gestaltungsspielräume übermäßig einschränkt werden. Beispielsweise darf ein Gesetz nicht vorschreiben, welche konkrete Software eingesetzt werden darf, sondern nur,

[31] ErwG 2, ErwG 4 DSGVO.

[32] ErwG 2 DSGVO.

[33] Siehe auch ErwG 4 S. 2 DSGVO.

welche Zielvorgaben die einzusetzende Software erfüllen muss. Zudem entstehen bei zu enger Umschreibung Schutzlücken, weshalb die DSGVO technikneutral formuliert ist.[34]

Der Rechtsanwender steht damit im konkreten Einzelfall vor großen praktischen Herausforderungen, weshalb nachfolgend zur Verfügung stehende Auslegungshilfen näher betrachtet werden.

2.1.2.1 Auslegungshilfen

Die komplexe, alle Interessen entsprechend der grundrechtlichen Wertvorgaben berücksichtigende Auslegung wird, soweit ungeklärte Rechtsfragen auftreten, durch die Verwendung unbestimmter Rechtsbegriffe auf den einzelnen Rechtsanwender übertragen. Die unbestimmten Rechtsbegriffe müssen im Wege der Gesetzesauslegung anhand einer grundrechtskonformen Auslegung am Maßstab der Grundrechte konkretisiert und so bestimmbar gemacht werden. Die Komplexität wird durch die Verzahnung von Europarecht und nationalem Recht in der DSGVO verstärkt.

Die Schaffung von Rechtssicherheit muss daher bei diesem komplexen Regelungswerk an erster Stelle stehen und ist für eine gelingende Anwendungspraxis essentiell. Die nachfolgend dargestellten Auslegungshilfen können hierfür herangezogen werden.

2.1.2.1.1 Materialien des Verordnungsgebers

Insbesondere der sorgfältigen und frühzeitigen Klärung, ob tatsächlich eine ungeklärte Rechtsfrage vorliegt, kommt wachsende Bedeutung zu. In vielen Fällen dürfte die Rechtsfrage bereits durch eine sorgfältige Auslegung zu klären sein. So kann nach der europarechtlichen Doktrin des „acte claire“ [35], das Auslegungsergebnis bereits offensichtlich sein, zum Beispiel weil bereits Interpretationshilfen wie verschiedene amtliche Sprachfassungen oder gesetzliche die Erwägungsgründe des Verordnungsgebers eine Lösung vorgeben. Die DSGVO enthält nämlich auch neben 99 verbindlichen Artikeln auch 173 Erwägungsgründe (ErwG), die neben den unterschiedlichen Sprachfassungen und der amtlichen englischen Fassung zur Auslegung herangezogen werden können.[36]

2.1.2.1.2 Rechtsprechung des EuGH zu den Zielen und Grundsätzen der Datenschutzrichtlinie 95/46/EG

Auslegungshilfen für die Auslegung der DSGVO finden sich auch in der Rechtsprechung des EuGH zur abgelösten Datenschutzrichtlinie 95/46/EG, deren Ziele und Grundsätze

---

[34] ErwG 15 DSGVO.

[35] Kühling/Drechsler, NJW 2017, 2950 (2952 f.).

[36] Vgl. BGH, Urteil v. 12.07.2018, -III ZR 183/17-, DE:BGH:2018:120718UIIIZR183.17.0, Rn. 87.

auch unter der DSGVO nach dem klaren Willen des Verordnungsgebers[37] fortgelten, da sie die grundrechtlichen Vorgaben der Artt. 7, 8 GRCh konkretisieren.

Nach der europarechtlichen Doktrin des sog. „acte éclairé („geklärter Fall“) ist daher stets zu prüfen, ob eine Streitfrage bei der Auslegung anhand bereits bestehender gesicherter Rechtsprechung des EuGH in vergleichbaren Fällen beantwortet werden kann, wobei die Fragen nicht vollkommen identisch sein müssen.[38] Die DSGVO behält die bereits unter der Datenschutzrichtlinie 95/46 EG geltenden, aus den Grundrechten folgenden Grundsätze und Prinzipien im Wesentlichen bei. Die zwischenzeitlich vorgenommene Konkretisierung dieser Werte und Prinzipien durch die Rechtsprechung des EuGH wurde zum Großteil in den Gesetzestext der DSGVO übernommen. Ein Beispiel hierfür ist das „Recht auf Vergessenwerden“ in Art. 17 DSGVO, das der EuGH bereits in einer Entscheidung im Jahr 2014[39] im Wege grundrechtskonformer Auslegung der Datenschutzrichtlinie 95/46 EG entnommen hat. Auch die Rechtsgrundlagen in Art. 6 Abs. 1 DSGVO beruhen auf der Richtlinie.[40] Die Rechtsprechung des EuGH zur Datenschutzrichtlinie 95/46/EG ist daher in wesentlichen Teilen auch bei der Auslegung der DSGVO zu beachten.

2.1.2.1.3 Leitlinien, Stellungnahmen und Beschlüsse der Abstimmungsgremien der Datenschutzaufsichtsbehörden

Da im Geltungsbereich der DSGVO nahezu ausschließlich der EuGH letztverbindlich über datenschutzrechtliche Auslegungsfragen entscheidet, ist mit langen Verfahrensdauern und damit lange bestehender Rechtsunsicherheit zu rechnen. So ist in einem prominenten Fall zur gewichtigen Frage der Anwendbarkeit des Datenschutzrechts erst neun Jahre nach der erstinstanzlichen Entscheidung eine rechtsverbindliche Entscheidung ergangen.[41] Den unabhängigen Aufsichtsbehörden kommt im Sinne effektiven, vorwirkenden Grundrechtsschutzes daher eine wichtige Unterstützungsfunktion bei der Auslegung zu.

Auslegungshilfen finden sich daher auch in den offiziellen Leitlinien, Stellungnahmen und Beschlüssen der Datenschutzberatungsgremien, wie der Artikel 29–Datenschutzgruppe, dem Europäischen Datenschutzausschuss (EDSA) oder auch –bei

---

37 ErwG 9 DSGVO.

38 Kühling/Drechsler, NJW 2017, 2950 (2952).

39 EuGH, Urt. v. 13.05.2014, Google Spain SL und Google Inc., C–131/12, EU:C:2014:317.

40 Vgl. BGH, Urteil v. 12.07.2018, -III ZR 183/17-, DE:BGH:2018:120718UIIIZR183.17.0, Rn. 75, 94.

41 Vgl. den Verfahrensgang: AG Berlin-Tiergarten, 13.08.2008 - 2 C 6/08-; LG Berlin, 07.04.2009 - 57 T 62/08-; BGH, 29.10.2009 - III ZB 40/09- ; LG Berlin, 31.01.2013 - 57 S 87/08-; BGH, 28.10.2014 - VI ZR 135/13-; Generalanwalt beim EuGH, 12.05.2016 - C-582/14-; EuGH, 19.10.2016 - C-582/14-; EuGH, 06.12.2016 - C-582/14-; BGH, 16.05.2017 - VI ZR 135/13-.

der Auslegung der nationalen Bestimmungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK). [42] Die Artikel 29–Datenschutzgruppe war ein aufgrund der Artt. 29, 30 der Datenschutzrichtlinie 95/46/EG gegründetes Beratungsgremium, dem die Datenschutzbehörden der EU, der Mitgliedstaaten und ein Vertreter der Europäischen Kommission angehörten. Sie ist am 25.05.2018 vom EDSA gem. Art. 68 DSGVO abgelöst worden. Der EDSA hat in seinen ersten Sitzungen bereits zahlreiche Stellungnahmen der Artikel 29–Datenschutzgruppe gebilligt.[43]

2.1.2.1.4 Nationale Grundrechte im Grundgesetz

Die Auslegung der DSGVO erfolgt, wie bereits erläutert, primär am Maßstab der Charta der Grundrechte der EU. Fraglich ist, ob daneben die nationalen Grundrechte bei der Auslegung der DSGVO weiterhin zu beachten sind.

Die Überprüfung von Maßnahmen der Europäischen Union unterfällt dem europarechtlichen Anwendungsvorrang[44] und wird nur in Ausnahmefällen vom BVerfG am Maßstab der nationalen Grundrechte überprüft.[45]

Gleichwohl sollten bei der Auslegung auch weiterhin die deutschen Grundrechte zumindest rechtsvergleichend berücksichtigt werden. Der Grundrechtsschutz auf EU-Ebene dient nämlich einem hohen Schutzstandard. Durch die GRCh soll der Schutz der Grundrechte gestärkt werden, vgl. Abs. 4 der Präambel der GRCh. In Art. 53 Var. 4 GRCh ist daher ausdrücklich festgeschrieben, dass keine Bestimmung der Charta als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten, wie sie durch die Verfassungen der Mitgliedstaaten anerkannt werden, ausgelegt werden darf. Soweit Widersprüche zwischen den unterschiedlichen Grundrechtsebenen bestehen, gilt nach Art. 53 GRCh, Art. 6 Abs. 1 EUV der jeweils höchste Schutzstandard. Der Schutz auf mehreren Ebenen soll folglich einen lückenlosen Grundrechtsschutz ermöglichen.

Darüber hinaus hat sich das BVerfG als Hüter des Grundgesetzes vorbehalten, die Prüfung unter gewissen Umständen wieder an sich zu ziehen und an den grundrechtlichen Vorgaben des Grundgesetzes zu messen, wenn ein Absinken des Grundrechtstandards auf europäischer Ebene unter den integrationsfesten Kern des Grundgesetzes droht.[46] Auch wenn das grundsätzlich zwischen BVerfG und EuGH

---

[42] Vgl. zu den Aufgaben des EDSA Art. 70 und ErwG 77 DSGVO.

[43] Vgl. EDSA, Endorsement 1/2018.

[44] EuGH, Urt. v. 26.02.2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 45.

[45] Vgl. BVerfG, Beschluss v. 15.05.2017, – 2 BvR 865/17–, Rn. 7 (m.w.N.), juris.

[46] BVerfG, Urteil v. 21.06.2016, – 2 BvE 13/13 – (m.w.N.), juris.

bestehende Kooperationsverhältnis[47] nicht abschließend beurteilt werden kann,[48] behält sich das BVerfG derzeit die Prüfung der sog. Verfassungsidentität einschließlich des grundrechtlichen Schutzstandards am Maßstab des Grundgesetzes weiterhin vor.[49]

Da ein Absinken des Schutzstandards unterhalb des Grundgesetzes daher sowohl auf europäischer als auch nationaler Ebene möglichst vermieden werden soll, bedarf es auch aus diesen Gründen bei der Auslegung und Anwendung der Bestimmungen der GRCh und der DSGVO einer rechtsvergleichenden Argumentation anhand der Maßstäbe des Grundgesetzes. Rückgriffe auf die frühere Praxis der Aufsichtsbehörden oder bestehende Rechtsprechung bedürfen aber künftig der Rückversicherung, dass kein anderweitiges einheitliches europäisches Verständnis entgegensteht.

2.1.2.2 Operationalisierung im Bereich des technischen Datenschutzes

Die Möglichkeiten für Grundrechtsverletzungen nehmen aufgrund des technologischen Wandels und der zunehmenden Digitalisierung zahlreicher Lebensbereiche beträchtlich zu. Die DSGVO trägt dem in erhöhten Anforderungen Rechnung.

Art. 24 DSGVO verpflichtet daher die Stelle, die für die Verarbeitung verantwortlich ist, die Einhaltung der DSGVO durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Dabei sind die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Person zu berücksichtigen. Art. 25 DSGVO fordert zudem ausdrücklich Maßnahmen zur datenschutzfreundlichen Technikgestaltung (data protection by design) und zu datenschutzfreundlichen Voreinstellungen (data protection by default). Art. 32 DSGVO verlangt Maßnahmen zur Sicherheit der Verarbeitung, um damit ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Nach den Artt. 25, 32 DSGVO sind bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen auch der Stand der Technik und die Implementierungskosten zu berücksichtigen.

Fraglich ist, wie diese Forderungen nach technischem Datenschutz operationalisiert werden können. Die maßgeblichen Artikel der DSGVO sind notwendigerweise abstrakt und technikoffen formuliert und schreiben gerade keine konkreten Maßnahmen vor. Der Rechtsanwender steht daher vor der Herausforderung, konkrete Maßnahmen aus

---

[47] Der latent bestehende Kompetenzkonflikt zwischen dem EuGH, der unbedingten Anwendungsvorrang proklamiert, und dem BVerfG, das von einem bedingten Anwendungsverzicht ausgeht, ruht zugunsten eines Kooperationsverhältnisses, vgl. BVerfGE 89, 155 ff.

[48] Ausführlich: Britz, 2014.

[49] Vgl. BVerfG, Beschluss vom 15.12.2015, -2 BvR 2735/14-, https://www.bundesverfassungsgericht.de.

den allgemeinen Vorgaben der DSGVO unter Beachtung der grundrechtlichen Vorgaben abzuleiten.

Dieses Spannungsverhältnis kann durch das Standard-Datenschutzmodell (SDM)[50] aufgelöst werden. Das SDM ist ein Konzept zur grundrechtsorientierten Beratung und Prüfung, das von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder empfohlen wird.[51] Es ist Bestandteil des BSI-Grundschutz-Kompendiums und wird von der Artikel 29–Datenschutzgruppe als Framework für die Durchführung der Datenschutzfolgenabschätzung nach Art. 35 DSGVO empfohlen.[52]

Im SDM werden die bei Datenverarbeitungsvorgängen zu schützenden Gewährleistungsziele definiert, Verfahren in Daten, IT-Systeme und Prozesse gegliedert und unterschiedliche Schutzbedarfe definiert. Ferner werden derzeit konkrete Schutzmaßnahmen abgestimmt, die in einem dem Modell angehängten Maßnahmenkatalog veröffentlicht werden sollen. Erste Bausteine stehen bereits für die Felderprobung zu Verfügung.[53] Das SDM ermöglicht damit die systematische Entwicklung und Prüfung konkreter Maßnahmen zum Schutz der Rechte betroffener Personen im Kontext von Datenverarbeitungsverfahren. Aus den gesetzlichen Vorgaben der DSGVO lassen sich Gewährleistungsziele ableiten, um die mit der Verarbeitung einhergehenden operativen Risiken in kompakter und methodisch zugänglicher Form explizit zu machen. Sieben Gewährleistungsziele (vgl. Abbildung 1) sind anerkannt.[54]

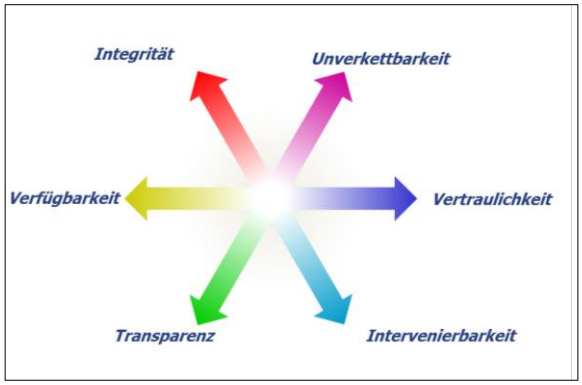

Abbildung 1: Sechs Gewährleistungsziele nach dem SDM + das zugrundeliegende Prinzip der Datensparsamkeit

[50] SDM, V.1.1.

[51] Weiterführende Informationen sind abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (letzter Abruf: 10.12.2018).

[52] Artikel 29-Datenschutzgruppe, WP 248 rev.01, Anhang 1, S. 26.

[53] Die einzelnen Bausteine sind abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (letzter Abruf: 10.12.2018).

[54] SDM, V.1.1; S. 12 ff.; Forum Privatheit, DSFA, S. 28.

Neben das grundlegende Prinzip der Datensparsamkeit, das stets zu beachten ist, treten die klassischen Datenschutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit. Daneben gelten die aus der IT-Sicherheit bekannten Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, allerdings mit einer anderen Schutzrichtung. Der Schutz der Grundrechte verlangt hier, anders als der Schutz von Geschäftsabläufen, dass alle aus der Datenverarbeitung entstehenden Risiken für Rechte und Interessen betroffener Personen, betrachtet werden müssen. Davon umfasst sind daher auch die von der für den Datenverarbeitungsvorgang verantwortlichen Organisation ausgehenden Risiken. Methodisch gesprochen muss sich damit nicht nur eine Person gegenüber einer Organisation durch überprüfbare Eigenschaften als vertrauenswürdig ausweisen, sondern auch eine Organisation gegenüber einer Person.[55]

Die Gewährleistungsziele bilden damit die wesentlichen Risiken systematisch ab, vor denen es durch eine angemessene Verfahrensgestaltung und Maßnahmen zu schützen gilt. Dabei stehen hinter jedem Schutzziel weitere, von ihnen abgeleitete Schutzziele, die die konkreten Vorgaben der DSGVO abbilden.[56]

Bei der Anwendung der Gewährleistungsziele ist zu beachten, das zwischen ihnen Wechselwirkungen bestehen und sie je nach Kontext unterschiedlich priorisiert werden müssen. Im Rahmen der Abwägungsentscheidung unterstützt eine Betrachtung nach Gewährleistungszielen, indem diese inhärenten Ziel-Konflikte erkennbar werden, z.B. zwischen dem Ziel der beweissicheren Datenhalteung (Integrität) und den durch die Intervenierbarkeit verkörperten Betroffenenrechten auf Löschung und Berichtigung. Ziel ist, die gegebenenfalls bestehenden Interferenzen unter Berücksichtigung der grundrechtlichen Vorgaben im jeweiligen Einzelfall in einen angemessenen und damit bestmöglichen Ausgleich zu bringen.

Der im Projektkontext entwickelte datenschutzrechtliche Anforderungskatalog[57] beruht ebenso wie die durchgeführte Datenschutzfolgenabschätzung[58] auf einem Vorgehen nach dem Standard-Datenschutzmodell. [59]

---

[55] SDM, V.1.1, S. 15.

[56] Weiterführend SDM, V.1.1, S.18–21.

[57] Vgl. das iKoPA–Deliverable 1v2 (im Erscheinen), abrufbar: https://ikopa.de/de/arbeitsergebnisse/ (letzter Abruf:14.12.2018).

[58] Vgl. das iKoPA–Deliverable 3.3 (im Erscheinen), abrufbar: https://ikopa.de/de/arbeitsergebnisse/ (letzter Abruf:14.12.2018).

[59] Vgl. zur Anwendung des SDM bereits das iKoPA–Deliverable 3.1, abrufbar: https://ikopa.de/de/arbeitsergebnisse/ (letzter Abruf:14.12.2018).

2.2 Anwendungsbereich der DSGVO

Zunächst ist der Anwendungsbereich der DSGVO zu klären. Der sachliche Anwendungsbereich erfordert gemäß Art. 2 DSGVO die Verarbeitung (2.2.1) personenbezogener Daten (2.2.2) In örtlicher Hinsicht gilt das Marktort- und Niederlassungsprinzip (2.2.3). Zudem sind einige Regelungsgegenstände vom Anwendungsbereich der DSGVO generell ausgenommen (2.2.4).

2.2.1 Datenverarbeitungsvorgang

Ein Datenverarbeitungsvorgang ist nach Art. 2 DSGVO jede ganz oder teilweise automatisierte Verarbeitung sowie jede nichtautomatisierte Verarbeitung soweit die Speicherung in einem Dateisystem beabsichtigt ist. Damit ist nahezu jeder Umgang mit personenbezogenen Daten erfasst. Art. 4 Nr. 2 DSGVO benennt ferner ausdrücklich das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Für jeden einzelnen der Verarbeitungsschritte ist der Personenbezug gesondert zu untersuchen.

2.2.2 Personenbezug

Der Begriff des Personenbezugs erfährt in der DSGVO mehrere Präzisierungen, weshalb die geänderte Rechtslage eingehender zu betrachten ist. Das umfasst die nachfolgende begriffliche Untersuchung des Personenbezugs sowie die Einordnung in den Kontext des automatisierten, vernetzten und kooperativen Fahrens (2.2.2.1) einschließlich pseudonymisierter (2.2.2.2) und anonymer (2.2.2.3) Daten.

Nach der neuen Legaldefinition in Art. 4 Nr. 1 DSGVO sind solche Informationen personenbezogen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Vollständig anonymisierte Daten unterfallen wie bisher nicht dem Anwendungsbereich des Datenschutzrechts. Wie schon zuvor können sich auch keine juristischen Personen (z.B. GmbH, OHG), sondern nur die hinter dieser Rechtsfigur stehenden Individuen auf den Schutz ihrer personenbezogenen Daten berufen.

Ausreichend für die indirekte Identifizierbarkeit nach Art. 4 Nr. 1 DSGVO ist bereits die Möglichkeit der Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Damit wird, der Rechtsprechung des EuGH folgend, der Begriff des Personenbezugs nun auch ausdrücklich im Gesetzeswortlaut weit definiert.

Insbesondere erkennt die DSGVO an, dass aufgrund der fortgeschrittenen technologischen Entwicklungen mit den Möglichkeiten zur Profilbildung, sei es über Kennungen, Kennnummern technischer Geräte oder Standortdaten, auch Möglichkeiten zur Identifizierung und damit ein Personenbezug einhergehen kann.[60]Die Identifizierung ist insbesondere möglich über technische Identifikatoren wie Gerätekennungen, Protokolle, Apps, sowie über Online Kennungen wie IP-Adressen oder Cookies oder auch Funkfrequenzkennungen.[61]

Die DSGVO adressiert damit den Schutzbedarf, der daraus resultiert, dass bei der Nutzung informations- oder kommunikationstechnologischer Komponenten in der Regel zahlreiche identifizierende Merkmale in Form von Metadaten entstehen, die regelmäßig auch an Dritte mit übertragen werden.[62] Diese im Rahmen der Nutzung von Internet oder Telekommunikation anfallenden digitalen Datenspuren können mit weiteren Informationen zur Profilbildung und damit zur Wiedererkennung und Identifikation genutzt werden.[63]

Profiling ist dadurch gekennzeichnet, dass eine automatisierte Bewertung persönlicher Aspekte anhand von Algorithmen erfolgt, insbesondere um persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsorte oder Ortswechsel einer Person vorherzusagen. Als Ergebnis können daraus z.B. Einkaufstipps, Routenvorschläge oder Bewertungen der Zahlungsbereitschaft erwachsen.[64]

Die Identifizierungsrisiken können aufgrund der beständigen Entwicklung von Analysemöglichkeiten, die immer neue Verkettungsmöglichkeiten durch zusammenhänge Muster sichtbar werden lassen, nicht abschließend benannt oder kategorisiert werden. Durch die DSGVO ist nun aber klargestellt, dass sowohl statische, als auch dynamische Attribute einen Personenbezug ermöglichen können. Die persönliche Identität kann insofern als eine Zusammensetzung statischer sowie dynamischer Merkmale verstanden werden, durch die die Person individualisiert bzw. wiedererkannt werden kann.

Statische Merkmale sind als gleichbleibende Attribute weitgehend unveränderbar und klar definiert. Darunter fallen neben Personenkennzeichen auch die spezifischen Personenmerkmale, Identifikationsnummern und auch technische Identifikatoren. Beispiele sind Name, Geburtstag, -Ort, biometrische Merkmale oder eindeutige

---

60 ErwGe 30, 26 S. 3 a. E. DSGVO.

61 ErwG 30 S.1 DSGVO.

62 Vgl. ErwG 30 DSGVO.

63 ErwG 30 S. 2 DSGVO.

64 Paal/Pauly-*Martini*, DSGVO, Art. 22, Rn. 21.

Kennzeichen wie die Fahrzeugidentifikationsnummer (FIN), das amtliche Kennzeichen, feststehende Gerätenummern (beispielsweise von separaten Speichereinheiten nach der eCall-Verordnung oder nach § 63a StVG), die Nummer der integrierten eSiM der von SIM-Karten aus gekoppelten Geräten oder auch feste Mac-Adressen.

Dynamische Attribute (z.B. Gewohnheiten, Vorlieben oder Nutzungsverhalten), hingegen unterliegen ständigen Änderungen. Insbesondere können neue digitale Technologien, wie Big-Data-Anwendungen, auch neue dynamische Techniken zur Identifikation hervorbringen, beispielsweise neue Methoden des Fingerprinting.[65] Die zur Erstellung eines Fingerprints genutzten Daten sind oft nicht unmittelbar personenbezogen, ermöglichen aber eine Wiedererkennung und damit ein Profiling. Die DSGVO adressiert dieses Risiko ausdrücklich und verlangt damit eine Änderung der bestehenden Praxis.[66]

2.2.2.1 Personenbezug von Fahrzeugdaten

Unstreitig liegt der Personenbezug der Fahrzeugdaten nach der gemeinsamen Erklärung des Verbands der Automobilindustrie und der Aufsichtsbehörden aus dem Jahr 2016 jedenfalls dann vor, wenn Informationen aus dem Fahrzeug mit der FIN oder dem amtlichen Kfz-Kennzeichen verknüpft werden.[67] Allerdings ist die Erklärung unvollständig und bezeichnet nur zwei evidente Identifikationsmöglichkeiten neben weiteren, die vor dem bereits dargestellten rechtlichen Hintergrund der DSGVO und der neueren EuGH-Rechtsprechung eine eingehendere Betrachtung erfordert. [68]

Im Kontext vernetzten, automatisierten und kooperativen Fahrens bestehen zahlreiche Identifikationsmöglichkeiten, die weit über die Fahrzeugidentifikationsnummer (FIN) oder das amtliche Kfz-Kennzeichen hinausgehen.

Zur Identifizierung können zunächst Besitzer- und Fahrerdaten, Authentifizierungsdaten inkl. biometrischer Daten (Sprache, Fingerabdrücke etc.) oder Gesundheitsdaten (z. B. Müdigkeitserkennung) dienen. Weitere Identifikatoren sind (neben Klarnamen und Kontaktdaten) das amtliche Kfz–Kennzeichen und die Fahrzeugidentifikationsnummer (FIN), aber auch SIM-Karten-Nummern (z. B. bei der fest verbauten eSIM oder von SIM-Karten in gekoppelten Geräten) oder sonstige Gerätekennungen wie feste MAC-Adressen oder SpeicherIDs (z. B. bei den gesetzlichen Pflichtspeichern nach der eCall-Verordnung oder nach § 63 a StVG). Auch mitübertragene Standortdaten oder für eine

---

[65] Strauß, DuD 2018, 497 (498).

[66] Vgl. ErwG 30 DSGVO.

[67] DSK und VDA, Gemeinsame Erklärung, S. 1 .

[68] Vgl. DSK und VDA, gemeinsame Erklärung, S. 1; OVG Münster, Urt. v. 19.10.2017, – 16 A 770/17–, NVwZ 2018, S. 742 ff. (744); Weichert, NZV 2017, 507 ff.

Registrierung verwendete Pseudonyme können die Widererkennung ermöglichen, ebenso wie individuelle Einstellungsmerkmale durch Methoden des Fingerprinting.[69]

Zusatzinformationen, die die Identifikation ermöglichen, können beabsichtigt, aber auch unbeabsichtigt als Folge der Nutzung der jeweils eingesetzten Technologie entstehen. Diese Informationen können im Fahrzeug selbst oder im Umfeld, vorhanden sein, etwa bei dem für eine Videoüberwachung (die künftig zur ergänzenden Standortbestimmung in Tiefgaragen oder Parkhäusern eingesetzt werden soll) oder für ein Kennzeichenscanning Verantwortlichen oder auch in intelligenten Verkehrsinfrastrukturelementen.

2.2.2.1.1 Kategorisierung anhand des Schutzbedarfs

Eine sinnvolle systematische Kategorisierung der Fahrzeugdaten anhand von Schutzbedarfsklassen existiert derzeit nicht.[70] Der Personenbezug und der Schutzbedarf eines Fahrzeugdatums darf insoweit auch nicht abstrakt bzw. isoliert betrachtet werden. Er richtet sich vielmehr nach dem Verwendungszusammenhang und den konkreten Verarbeitungsumständen. Die unterschiedlichen Versuche, Fahrzeugdaten anhand ihrer persönlichkeitsrechtlichen Relevanz zu kategorisieren[71] sind daher nur dann geeignet, den Personenbezug und den Schutzbedarf der Fahrzeugdaten abzubilden, wenn dabei die jeweils eingesetzte Technologie, in deren Rahmen die Daten verarbeitet werden sollen, auch in die Betrachtung miteinbezogen wird.

Eine Kategorisierung ohne Berücksichtigung der Umstände der Verarbeitung, wie der Zwecke und der eingesetzten technischen Mittel, legt Fehleinschätzungen nahe, da auch aus scheinbar harmlosen Daten je nach Verwendungskontext Nutzungs- oder Bewegungsprofile erstellt werden können. So sind etwa technische Fahrzeugdaten oder Kfz-Betriebswerte indirekt mit dem Fahrer verknüpft und ermöglichen Rückschlüsse auf die Fahrweise oder Benutzung des Fahrzeugs oder einzelner Bauteile. Sie können damit Aufschluss über den Gebrauch durch ihren Nutzer geben und die Erstellung von Verhaltens- oder Bewegungsprofilen ermöglichen. Diese Daten könnten in zivilrechtlichen Gewährleistungs- und Haftungsfällen oder sogar in Straf- oder Bußgeldverfahren[72] relevant werden, weshalb eine Erhebung dieser Daten in den Anwendungsbereich der DSGVO fällt.

---

[69] Ausführlich: Hansen, DuD 2015, 367 ff.

[70] Klink-Straub/Straub, NJW 2018, 3201 (3205).

[71] VDA, Datenschutzprinzipien, S. 2, Anhang; VDA, Position Zugang, S. 6 ff.

[72] Vgl. Artikel-29-Datenschutzgruppe, WP 252, S. 10.

Die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation unterteilt die zu betrachtenden Datenarten in folgende Kategorien:[73]

- vom Fahrzeug (einschließlich der im Fahrzeug eingebauten Informations- und Unterhaltungssysteme) gesammelten und verarbeiteten Daten;
- Daten, die zwischen dem Fahrzeug und den angeschlossenen persönlichen Geräten ausgetauscht werden;
- Daten, die zwischen dem Fahrzeug und externen Stellen (z. B. Infrastrukturbetreibern, Fahrzeugherstellern, Versicherungen und Kfz-Werkstätten) ausgetauscht werden;
- Daten, die an umliegende Fahrzeuge und Infrastruktureinrichtungen übertragen werden, um kooperative intelligente Verkehrssysteme (C-ITS) zu ermöglichen.

Nachfolgend werden einige dieser Datenkategorien und typische Verarbeitungssituationen näher auf ihre Persönlichkeitsrelevanz untersucht.

2.2.2.1.2 Daten, die bei der Nutzung von C-ITS-Diensten anfallen

Daten, die die C-ITS-Dienste von den Fahrzeugen aussenden, werden grundsätzlich als personenbezogene Daten angesehen.[74] Zu den Diensten gehören z.B. Warnungen bei bestimmten Ereignissen, Geschwindigkeitsbegrenzungen im Fahrzeug, Grünphasenprädiktion, kooperative Fahrzeugdaten, Informationen über Tankstellen und Ladestationen, Parkplatzinformationen sowie vernetztes und kooperatives Navigieren.[75]

2.2.2.1.3 Daten, die über das Mobilfunknetz versendet werden

Daten, die aus dem vernetzten Fahrzeug über das Mobilfunknetz erhoben werden, können sowohl direkt, als auch indirekt einer natürlichen Person zugeordnet werden. Da bei der Individualkommunikation über Kommunikationsnetze zahlreiche technische Identifikatoren anfallen.[76]

2.2.2.1.4 Automobile Fingerprinting

Daten, die für eine Profilbildung geeignet sind, ermöglichen in der Regel auch eine Identifizierung und sind damit Persönlichkeitsrelevant. Im Kontext des vernetzten, automatisierten und kooperativen Fahrens betrifft das grundsätzlich alle Daten, die entweder Rückschlüsse auf den Gebrauch durch einen Benutzer zulassen, oder

---

[73] IWGDP, vernetzte Fahrzeuge, S. 4.

[74] Europäische Kommission, COM(2016) 766 final, S. 9.

[75] Vgl. die Liste der C-ITS-Dienste für den Tag 1 und den Tag 1,5: Europäische Kommission, COM(2016) 766 final, S. 7.

[76] Hansen, DuD 2015, 367 (369).

Standortdaten oder umfangreiche Datensätze enthalten, wodurch eine Profilerstellung erleichtert wird.

Auch über einzelne, oft als „harmlos“ betrachtete Daten kann ein Bewegungsprofil erstellt werden. So kann bereits heute über die im Fahrzeug erzeugten Sensordaten in kurzer Zeit ein „Automobile Fingerprint“ erstellt werden, bei ausreichenden großen Datenmengen ist das bereits anhand der Daten nur eines Sensors, beispielsweise des Gaspedals, möglich.[77] Aus diesem Grund sind auch vermeintlich rein technische Fahrzeugdaten, die Aufschluss über ihren Verschleiß oder den Wartungszustand geben, personenbezogen.

Bei Standortdaten bestehen besonders viele Verkettungsrisiken. Bereits wenige Standortdaten können, unabhängig von der Frage, mithilfe welcher Technologie sie erhoben wurden, zum Profiling genutzt werden: Bereits vier Ortsdaten können ausreichen, um individuelle Bewegungsprofile zu erstellen.[78] Auch die Kenntnis von einem Startort und Geschwindigkeitsdaten reicht hierfür bereits aus.[79] Auch aus Verhaltensprofilen können Standortdaten und damit Bewegungsprofile abgeleitet werden.[80] Mit Mobilitätsdaten erstellte Bewegungsprofile sind zudem eindeutig voneinander unterscheidbar und können daher besonders leicht zur Wiedererkennung genutzt werden.[81] Ein solches Mobilitätsprofil enthält einen immensen Informationsgehalt, aus dem sich Wohnort, Arbeitsstätte, Freizeitaktivitäten und persönliche Kontakte ablesen lassen, die in ihrer Kombination identifizierend wirken.[82]

Die Persönlichkeitsrelevanz von Standortdaten, die bereits anhand weniger Standortdaten eine Personenbeziehbarkeit ermöglichen, wird vielfach übersehen und der Personenbezug der Fahrzeugdaten wird von den Verantwortlichen oftmals nicht wahrgenommen.[83] In der Folge unterbleibt u. a. die vorgesehene Unterrichtung der Betroffenen womit die Verarbeitung heimlich erfolgt und wesentlicher Verarbeitungsgrundsätze missachtet werden. Die heimliche Verarbeitung ist besonders eingriffsintensiv und damit schutzbedürftig.

Fingerprinting ist aber auch bei Informationen über die Ladespannung der Batterie eines Smartphones oder für Dienstanbieter bei frei ablesbaren Sensordaten eines

---

77 Enev et al 2016.

78 Montjoye et. al., 2013, 1 (3).

79 Gao et al., 2014, 975 ff.

80 Dewri et al., 2013, 267 ff.

81 Montjoye et. al., 2013, 1 ff.

82 Hansen, DuD 2015, 367 (369).

83 IWGDP, vernetzte Fahrzeuge, S. 11.

Smartphones möglich[84]. Eine Wiedererkennung ist daher auch über gekoppelte Geräte oder auch das Batteriemanagement von E-Fahrzeugen möglich.

Ferner ist ein Personenbezug auch anhand der als bloße Nebenfolge der Technologienutzung entstehenden Metadaten herstellbar.

Bei der Integration unterschiedlicher Technologien und Dienste in das Gesamtsystem des vernetzten und automatisierten Verkehrs ist ferner zu beachten, dass durch die Verbindung ein sozio-technisches System[85] entsteht, dass sich nicht nur aus der Summe der Einzelelemente, sondern auch der Beziehungen untereinander und zu ihrer Umwelt innerhalb und außerhalb des Systems zusammensetzt und damit neue Verkettungsmöglichkeiten schafft. Bei der Zusammenführung unterschiedlicher Kommunikationsansätze (z.B. Individualkommunikation über das Mobilfunknetz und das Internet, Rundfunktechnologie und verschiedene W-LAN-Standards, in-car Wi-Fi, Bluetooth und RFID-Technologien) auf einer gemeinsamen Plattform ergeben sich daher Identifikationsmöglichkeiten nicht nur isoliert aus der jeweiligen Technologie, sondern auch aus dem kombiniertem Einsatz. Die Gefahr der Wiedererkennung und Verknüpfung steigt zudem mit zunehmenden Analysemöglichkeiten und wachsendem Datenumfang.

2.2.2.1.5 Standortdaten

Besonders sensibel sind Standortdaten[86], die aufgrund des technologischen Fortschritts aus anderen Daten zunehmend leicht abgeleitet werden können. Insoweit ist zunächst auf die obigen Ausführungen zum Automobile Fingerpinting zu verweisen.

Der hohe Schutzbedarf von Standortdaten resultiert aus ihrer hohen Aussagekraft und dem damit verbundenen hohen Risiko der Erstellung von Persönlichkeitsprofilen.[87]

Neben dem Einsatz globaler Navigationssatelitenssysteme (GNSS) kann der Standort auch unter bestimmten Voraussetzungen mithilfe der W-LAN-Technik oder bei der Internetnutzung über die IP-Adresse bestimmt werden. Standortdaten werden zudem regelmäßig als Metadatum im Rahmen der Nutzung von Kommunikationstechnologien mitübertragen.

Risiken für Datenschutz und Privatsphäre gehen daher auch mit der Erhebung von gerätebezogenen Informationen und der Ableitung von Aufenthaltsinformationen aus

---

84 Michaelsky et. al., 2015; Watanabe et. al. 2017.

85 Strauß, DuD 2018, 497 (498).

86 Zum hohen Schutzbedarf bei Standortdaten vgl. BGH, Beschluss v. 8.2.2018, - 3 StR 400/17 -, Rn. 6 (a. E.); Zur entsprechenden Anwendbarkeit von § 98 TKG: Weichert, SVR 2014, 201 (206).

87 Zur hohen Aussagekraft von Ortsdaten vgl. BVerfG, Urteil v. 11.03.2008, - 1 BvR 2074/05 -, Rn. 87 f., juris.

den Verkehrsdatensätzen der Mobilfunkanbieter einher.[88] Verkehrsdatensätze erzeugt beispielsweise jedes mobile Empfangsgerät beständig zur bloßen Sicherung der Betriebsbereitschaft in der jeweiligen Funkzelle beim Telekommunikationsanbieter. Aus den Verkerhsdatensätzen können präzise Bewegungsprofile abgeleitet werden. [89]

Die Verfolgung von Aufenthaltsorten ist aber auch für Andere als den Nutzer innerhalb der Reichweite einer drahtlosen Basisstation, beispielweise bei Wi-Fi-Zugangspunkten, anhand der übertragenen Signale, die oft feststehende technische Identifier wie MAC-Adressen enthalten, derzeit möglich.[90] Ferner soll beim automatisierten Fahren ein Technologiemix zum Einsatz kommen, der neben der Ortung durch die Fahrzeugsysteme selbst auch eine Standortbestimmung durch das Umfeld bzw. die Infrastruktur, beispielsweise in Parkhäusern oder Tiefgaragen ermöglicht. Der Schutzbedarf steigt dabei mit der steigenden Verfügbarkeit der Standortdaten erheblich an, da sich der Aussagegehalt und die Missbrauchsgefahr der Standortdaten weiter erhöht.

Die Persönlichkeitsrelevanz von Standortdaten, die bereits anhand weniger Standortdaten eine Personenbeziehbarkeit ermöglichen, wird vielfach übersehen und der Personenbezug der Fahrzeugdaten wird von den Verantwortlichen oftmals nicht wahrgenommen.[91] In der Folge unterbleibt u. a. die vorgesehene Unterrichtung der Betroffenen womit die Verarbeitung heimlich erfolgt und wesentlicher Verarbeitungsgrundsätze missachtet werden. Die heimliche Verarbeitung ist besonders eingriffsintensiv und damit schutzbedürftig.

2.2.2.1.6 Technische Fahrzeugdaten

Anders als Maschinendaten in der industriellen Fertigung haben Fahrzeuge und jedes Fahrzeugteil stets einen Benutzer, dessen Verhalten sie offenbaren können. So sind etwa technische Fahrzeugdaten oder Kfz-Betriebswerte indirekt mit dem Fahrer verknüpft und ermöglichen Rückschlüsse auf die Fahrweise oder Benutzung des Fahrzeugs oder einzelner Bauteile. Diese Daten haben einen hohen Schutzbedarf, wenn sie nicht vollständig anonymisiert erhoben werden, da sie zur Erstellung von Profilen genutzt werden können, um damit Garantie- oder Gewährleistungsansprüche abzuwehren. [92] Auch im Straf- und Bußgeldverfahren könnten sie herangezogen werden.[93]

---

88 IWGDP, Verfolgung von Aufenthaltsorten.

89 Zum Schutzbedarf von TK-Daten vgl. BVerfG, Beschluss v. 13. 11. 2010 – 2 BvR 1124/10 –, Rn. 18, juris.

90 IWGDP, Verfolgung von Aufenthaltsorten.

91 IWGDP, vernetzte Fahrzeuge, S. 11.

92 Vgl. Balzer/ Nugel, NJW 2016, 193 ff.

93 Weichert, NZV 2017, 507 (513), Artikel-29-Datenschutzgruppe, WP 252, S. 10.

Zudem dürfte es aufgrund der zunehmenden Analyse- und Verkettungsmöglichkeiten in kooperativen und vernetzten Systemen äußerst schwierig werden, Daten vollständig zu anonymisieren. Eine nicht der DSGVO unterfallende Erhebungsmöglichkeit von anonymen Daten aus dem Fahrzeug wäre wünschenswert, ist aber derzeit nicht ersichtlich, da jedenfalls identifizierende Metadaten bei der Nutzung von Kommunikationstechnologien anfallen und auch beim manuellen Auslesen regelmäßig die FIN übertragen wird.[94]

2.2.2.2 Pseudonymisierte Daten und Zusatzwissen Dritter

Auch pseudonymisierte Daten sind nach der genannten Definition in Art. 4 Nr. 5 DSGVO, personenbezogen, da sie durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können und auf eine identifizierbare Person beziehbar sind.[95] Die Pseudonymisierung kann zwar als Maßnahme zur Risikominderung eingesetzt werden, aber das Risiko für die Grundrechte in der Regel nicht vollständig minimieren.[96]

Die DSGVO setzt damit die höchstrichterliche Rechtsprechung um, die den langwierigen Streit um den Maßstab zur Klärung der Personenbeziehbarkeit entschieden hat. Im Kern ging es um die Frage, ob nur das Wissen des Verantwortlichen, oder auch Zusatzwissen Dritter bei der Klärung des Personenbezugs zu berücksichtigen ist. Der EuGH[97] und ihm folgend der Bundesgerichtshof (BGH)[98] haben entschieden, das nicht nur das Wissen des Verantwortlichen, sondern auch das Zusatzwissen Dritter in die Prüfung des Personenbezugs einzubeziehen ist, sofern dem Verantwortlichen Mittel, die vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden können, zur Verfügung stehen. Bei der Beurteilung, ob ein Mittel vernünftigerweise zur Verfügung steht, sind alle objektiven Mittel zu berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, wie beispielsweise das Aussondern.[99] Maßgeblich sind insoweit alle objektiven Faktoren (wie die Kosten der Identifizierung und der erforderliche Zeitaufwand), ebenso wie die zum Zeitpunkt der Verarbeitung verfügbaren Technologien und technologischen Entwicklungen.[100]

---

94 Vgl. Hansen, DuD 2015, 367 ff.

95 ErwG 26 S. 2 DSGVO.

96 ErwG 28 DSGVO.

97 EuGH, Urteil v. 19.10.2016, Breyer, C–582/14, ECLI:EU:C:2016:779.

98 BGH, Urteil v. 16.05.2017, – VI ZR 135/13 –, NJW 2017, 2416, beck-online.

99 ErwG 26 DSGVO.

100 ErwG 26 DSGVO.

2.2.2.2.1 Rechtliche Zugriffsmöglichkeiten auf das Wissen Dritter

Nach der neueren Rechtsprechung des EuGH sind auch die rechtlichen Zugriffsmöglichkeiten auf das Zusatzwissen Dritter zu beachten. [101] Diese Rechtsprechung, die zur Datenschutzrichtlinie 95/46 EG ergangen ist, gilt fort.[102]

Der EuGH stellt in der genannten Entscheidung klar, dass auch rechtliche Möglichkeiten, auf das bei Dritten vorhandene Zusatzwissen zur Identifizierung zugreifen zu können, verfügbare Mittel zur Identifikation darstellen. Konkret entschied der EuGH, dass neben statischen auch dynamische IP-Adressen personenbezogen sind, da zur Identifizierung verfügbare rechtliche Mittel zur Verfügung stehen. Mit Hilfe der zuständigen Behörden (beispielweise durch Stellen einer Strafanzeige und entsprechendem behördlichem Tätigwerden) ist nämlich die Zuordnung der IP-Adresse zu einem konkreten Nutzer und damit eine Identifikation möglich, da die Behörden Zusatzinformationen, über die der Internetzugangsanbieter verfügt, ermitteln können.[103] Der BGH folgt der Auffassung des EuGH und führt aus, dass Personenbezug nicht nur dann vorliegt, wenn – im Falle einer bereits eingetretenen Schädigung – Strafanzeige bei den Strafverfolgungsbehörden erstattet werden könne, sondern auch im Falle der drohenden Schädigung mithilfe der für die Gefahrenabwehr zuständigen Behörden, der Verfassungsschutzbehörden des Bundes und der Länder, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes.[104]

Die englische Originalfassung des genannten EuGH-Urteils legt zudem nahe, dass das rechtliche Mittel nicht genutzt werden muss, sondern die abstrakte Erreichbarkeit in Form des grundsätzlichen Bestehens eines Auskunftsanspruchs bereits ausreicht, selbst wenn dafür ein richterlicher Beschluss erforderlich ist.[105] Dafür streitet auch die ständige Rechtsprechung des BVerfG, die maßgeblich auf die Nutzbarkeit und Verwendungsmöglichkeit eines Datums aufgrund der mit der Verarbeitung verfolgten Zwecke und der eingesetzten Technologien abstellt.[106]

Die Aussagen der beiden Gerichte lassen sich auch auf andere rechtliche Zugriffsbefugnisse übertragen, beispielweise weil ein Auskunftsrecht vertraglich vereinbart wurde oder sich aus einer Rücksichtnahme- oder Treuepflicht ergibt.

---

[101] EuGH, Urteil v. 19.10.2016, Breyer, C–582/14, ECLI:EU:C:2016:779.

[102] ErwG 26, 9 DSGVO.

[103] EuGH, Urteil v. 19.10.2016, Breyer, C–582/14, ECLI:EU:C:2016:779.

[104] BGH, Urteil v. 16.05.2017, – VI ZR 135/13 –, NJW 2017, 2416, Rn. 24, beck-online.

[105] OVG Münster, Urt. v. 19.10.2017, – 16 A 770/17 –, NVwZ 2018, S. 742 ff. (744 m.w.N.).

[106] BVerfGE 65, 1, Rn. 176, openjur; BVerfG, Urteil v. 11.03. 2008, –1 BvR 2074/05, 1 BvR 1254/07 –, NJW 2008, 1505 (1506), Rn. 62 f., Rn. 66.

Fraglich ist die Grenzziehung für zu berücksichtigendes berücksichtigungsfähiges Zusatzwissen Dritter durch rechtliche Zugriffsmöglichkeiten. Dabei ist zu beachten, dass jedenfalls über das Stellen einer Strafanzeige, wie vom EuGH und BGH ausdrücklich benannt, die Identifizierung ermöglicht wird. Daher ist eine Grenze nur bei rechtlichen Kenntnisnahme- bzw. Aussageverboten anzunehmen, z.B. bei Berufsgeheimnisträgern.[107] Zeugnis- und Auskunftsverweigerungsrechte begründen gegenüber staatlichen Organen keine solchen Verbote, sondern eröffnen lediglich eine Nichtaussagemöglichkeit, die auch ausgeschlagen werden kann. Auch das OVG Münster stellt daher darauf ab, dass ein gesetzliches Verbot die Identifizierung der betroffenen Person verbieten muss.[108] Rechtliche Mittel stellen damit regelmäßig erreichbare Mittel dar, wenn die Information nicht durch rechtliche Verbote vor einer Kenntnisnahme geschützt ist.

2.2.2.2.2 Pseudonymisierung durch Auftragsverarbeiter

Im Kontext des vernetzten, automatisierten und kooperativen Fahrens ist die bereits dargestellte Entscheidung des EuGH zu den rechtlichen Zugriffsmöglichkeiten von hoher Relevanz. Die früher vertretene Auffassung[109], dass durch dauerhafte organisatorische Trennung technischer Einzeldaten des Fahrzeugs von Identifizierungsmerkmalen eine faktische Anonymisierung erreicht werde, wenn entweder einer der Datensätze oder bei Verschlüsselung der Codeschlüssel an eine andere Stelle, etwa einen Auftragsverarbeiter, ausgelagert wird, kann nach der oben dargestellten höchstrichterlichen Rechtsprechung nicht mehr vertreten werden.

Für die Auflösungsmöglichkeit der darin liegenden Pseudonymisierung ist insbesondere unerheblich, ob der Verantwortliche selbst oder lediglich ein Dritter über die Identifikationsmöglichkeit bzw. den Schlüssel zu Re-Identifikation verfügt, solange der Zugriff bzw. die Kenntnisnahme nicht durch ein gesetzliches Verbot abgesichert ist. Aufgrund seines Weisungsrechts existieren für den Verantwortlichen stets rechtliche Mittel zur Kenntnisnahme gegenüber dem Auftragsverarbeiter, vgl. Art. 28 Abs. 3 lit. a, lit. g, Art. 29 DSGVO. Die Daten des Auftragsverarbeiters sind daher für den Verantwortlichen stets personenbezogen.

2.2.2.3 Anonyme Daten und Risiko der De-Anonymisierung

Nur bei anonymisierten Daten besteht mangels Personenbeziehbarkeit grundsätzlich kein Schutzbedarf und die DSGVO ist nicht anwendbar.[110]

---

[107] Roßnagel, ZD 2018, 243 (245, 247).

[108] OVG Münster, Urt. v. 19.10.2017, – 16 A 770/17 –, NVwZ 2018, S. 742 ff. (743).

[109] Ernsthaler, SIM-TD D5.5, S. 23 f.

[110] ErwG 26 S. 6 DSGVO.

Die DSGVO verlangt aber von dem für die Verarbeitung anonymer Daten von dem potentiell Verantwortlichen, dass er die technologischen Entwicklungen beobachtet und rechtzeitig wirksame Vorkehrungen gegen eine De-Anonymisierung trifft.[111]

Um das Risiko einzuschätzen, ist eine Differenzierung zwischen absoluter und gesetzlich fingierter Anonymität hilfreich. Die DSGVO bezieht nämlich, wie auch schon die Datenschutzrichtlinie 95/46 EG, nicht nur absolute Anonymität, sondern auch eine gesetzliche Fiktion in die Begriffsbestimmung anonymer Daten mit ein. Während bei absoluter Anonymität ein Personenbezug nicht mehr herstellbar ist, ist in den Fällen, in denen die Identifizierung mit einem unverhältnismäßigen Aufwand für den potentiell Verantwortlichen verbunden wäre, eine Identifizierung theoretisch weiterhin denkbar, jedoch so unwahrscheinlich, dass die Annahme einer gesetzlichen Fiktion gerechtfertigt erscheint.[112] Der technologische Wandel bedingt in Zeiten von Big Data und Ubiquitous Computing, dass bereits heute diese gesetzlich fingierte Anonymität den Regelfall darstellt.

Das Risiko der Identifikation ist bei der gesetzlich fingierten Anonymität aufgrund des raschen technologischen Wandels gegenüber der absoluten Anonymität erhöht, da die Identifizierungsmöglichkeiten sowohl infolge der wachsenden technischen Analysemöglichkeiten zur Verkettung von Datenbeständen als auch mit den zunehmenden Identitätsschatten infolge der Digitalisierung unterschiedlichster Lebensbereiche stetig anwachsen.[113] Die Identifizierungsgefahr ist bei Standortdaten besonders hoch und eine Anonymisierung besonders leicht umkehrbar.[114]

Dieses Risiken muss der potentiell Verantwortliche fortlaufend überwachen, neu bewerten und rechtzeitig angemessene Schutzmaßnahmen ergreifen, wobei der Stand der Wissenschaft maßgeblich ist.

2.2.2.3.1 Beobachtungspflicht hinsichtlich technologischer Entwicklungen

Die Beobachtungspflichten umfassen nach der DSGVO begrifflich *„verfügbare Technologien und technologische Entwicklungen“* [115], wodurch klargestellt wird, dass nicht nur der Stand der Technik, sondern bereits der Stand der Wissenschaft zu beobachten und zu berücksichtigen ist. Bei Änderungen in der Risikobewertung müssen rechtzeitig Vorsorgemaßnahmen zur Risikominderung ergriffen werden können.[116]

---

[111] ErwG 26 S. 4, S. 5 DSGVO.

[112] Ausführlich: Artikel 29-Datenschutzgruppe, WP 216.

[113] Strauß, DuD 2018, 497 (498).

[114] Vgl. Zang/ Bolot, 2011.

[115] ErwG 26 S. 4 a.E.

[116] BVerfG, Beschluss v. 08.08.1978, –2 BvL 8/77 –, Rn. 108 (juris).

Der Begriff des Standes der Wissenschaft ist fortschrittlicher als der Stand der Technik und zwingt zur Auswertung neuester Erkenntnisse und fachlicher Meinungen verschiedener Experten: *„Dabei muss diejenige Vorsorge gegen Schäden getroffen werden, die nach den neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird.“*[117] *„Die erforderliche Vorsorge wird mithin nicht durch das technisch gegenwärtig Machbare begrenzt“*.[118] Ist die Vorsorge technisch noch nicht machbar, ist folglich ein Personenbezug anzunehmen.

2.2.2.3.2 Temporär gespeicherte Fahrzeugdaten

In Bezug auf Fahrzeugdaten, die nur temporär erhoben werden, ist ein Personenbezug am Maßstab des deutschen Grundgesetzes nur dann zu verneinen, wenn das erhobene Datum unmittelbar nach der Erfassung technisch wieder spurenlos und ohne Auswertungsmöglichkeit gelöscht wird, wobei zusätzlich rechtlich und technisch sichergestellt sein muss, dass die Daten bis zur vollständigen Löschung tatsächlich anonym bleiben.[119]

Das Bundesverfassungsgericht hat zudem kürzlich klargestellt, dass auch eine vollautomatiserte Auswertung ohne direkte Kenntnisnahme durch den Verantwortlichen und anschließendem Verwerfen der Nichttreffer einen empfindllichen Eingriff in das Persönlichkeitsrecht bedeuten kann, besonders wenn der Abgleich anlasslos, flächendeckend und heimlich erfolgt.[120] Nach dieser Entscheidung liegt der Schluss nahe, das auch nur temporär gespeicherte Datensätze, die aber von den Fahrezugsystemen ausgewertet werden und zur Grundlage von Entscheidungen mit nicht unerheblichen Konsequenzen für die betroffene Person dienen könnten, als personenbezogen anzusehen sind.

Darüber hinaus wäre eine sofortige Löschung der Fahrzeugdaten, die beispielweise zu Zwecken des automatiserten Fahrens erhoben werden, zwar denkbar. Es ist aber zu erwarten, dass die zunehmende Automatisierung auch umfangreichere Speicherpflichten mit sich bringen wird, um nachprüfen zu können, ob das System korrekt funktioniert hat und den damit einhergehenden vielfältigen Beweis- und

[117] Vergl. zum Begriff Stand der Technik BVerfG, Beschluss v. 08.08.1978, –2 BvL 8/77 –, Rn. 108.

[118] BVerfG, Beschluss v. 08.08.1978, –2 BvL 8/77 –, Rn. 109.

[119] BVerfG, Urteil v. 11.03. 2008,–- 1 BvR 2074/05, 1 BvR 1254/07–, NJW 2008, 1505 (1506f. Rn. 62, Rn. 68) ; BVerfG,Beschluss v. 18.12.2018 ,-1 BvR 142/15-, Rn. 43, 48, 50, juris.

[120] BVerfG,Beschluss v. 18.12.2018 ,-1 BvR 142/15-, juris.

Speicherinteressen zu genügen.[121] Auch sonstige Dienstanbieter werden sich in der Regel auf Speicher- und Nachweisinteressen berufen. Somit ist der Personenbezug auch bei nur temporär gespeicherten Fahrzeugdaten regelmäßig anzunehmen.

2.2.2.3.3 Erhebung personenbezogener Daten in Anonymisierungsabsicht

Die DSGVO ist auch dann anwendbar, wenn nach der Erhebung des personenbezogenen Datums eine Anonymisierung angestrebt wird. Die bloße Absicht, personenbezogene Daten zunächst zu erheben und sogleich nach Erhalt zu anonymisieren, führt nämlich nicht dazu, dass bereits die ursprüngliche Erhebung als anonym gilt. Die Anonymisierung tritt nämlich erst durch eine weitere, im Erhebungszeitpunkt nicht wirksame, sondern bloß beabsichtigte Verarbeitung eines zum Verarbeitungszeitpunkt personenbeziehbaren Datums ein. Dadurch werden Risiken für die Persönlichkeitsrechte eröffnet, vor denen das Datenschutzrecht gerade schützen soll. Die Erhebung personenbeziehbarer Daten in Anonymisierungsabsicht benötigt daher, ebenso wie der Anonymisierungsvorgang selbst, eine ausdrückliche gesetzliche Erlaubnis.[122] Die DSGVO ist auch in diesem Fall anwendbar. Ein Verfahren muss daher auch technisch eine anonyme Erhebung von Anfang an aus dem Fahrzeug gewährleisten, um nicht den Schutzbereich der DSGVO zu eröffnen.

Daher muss beispielsweise der Hersteller des Fahrzeugs, eines Bauteils oder einer sonstigen Fahrzeugkomponente, der zur Produktverbesserung die technischen Daten aus einem Fahrzeug anonym verarbeiten möchte, sowohl bei der Erhebung als auch bei der Anonymisierung selbst die Vorgaben der DSGVO beachten, insbesondere da die Daten bis zu ihrer vollständigen Anonymisierung auch Aufschluss über die Benutzung durch den Nutzer geben können.

2.2.2.3.4 Abgrenzung zur Verordnung für einen freien Verkehr nicht–personenbezogener Daten in der EU

Die Abgrenzung zwischen personenbezogenen und anonymen Daten wird künftig vor dem Hintergrund der neuen Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union[123], über die kürzlich eine politische Einigung erzielt wurde,[124] zusätzliche Bedeutung erlangen. Der europäische

---

[121] Vgl. die weitreichenden Speicher- und Übermittlungspflichten an die Straßenverkehrsbehörden und an Private nach dem zukunftsweisenden § 63a Abs. 1, Abs. 2 StVG bei hoch- und vollautomatisierten Fahrfunktionen.

[122] Vgl. BVerfGE 65, 1, Rn. 190, openjur.

[123] Europäische Kommission, COM (2017) 495 final.

[124] Vgl. die entsprechende Pressemitteilung, abrufbar unter: http://europa.eu/rapid/press-release_IP-18-4227_de.htm (letzter Abruf: 20.11.2018).

Gesetzgeber betont zwar das Exklusivitätsverhältnis im Verhältnis zur DSGVO, da personenbezogene Daten nicht unter die Verordnung fallen sollen, sondern nur anonyme Daten aus industriellen Fertigungsanlagen oder sonstige vollständig anonymisierte Daten.[125] Durch den großen Anwendungsbereich der gesetzlich fingierten Anonymität sind bei einer extensiven Anwendung dieser neuen Verordnung aber erhöhte Risiken für die Persönlichkeitsrechte absehbar.[126] Um Schutzlücken zu vermeiden, ist daher bei nicht absolut anonymisierten Daten im Zweifel von einem Schutzbedarf im Sinne der DSGVO auszugehen.[127]

Ferner gelten bei gemischten Datensätzen, die sowohl personenbezogene als auch anonymisierte Daten enthalten, die Vorgaben der DSGVO.[128]

Die Verordnung dürfte daher nur einen kleinen Anwendungsbereich haben und nur bei absolut anonymen Daten, beispielweise in der industriellen Produktion gelten. Technische Fahrzeugdaten fallen in der Regel nicht in den Anwendungsbereich, da sie stets Aufschluss über ihren Gebrauch durch einen oder mehrere bestimmte Nutzer geben können und eine Profilbildung ermöglichen. Die „Maschinendaten“ eines Fahrzeugs können stets auch Bezug zu dem Fahrer, Eigentümer, Halter oder Mitfahrern haben und haben Bezug zu ihren Nutzern, insbesondere zu der Person, die die Maschine entsprechend ihrer Bedürfnisse konfiguriert, lenkt und steuert.[129]

2.2.2.4 Zwischenergebnis

Ob Personenbezug vorliegt, ist zusammenfassend nach einem relativen Maßstab zu untersuchen. Stellt die Verknüpfung einer Information mit identifizierendem Zusatzwissen ein Mittel dar, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann, liegt Personenbezug vor. Das Wissen kann auch bei Dritten vorliegen. Ferner sind rechtliche Zugriffsmöglichkeiten, insbesondere die Möglichkeiten zur Einschaltung von Strafverfolgungs- oder Gefahrenabwehrbehörden, zu berücksichtigen.

Anonyme Daten, die nicht der DSGVO unterfallen, liegen nur dann vor, wenn absolut kein Personenbezug mehr herstellbar ist oder die Identifizierung einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, oder die Identifizierung der betreffenden Person gesetzlich verboten wäre, so dass das Risiko einer Identifizierung vernachlässigbar erscheint. In diesem Fall kann man auch von einer

---

[125] Europäische Kommission, COM (2017) 9 final, S. 9 f.

[126] DAV, Stellungnahme 4/2018, S. 6 f.

[127] Europäische Kommission, COM (2017) 9 final, S. 9 f.

[128] Europäische Kommission, C (2018) 5356 final, S. 3.

[129] DAV, Stellungnahme 4/2018, S. 7.

gesetzlichen Fiktion oder gesetzlich fingierter Anonymität sprechen, bei der ein höheres Restrisiko der De-Anonymisierung besteht.

Das Risiko der De-Anonymisierung trägt der potentiell Verantwortliche, wobei er bereits die neuesten technologischen Entwicklungen berücksichtigen muss, um rechtzeitig geeignete Schutzmaßnahmen zu ergreifen. Auch rechtliche Risiken, wie beispielweise die offenen Rechtsfragen bei automatisierten und vernetzten Fahrzeugen, oder absehbare Gesetzesänderungen müssen beobachtet werden. Die getroffenen Vorkehrungen und ihre Effizienz unterliegen der Rechenschaftspflicht des Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO.

In Bezug auf die unterschiedlichen Fahrzeugdaten besteht Personenbezug regelmäßig bereits aufgrund des Umfangs der Datensätze, enthaltener Standortdaten oder der bei der Nutzung digitaler Technologien, z. B. Kommunikationstechnologien, entstehenden Metadaten. In der Regel sind auch vermeintlich rein technische Fahrzeugdaten personenbezogen und die vielfältigen Auswertungsmöglichkeiten können erhebliche Konsequenzen für die betroffenen Personen haben. Damit bleibt festzuhalten, dass die sämtliche Fahrzeugdaten grundsätzlich in den Anwendungsbereich der DSGVO fallen.

2.2.3 Marktort- und Niederlassungsprinzip

In örtlicher Hinsicht unterliegen unterliegen alle Anbieter auf dem europäischen Markt gemäß Art. 3 DSGVO den Regeln der DSGVO.[130] Der örtliche Anwendungsbereich ist zunächst dann eröffnet, wenn die Verarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU stattfindet. Eine Niederlassung besteht unabhängig von einer eigenen Rechtspersönlichkeit bereits dann, wenn eine Tätigkeit effektiv und tatsächlich durch eine feste Einrichtung in der EU ausgeübt wird.[131]

Eine Niederlassung in der Union ist dann erforderlich, wenn einer betroffenen Person innerhalb der EU entgeltlich oder unentgeltlich Waren oder Dienstleistungen angeboten oder ihr Verhalten beobachtet werden soll.

2.2.4 Ausnahmen vom Anwendungsbereich

Einige Bereiche sind in Art. 2 DSGVO von dem Anwendungsbereich der DSGVO ausgenommen, da sie in speziellen Vorschriften geregelt sind oder der sog. Haushaltsausnahme unterfallen.

---

[130] DSK, KP Nr. 7.

[131] ErwG 22 DSGVO.

2.2.4.1 Bereichsausnahmen für spezielle Rechtsbereiche

Eigenen Regeln unterliegt zunächst die Verarbeitung personenbezogener Daten im Bereich der nationalen Sicherheit, sowie zur Strafverfolgung und Gefahrenabwehr. Zeitgleich mit der DSGVO hat auch die Richtlinie (EU) 2016/680[132] (Polizei-Richtlinie) für den Sonderbereich der Polizei und Justiz Geltung (Art. 2 lit. d DSGVO) erlangt. Für die EU-Organe existieren unionsrechtliche Sondervorschriften.

Die bestehenden staatlichen Zugriffs- und Verwendungsmöglichkeiten sind jedoch nach der bereits dargestellten jüngsten EuGH-Rechtsprechung für die Beurteilung des Personenbezugs und des datenschutzrechtlichen Schutzbedarf der Fahrzeugdaten relevant.[133]

2.2.4.2 Persönliche und familiäre Tätigkeiten

Die Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO schließt Verarbeitungen zur Ausübung ausschließlich persönlicher und familiärer Tätigkeiten vom Anwendungsbereich der DSGVO aus. Die Norm ist aus der Datenschutzrichtlinie 95/46 EG übernommen worden. Nach der Rechtsprechung des EuGH werden dabei nur solche Tätigkeiten erfasst, die ausschließlich zum Privat- und Familienleben von Privatpersonen gehören.[134] Bei Bezug der Datenverarbeitung zu wirtschaftlichen oder beruflichen Tätigkeiten gilt die DSGVO.[135] Die DSGVO gilt auch dann, wenn die Tätigkeit sich *„auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der Sphäre desjenigen gerichtet ist, der die Daten verarbeitet.“*[136]

Die Ausnahme gilt nicht für diejenigen Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung im Bereich der Haushaltsausnahme bereitstellen.[137] Dienstanbieter oder Hersteller können sich daher unter keinen Umständen auf die Haushaltsausnahme berufen.

---

[132] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[133] Weiterführend: Gagzow, Gundula/ Körffer, Barbara, Fahrzeugdaten als Beweismittel im Straf- und Bußgeldverfahren, in: Roßnagel, Alexander/ Hornung, Gerrit (Hrsg.), Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, im Erscheinen.

[134] EuGH, Urteil v. 10.07.2018, C-25/17, EU:C:2018:551; EuGH, Urt. v. 11.12.2014, Rynes, C-212/13, EU:C:2014:2428, Rn. 30.

[135] ErwG 18 S. 1 DSGVO.

[136] EuGH, Urteil v. 10.07.2018, C-25/17, EU:C:2018:551, Rn. 42 (m.w.N.).

[137] ErwG S. 3 DSGVO.

Fraglich ist aber, ob der jeweilige Halter oder auch der Fahrer sich auf die Haushaltsausnahme berufen kann, soweit durch die Fahrzeugsensorik das Umfeld oder die Fahrzeuginsassen erfasst und analysiert werden. Die Ausnahme vom Anwendungsbereich bei rein persönlichen oder haushaltsbezogenen Tätigkeiten ist eng auszulegen, und erfordert, dass die Verarbeitung sich strikt innerhalb des Fahrzeugs vollzieht, und dass der Autofahrer die volle Kontrolle darüber innerhalb des Fahrzeugs auch tatsächlich ausüben kann.[138] Sobald die Daten den Herrschaftsbereich des Fahrzeugs verlassen, ist die Ausnahme jedenfalls nicht mehr einschlägig. Dann wäre in einem weiteren Schritt die tatsächlich bestehende Verantwortung für den Datenverarbeitungsvorgang zu prüfen.

Im Kontext des vernetzten, automatisierten und kooperativen Fahrens dürfte die Haushaltausnahme daher nur einen sehr geringen Anwendungsbereich haben, beispielweise wenn Adressdaten anderer Personen in das Fahrzeugsystem eingebracht werden und es nicht verlassen.

2.3 Datenschutzrechtliche Verantwortung nach der DSGVO

Im komplexen Ökosystem vernetzter und automatisierter Fahrzeuge ist die Klärung der datenschutzrechtlichen Verantwortung besonders bedeutsam. Zahlreiche Akteure können bereits an der Datenerhebung beteiligt sein und noch mehr haben Interesse an einer Verwendung der Fahrzeugdaten, so dass mit einer steigenden Anzahl von datenverarbeitenden Stellen zu rechnen ist. Nach der Untersuchung spezialgesetzlicher Verantwortungszuweisungen (2.3.1) werden die Grundsätze zur Bestimmung der Verantwortung unter besonderer Beachtung der neuesten EuGH-Rechtsprechung zur gemeinsamen Verantwortung (2.3.2), gefolgt von einer Übersicht über die Pflichten des oder der Verantwortlichen (2.3.3) dargestellt.

2.3.1 Spezialgesetzliche Verantwortungszuweisungen

Eine für den Bereich vernetzter und automatisierter Fahrzeuge anzustrebende spezialgesetzliche Festlegung der Verantwortlichkeit im Sinne des Art. 4 Nr. 7, 2. Halbsatz (HS) DSGVO ist derzeit (noch) nicht ersichtlich.

Nach dem Messstellenbetriebsgesetz (MsbG) besteht aber eine gesetzliche Verantwortungszuweisung im Bereich der Infrastruktur intelligenter Ladesäulen, ebenso besteht eine Spezialzuweisung für das automatische Notrufsystem nach der eCall–Verordnung.

Neben die Anbieter der Dienstleistungen treten bei Diensten, die die Vernetzung des Fahrzeugs nutzen, auch die Netzbetreiber, die die jeweilige

[138] Artikel 29-Datenschutzgruppe, WP 252, S. 10.

Kommunikationsinfrastruktur bereitstellen und nach speziellen Regeln für damit einhergehende Datenverarbeitungen verantwortlich sind. In Zukunft kommen neue Kommunikationstechnologien hinzu, die teilweise eine direkte Kommunikation ohne Eingreifen eines Netzbetreibers zwischen Fahrzeugen oder Straßeninfrastruktureinrichtungen ermöglichen sollen (V2X- und V2V-Kommunikation).[139] Ob der Betrieb der für die V2X–Kommunikation benötigten straßenseitigen Infrastrukturanlagen den Mobilfunkanbietern oder der öffentlichen Hand obliegen wird, ist derzeit noch nicht absehbar und bedarf einer spezialgesetzlichen Regelung, ebenso wie die V2V–Kommunikation über Ad-hoc-Netzwerke.

Im Kontext von intelligenten Verkehrssystemen sollen in Zukunft Verkehrsmanagementzentralen und verschiedene Mobilitätsdienste – beispielsweise in den Bereichen Straßenverkehrssicherheit, Verbindung zwischen Fahrzeug und Verkehrsinfrastruktur oder Verkehrs- und Frachtmanagement – mit den Datenanbietern von Verkehrsinformationen kooperativ und vernetzt zusammenwirken.[140] Die zu schaffenden Gesetze sollten dann auch die Verantwortlichkeiten und Rollen der Beteiligten festlegen und ihre jeweiligen Pflichten klar definieren.

2.3.2 Bestimmung der Verantwortung nach der DSGVO

Für den Datenverarbeitungsvorgang verantwortlich ist, soweit eine spezielle Regelung nicht vorliegt, nach der Legaldefinition in Art. 4 Nr. 7, 1. HS DSGVO diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Jeder, der an dem Verarbeitungsvorgang beteiligt ist, ist nach den Vorgaben der DSGVO damit entweder (gemeinsam) Verantwortlicher oder Auftragsverarbeiter. Das maßgebliche Abgrenzungskriterium hierfür ist, ob eine Stelle allein oder mit anderen über die Zwecke und Mittel (mit-) entscheidet.[141]

Insoweit kommen zunächst Fahrzeughersteller, Zulieferer von Fahrzeugteilen oder Software, Werkstätten (freie und vertraglich an die Fahrzeughersteller gebundene) Wartungsunternehmen, Mietwagenanbieter, Car-Sharing-Anbieter, Leasingunternehmen, Fuhrparkbetreiber, sowie Anbieter von Unterhaltungs- und Mobilitätsdiensten in Frage, aber auch Halter oder der jeweilige Fahrer des Fahrzeugs, soweit er Kenntnis von der Verarbietung hat und Einfluss auf sie nehmen kann.

---

[139] IWGDP, vernetzte Fahrzeuge, S. 1.

[140] ausführlich BMVI, IVS–Aktionsplan „Straße“, S. 27 ff.

[141] Artikel 29-Datenschutzgruppe, WP 169, S.22; Kühling/Buchner-*Hartung*, DSGVO, Artikel 26, Rn.11.

Die Fahrzeugdaten sind dabei aufgrund ihres vielfältigen Aussagegehalts für Anbieter besonders interessant, deren Geschäftsmodelle auf datengetriebenen und/oder ortsbasierten Diensten aufsetzen. So bieten Versicherungen bereits Pay-As-You-Drive-Versicherungstarife an, die das Fahrverhalten in die Prämienberechnung einbeziehen. Im Bereich der Mobilitätsdienste haben vor allem Anbieter von Navigationsdiensten, intelligenten Routenplanern oder nutzerbezogenen Zusatzinformationen (z.B. Anzeigen und gegebenenfalls das Reservieren von Ladestationen entlang der Route, Stauinformationen, Grünphasenprädiktion (Green Light Optimal Speed Advisory, GLOSA) oder das Anzeigen freie Parkplätze) Interesse an den Fahrzeugdaten. Die unterschiedlichen Dienstleistungen können anhand ihrer Nutzungswecke klassifiziert werden.[142] Die Zahl der Interessierten und der verfolgten Zwecke nimmt dabei stetig zu. Die Prüfung der Verantwortlichkeit am Maßstab der DSGVO muss daher im Einzelfall erfolgen und sollte sich an vermehrt an Fallbeispielen orientieren, um eine pausschale Betrachtung möglichst zu vermeiden.

Durch das Zusammenwachsen von Auto und Netz ist, wie die Erfahrungen im Zusammenhang mit dem Internet veranschaulichen, zu befürchten, dass sich Beteiligte ihrer Verantwortung entziehen und ihre Geschäftsmodelle auf einer datenschutzwidrigen Datenverarbeitung aufbauen.[143] In Bezug auf Fahrzeugdaten wird die datenschutzrechtliche Verantwortung vielfach übersehen, weil bereits der oftmals herstellbare Personenbezug verkannt wird.[144]

2.3.2.1 Gemeinsame Verantwortung

Im kooperativen System des vernetzten und automatisierten Verkehrs mit einer Vielzahl von Akteuren stellt sich in erhöhtem Maß die Frage der gemeinsamen Verantwortung.

Die DSGVO übernimmt den Grundsatz der gemeinsamen Verantwortung aus der Datenschutzrichtlinie 95/46 EG.[145] Legen mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemäß Art. 26 Abs. 1 S. 1 DSGVO gemeinsam Verantwortliche. Sie sind verpflichtet, ihre jeweiligen Verpflichtungen in transparenter Form nach Art. 26 Abs. 1 S. 2, Abs. 3 DSGVO festzulegen. Die betroffene Person kann ihre Rechte gemäß Art. 26 Abs. 3 DSGVO gegenüber jedem der Verantwortlichen geltend machen.

Die Formen gemeinsamer Verantwortung sind vielfältig und können unterschiedlich stark verteilt sein, insbesondere ist es ausreichend, wenn sich die einzelnen Akteure nur

---

[142] Ausführlich: IWGDP, vernetzte Fahrzeuge, S. 1 f.

[143] Hansen, DuD 2015, S. 370 (m.w.N.).

[144] IWGDP, vernetzte Fahrzeuge, S. 11.

[145] DSK, KP Nr. 16.

für Zwecke, nur für Mittel oder nur Teile davon verantwortlich zeichnen.[146] In der DSGVO wird beispielhaft eine horizontale Zusammenarbeit bei der gemeinschaftlichen Erstellung eines Systems genannt,[147] wodurch deutlich wird, dass auch eine Aufgabenteilung verschiedener Verarbeitungsschritte durch verschiedene Akteure darunter fallen kann.[148] Zu prüfen ist, inwieweit in mehrpolaren Verhältnissen wie bei vernetzten und automatisierten Fahrzeugen ein an dem Verarbeitungsvorgang Beteiligter faktisch einen bestimmenden Einfluss ausübt.[149]

Der EuGH hat kürzlich klargestellt, dass für die Annahme einer gemeinsamen Verantwortung eine Zugriffsmöglichkeit auf die personenbezogenen Daten nicht erforderlich ist, sondern eine Beteiligung an der Entscheidung über die Zwecke und Mittel der Verarbeitung ausreicht.[150] Insbesondere der Umstand, dass ein Dienstanbieter eine von einem anderen betriebene Plattform und dazugehörige Dienstleistungen zur Datenverarbeitung nutzt, befreit ersteren nach dem EuGH nicht von der Beachtung seinen datenschutzrechtlichen Pflichten.[151]

Gemeinsam Verantwortliche müssen ihre jeweiligen Aufgaben nach der DSGVO genau festlegen und die Zuständigkeiten für die verschiedenen Maßnahmen, mit denen die Risiken für die Schutzgüter bearbeitet und die Rechte und Freiheiten natürlicher Personen geschützt werden sollen, nach Art. 26 Abs. 1 S. 2 DSGVO genau beschrieben und der betroffenen Person mitgeteilt werden. Davon ungeachtet gilt gemäß Art. 26 Abs. 3 DSGVO jeder Beteiligte gegenüber der betroffenen Person als allein Verantwortlicher und muss ihre geltend gemachten Rechte vollständig erfüllen. Intransparente Gestaltungen der Vereinbarungen oder Umgehungen der Verantwortungen führen mithin dazu, dass jeder, der gemeinsam Verantwortlichen die volle Verantwortung für die Information der betroffenen Personen sowie das Bestehen und die Zwecke der anderen übernehmen muss.[152]

Je nach Ausgestaltung im Einzelfall könnte die Anwendung der Kriterien zur gemeinsamen Verantwortung zum Beispiel auf den Fahrzeughersteller oder den jeweiligen Dienstanbieter, aber auch auf weitere Beteiligte wie Infrastrukturanbieter zutreffen. Grundsätzlich ist derjenige, der ein Geschäftsmodell betreibt, auch

---

146 Kühling/Buchner-*Hartung*, DSGVO, Artikel 26, Rn.15f.

147 ErwG 92 DSGVO.

148 Kühling/Buchner-*Hartung*, DSGVO, Artikel 26, Rn.13.

149 Artikel 29-Datenschutzgruppe, WP 169, S. 14.

150 EuGH, Urteil v. 05.06.2018, Wirtschaftsakademie Schleswig–Holstein, C–210/16, EU:C:2018:388, Rn. 38, 39.

151 EuGH, Urteil v. 05.06.2018, Wirtschaftsakademie Schleswig–Holstein, C–210/16, EU:C:2018:388, Rn. 40.

152 Artikel 29-Datenschutzgruppe, WP 252, S. 13.

verantwortlich im Sinne des Gesetzes. Insbesondere bei Plattformlösungen mehrerer Beteiligter wird die Abgrenzung aber zunehmend komplex und es verbieten sich pauschale Betrachtungen. So kann beispielweise auch der Hersteller des Fahrzeugs, der eine eSIM ins Fahrzeug integriert und auch gegenüber dem Fahrer abrechnet, als Verantwortlicher im Sinne des TKG anzusehen sein.[153]

2.3.2.1.1 Plattformlösungen

Besonders problematisch ist die klare Festlegung der Verantwortlichkeiten bei der Einbindung von Plattformanbietern in die Datenverarbeitung.

Bei dem Begriff des Plattformbetreibers handelt es sich aus juristischer Perspektive um einen Kunstbegriff, der durch den 10. Rundfunkänderungsstaatsvertrag als Rechtsbegriffe eingeführt wurde. Der Begriff beschreibt das Phänomen, dass sich zwischen Sender und Empfänger im Rundfunkbereich vermehrt Dritte als Intermediäre schalteten und sich als Gatekeeper gerierten.[154] Denkbar ist eine Instrumentalisierung von Standards oder Schnittstellen, aber auch durch die Programmführung.[155]

Häufig werden Plattformbetreiber als neue Akteure in der Wertschöpfungskette beschrieben, was bei einem Wechsel des Geschäftsmodells durchaus gerechtfertigt erscheint. Auch im Bereich vernetzter und automatisierter Fahrzeuge erweitern die Infotainment-Systeme zunehmend ihren Funktionsumfang: So geht es bei datenbasierten Geschäftsmodellen nicht mehr nur um einzelne Datenzugriffe, sondern um umfassende Mobilitätssysteme und oftmals um die Ausdehnung digitaler Plattformstrategien auf den Straßenverkehr. Wenn die neutrale Rolle eines reinen Informationsvermittlers verlassen wird, indem Informationen gebündelt (durch Erhebung und Verarbeitung der Kommunikationsinhalte) oder im eigenen Namen an die Endkunden vermarktet werden (aus Endkundensicht wird dadurch eine technische Transportdienstleistung (mit-) erbracht), kommen auch andere datenschutzrechtliche Vorgaben zur Anwendung.

Aus datenschutzrechtlicher Perspektive stellt sich bei Plattformbetreibern die praktische Frage, klar zu erkennen, wer (gemeinsam) Verantwortlicher ist. Der EuGH hat kürzlich entschieden, dass bei der Nutzung von Datenverarbeitungsdiensten auch zu eigenen Zwecken auf Plattformen eines anderen Verantwortlichen regelmäßig eine gemeinsame Verantwortung vorliegt. Dabei ist nicht erforderlich, dass jeder Verantwortliche

[153] Stender-Vorwachs/ Steege, MMR 2018, 212 ff.

[154] Assion, 2015, S. 1.

[155] Assion, 2015, S. 121 f.

tatsächlich Zugriff auf die Daten erhält.[156] Ausreichend ist bereits, dass dem Beteiligten ein eigener Entscheidungsspielraum zukommt, etwa indem ausdifferenzierte Kriterien für die Auswahl der technischen und organisatorischen Mittel fehlen.[157] Eine gemeinsame (Mit-)Verantwortung des Plattformbetreibers könnte daher auch dann vorliegen, wenn die Fahrzeugdaten im Rahmen einer von ihm betriebenen Infrastruktur aufbereitet und an weitere Akteure übermittelt werden oder zugleich eigene Zweck verfolgt werden, zum Beispiel um Aussagen über den Verschleiß von Teilen oder zur Optimierung von Services zu treffen, oder wenn die Weitergabe personenbezogener Daten zum Geschäftsmodell erhoben wird. Die Frage der Verantwortlichkeit ist in jedem konkreten Einzelfall zu klären.

Eine große Herausforderung im Kontext vernetzter und automatisierter Fahrzeuge liegt ferner in der Gewährleistung von Nachvollziehbarkeit der Verantwortlichkeiten. Es entsteht ein komplexes Ökosystem mit mehrpoligen Rechtsverhältnissen und zahlreichen Interessen, die letztlich zu einer unübersichtlichen Gemengelage führen können. Die Integration einer hersteller- und betreiberunabhängigen Kommunikationsplattform in die lokalen Fahrzeugsysteme, über die auf die Fahrzeugdaten zugegriffen werden kann, bietet hier kare Vorteile. Dadurch wird eine klare Verantwortungszuweisung an den jeweiligen auf die Daten zugreifenden Dienstanbieter ermöglicht. Unklare und intransparente Verantwortungsgeflechte, wie sie bei der Einbindung von Plattformanbietern oft bestehen, können so vermieden werden.

Neben dem datenzugreifenden Dienstanbieter ist die Verantwortung für die Generierung der Fahrzeugdaten durch die Fahrzeugsysteme im Fahrzeug selbst zu klären. Das eröffnet die Frage, ob die lokale Verarbeitung in den Fahrzeugsystemen eine Mitverantwortung begründen kann, und wem diese obliegt.

2.3.2.1.2 Offline-Verarbeitung/ lokale Verarbeitung

Zu klären ist, wer für die sogenannte offline-Verarbeitung lokal im Fahrzeug die Verantwortung trägt, wenn keine Datenübertragung an ein Server-Backend erfolgt. Die Frage ist auch relevant zur Klärung einer bestehenden Mitverantwortung neben dem Dienstleister, soweit die Fahrzeugsysteme in die Verarbeitung einbezogen sind.

In der gemeinsamen Erklärung von DSK und VDA wird angedeutet, dass es an einem Verantwortlichen für den offline-Verarbeitungsvorgang fehle, da eine tatsächliche Zugriffsmöglichkeit auf die Daten, die lokal im Fahrzeug abgelegt sind, regelmäßig nicht

---

[156] EuGH, Urteil v. 05.06.2018, Wirtschaftsakademie Schleswig–Holstein, C–210/16, EU:C:2018:388, Rn. 38, 40.

[157] VGH München, Beschluss v. 26.09.2018, – 5 CS 18.1157 –, BeckRS 2018, 25018, Rn. 16 f.

vorliege.[158] Dies ist vor dem Hintergrund der kürzlich ergangenen Entscheidung des EuGH zur gemeinsamen Verantwortung neu zu bewerten, da der EuGH darin Grundsätze für die Prüfung der Verantwortung festgelegt hat.[159]

Der Begriff des Verantwortlichen ist nach dem EuGH weit zu bestimmen, um Schutzlücken zu vermeiden und einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten. [160] Die Situation, dass zwar eine Datenverarbeitung stattfindet, aber kein Verantwortlicher existiert, soll daher nach der gesetzlichen Konzeption gerade vermieden werden. Bei der offline-Verarbeitung kommen als Verantwortliche entweder der Halter bzw. Fahrer oder der Hersteller des Fahrzeugs in Betracht.

2.3.2.1.2.1 Fahrzeughalter und Fahrzeugführer

Gegenüber (Mit–) Fahrern und weiteren Fahrzeugnutzern könnten der Fahrzeughalter oder auch der jeweilige Fahrer gegebenenfalls datenschutzrechtlich (mit–) verantwortlich sein.

Grundsätzlich entscheidet der Halter über die Nutzung und die Art der Verwendung des Fahrzeugs und damit auch darüber, wer das Fahrzeug fährt und die Fahrdaten erzeugt. In Betracht kommt deshalb je nach Konstellation eine alleinige oder gemeinsame Verantwortung.[161] Die Frage ist besonders relevant bei privater Dienstwagennutzung eines Arbeitnehmers oder gewerblichen Car-Sharing-Angeboten und muss in jedem Einzelfall geprüft werden.

Ist auch der jeweilige Fahrezugführer (im Folgenden: Fahrer) in der Lage, die Datenverarbeitung zu kontrollieren und zu unterbinden, könnte auch er gegenüber den Mitfahrern datenschutzrechtlich (mit-) verantwortlich sein. Bezogen auf den jeweiligen Fahrer setzt das aber zumindest die Kenntnis der Verarbeitungsumstände voraus und das der Fahrer die Zwecke und Mittel der Verarbeitung zumindest mitbestimmen, sie insbesondere wirksam unterbinden kann. Es ist aber derzeit nicht erkennbar, inwieweit der Fahrer dann auch über die Möglichkeiten verfügt, die Datenerhebung tatsächlich zu beeinflussen.

---

158 DSK und VDA, Gemeinsame Erklärung.

159 EuGH, Urteil v. 05.06.2018, Wirtschaftsakademie Schleswig–Holstein, C–210/16, EU:C:2018:388.

160 EuGH, Urteil v. 05.06.2018, C–210/16, Facebook, ECLI:EU:C:2018:388, Rn. 28; EuGH, Urt. v. 13.05.2014, Google Spain SL und Google Inc., C-131/12, EU:C:2014:317, Rn. 34.

161 Zur Verantwortung Privater im IoT vgl. Wagner, ZD 2018, 307 ff.

Als Folge einer bestehenden Mitverantwortung des Halters oder Fahrers könnte der jeweilige Dienstanbieter den Fahrer beispielsweise zur Information der Mitfahrer über die Datenverarbeitung verpflichten. Ferner muss der Halter oder Fahrer als (mit-) Verantwortlicher die Einhaltung der Vorgaben der DSGVO sicherstellen. Bei fehlender Transparenz und Zugriffsmöglichkeit wird er aber beispielsweise die Informationspflichten und die Betroffenenrechte nicht erfüllen können. Bei fehlenden Einflussnahmemöglichkeiten auf die Verarbeitung bliebe ihm insoweit bei fehlender Datenschutzkonformität des Fahrzeugs nur die Möglichkeit, die Vorgaben der DSGVO einzuhalten, indem er das Fahrzeug stilllegt.

Die Fahrzeugsysteme müssten daher auch entsprechende Mechanismen vorsehen, um eine datenschutzrechtliche (Mit–) Verantwortung umsetzen zu können. Andernfalls stellt sich die Frage nach der Verantwortung des Herstellers.

2.3.2.1.2.2 Hersteller

Bei dem Hersteller der Fahrzeugsysteme stellt sich die Frage der datenschutzrechtlichen (Mit-) Verantwortung zum Beispiel dann, wenn er neben dem Dienstanbieter Datenrückflüsse aus dem Fahrzeug heraus erhält, oder er in der Lage ist, per Fernzugriff auf die Daten zuzugreifen.[162] Dann stellt sich insbesondere die Frage, ob der Hersteller bereits mit Beginn der Datenverarbeitung lokal im Fahrzeug als Verantwortlicher gelten muss. Bei Missachtung wesentlicher Verarbeitungsgrundsätze, wie fehlenden grundlegenden Mechanismen für Transparenz und Kontrolle des Verarbeitungsvorgangs, liegt dann gegebenenfalls sogar eine alleinige Verantwortung des Herstellers nahe.

Für die Annahme der datenschutzrechtlichen Verantwortung des Herstellers spricht in diesem Fall, dass der Hersteller bereits durch die Auswahl und Implementierung entsprechender Software einen bestimmenden Einfluss auf spätere Verarbeitungsvorgänge nimmt. Naturgemäß wird der jeweilige Hersteller bereits durch die Produktentwicklung so weitreichende Vorfestlegungen treffen und damit den Rahmen, innerhalb dessen die weiteren Akteure auf die Fahrzeugdaten zugreifen können, definieren.[163] Weichert[164] betont insofern zu Recht, dass der Hersteller meist vollständig die technische Gestaltung sowie Auslesemöglichkeiten bestimmt und er dadurch früher oder später zumindest auf indirektem Wege an die Daten gelangt, daher sei er dann auch von Anfang an Verantwortlicher. Es kommt nach der neuesten

[162] DSK und VDA, Gemeinsame Erklärung.

[163] Klink-Straub/ Straub, NJW 2018, 3201 (3202).

[164] Weichert, NZV 2017, 507 (512).

Rechtsprechung des EuGH zudem gerade nicht auf die tatsächliche Verfügungsmacht über die personenbezogenen Daten an.[165]

Wenn der potentiell Verantwortliche, in der Regel der Hersteller, Mechanismen einbaut bzw. einbauen lässt, die eine vollständig automatisierte Datenerfassung und Übersendung zu einem bestimmten Zeitpunkt vorsehen, ohne dass dies transparent gemacht wird und ohne dass eine Möglichkeit des Betroffenen zur Intervention besteht, dürfte daher zumindest in solchen Fällen, in denen heimliche Datenrückflüsse an den Hersteller bereits bei der Übergabe des Fahrzeugs an den Erwerber im technischen System implementiert sind, oder wenn sie über Fernzugriffe nachträglich implementiert werden, bereits mit Beginn der Datenverarbeitung offline im Fahrzeug eine Verantwortlichkeit vorliegen.

Die vorgebrachten Bedenken[166], dies könne im Extremfall dann zu unbilligen Ergebnissen führen, wenn der Eigentümer das Auslesen verweigert oder Komponenten zur Datenübertragung zerstört, verkennen, dass in solchen Fällen auch die eigentlich initiierte Datenverarbeitung unterbleibt, für die es einen Verantwortlichen geben könnte. Wenn die Zerstörung oder Entfernung der datenverarbeitenden Komponente sogar gesetzlich verboten ist, beispielsweise, weil dann die straßenverkehrsrechtliche Zulassung erlischt, ist die betroffene Person bei der offline-Verarbeitung schutzlos gestellt, da sie sich weder an einen Verantwortlichen wenden, noch die Datenverarbeitung im Fahrzeug selbst kontrollieren kann. Bei einer engen Betrachtung der offline-Verarbeitung würden daher Schutzlücken entstehen. Ein Datenverarbeitungsvorgang initiiert sich aber nicht von allein und ist auch nicht für sich selbst verantwortlich. Er wird vielmehr in ein technisches System implementiert, für dessen Produktion eine Gesamtverantwortung besteht. Ein Nichtverhindern bzw. fehlende Kontrollen der Datenschutzkonformität führen dazu, dass dies zumindest konkludent als Billigung durch den Gesamtverantwortlichen zu bewerten ist. Damit hat nach der Definition ein Verantwortlicher zumindest in schlüssiger Weise nach Treu und Glauben die Mittel der Verarbeitung festgelegt.

In Bezug auf unterschiedliche Geschäftsmodelle, die gegebenenfalls auf separaten Telemetrie- und Speichermöglichkeiten aufsetzen, dürfte eine Verantwortung spätestens ab dem Beginn der Datenerhebung anzunehmen sein, wenn die Speichereinheit im Eigentum des Anbieters steht, nach dem Vertragsende mit dem Nutzer des Dienstes an den Anbieter zurückzugegeben ist und während der Vertragslaufzeit vollautomatisiert ohne Eingriffsmöglichkeit der betroffenen Personen

[165] Weichert, NZV 2017, 507 (512).

[166] Klink-Straub/ Straub, NJW 2018, 3201 (3203).

Daten sammelt und speichert. Werden dabei die durch das Fahrzeug bereits aufbereiteten Daten ausgewertet, stellt sich zudem die Frage der gemeinsamen Verantwortung, wodurch die jeweilige Verantwortung jedoch nicht gemindert wird.[167]

2.3.2.2 Auftragsverarbeitung

Der Auftragsverarbeiter handelt nach Art. 4 Nr. 8, Art. 28f DSGVO im Auftrag des Verantwortlichen. Er wird nach Art. 29 DSGVO ausschließlich auf Weisung eines oder mehrerer Verantwortlicher tätig.

Unbeschadet der gewählten Bezeichnung oder Vertragsform gilt er nach Art. 28 Abs. 10 DSVO gegenüber der betroffenen Person dann als Verantwortlicher, wenn er tatsächlich über die Zwecke und Mittel der Verarbeitung (mit-)entscheidet. Das ist der Fall, wenn der Auftragsverarbeiter in der Wahl von Zweck oder Mitteln der Verarbeitung, beispielweise durch Verfolgung eigener Zwecke oder lückenhafte bzw. fehlende Anweisungen, nicht vollständig weisungsgebunden ist. Bei der Einordnung sind die bereits bei der Bestimmmung der Verantwortung dargstellten Grundsätze der neuesten EuGH-Rechtsprechung zu beachten.

Im Kontext vernetzter Fahrzeuge könnten die Vertragswerkstätten, die Daten aus dem Fahrzeug ausschließlich für Zwecke der Hersteller auslesen, bei entsprechender vertraglicher Absicherung Auftragverarbeiter sein. Bei der Verfolgung eigener Zwecke dürfte hingegen eine gemeinsame Verantwortung bestehen. Werden persönliche Daten, beispielweise im Infotainmentsystem abgelegte Telefonnummern, durch die Fahrzeugsysteme ohne Kenntnis- oder Einflussnahmemöglichkeit der betroffenen Person mit einem Backendsystem (z. B. einer Cloud) synchronisiert, könnte darin eine unbefugte Übermittlung personenbezogener Daten liegen, für die neben dem Verantwortlichen auch der für das Backendsystem Verantwortliche (z. B. der Cloud-Anbieter) haftbar wäre.

2.3.3 Pflichten des Verantwortlichen

Der Verantwortliche ist der Adressat der DSGVO. Er hat die Einhaltung der Vorgaben der DSGVO durch Implementierung geeigneter technischer und organisatorischer Maßnahmen sowie insgesamt sicherzustellen und ist dafür rechenschaftspflichtig.

2.3.3.1 Umsetzung technischer und organisatorischer Maßnahmen

Der Verantwortliche ist nach Art. 24 DSGVO verpflichtet, geeignete technische und organisatorische Maßnahmen auszuwählen und umzusetzen, um sicherzustellen, dass die Vorgaben der DSGVO insgesamt beachtet werden. Neben Maßnahmen zur

[167] EuGH, Urt. v. 13.05.2014, Google Spain SL und Google Inc., C-131/12, EU:C:2014:317, Rn. 40.

Gewährleistung der Grundsätze der Verarbeitung nach Art. 5 ff. DSGVO umfasst dies auch solche zur Gewährleistung der Grundsätze der datenschutzfreundlichen Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen nach Art. 25 DSGVO sowie Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO. Die allgemeine Pflicht zur Umsetzung technischer und organisatorischer Maßnahmen wird insoweit spezifiziert und ergänzt durch die Pflichten aus den Artt. 25 und 32 DSGVO.

Darüber hinaus gehören dazu Maßnahmen zur Gewährleistung der transparenten Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Personen nach den Artt. 12 ff. DSGVO. Zudem muss der Verantwortliche die Verhältnisse zu etwaigen Auftragsverarbeitern im Sinne der Artt. 28, 29 DSGVO ausgestalten, eine gemeinsame Verantwortung klar und transparent festlegen und nach Artt. 44 ff. DSGVO Garantien in Bezug auf die internationale Übermittlung von Daten vorhalten. Er muss ein Verzeichnis der Verarbeitungstätigkeiten führen und bei hohem Risiko muss er nach Art. 35 DSGVO eine Datenschutzfolgenabschätzung vor Beginn der Verarbeitungstätigkeit durchführen. Ferner bestehen bei Datenpannen Benachrichtigungs- und Meldepflichten.

Die Maßnahmen müssen nach Art. 24 Abs. 2 DSGVO erforderlichenfalls überprüft und aktualisiert werden. Erforderlich ist demnach eine regelmäßige und systematische Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen.

2.3.3.2 Rechenschaftspflicht

Der Verantwortliche unterliegt der Rechenschaftspflicht nach Artt. 5 Abs. 2, 24 Abs. 1 DSGVO. Er muss die Einhaltung der Vorgaben der DSGVO durch eine ausreichende Dokumentation nachweisen können und trägt in Streitfällen die Darlegungs- und Beweislast.[168]

2.3.3.2.1 Sanktionsmittel und Haftungsnormen

Die neue Rechtslage beinhaltet bei Verletzung der aus der DSGVO resultierenden Pflichten in den Artt. 77 ff. DSGVO verschärfte Sanktionsmittel der Aufsichtsbehörden gegenüber dem oder den Verantwortlichen. Neben Bußgeldverfahren nach den Artt. 83, 84 DSGVO, §§ 41, 43 BDSG n. F. kommen bei schwerwiegenden Verstößen auch strafrechtliche Konsequenzen, z.B. nach § 42 BDSG oder nach dem Strafgesetzbuch (StGB) in Betracht.

[168] Roßnagel, ZD 2018, 339 (341).

Der Verantwortliche haftet drüber hinaus bei materiellen oder immateriellen Schäden den betroffenen Personen aufgrund vermuteten Verschuldens auf Schadenersatz gemäß Art. 82 Abs.2, Abs. 3 DSGVO. Mehrere Verantwortliche haften gemäß Art. 82 Abs. 4 DSGVO als Gesamtschuldner jeweils auf den gesamten Schaden. Auch der Auftragsverarbeiter haftet bei Verstößen nach Maßgabe von Art. 82 Abs. 2 DSGVO.

Daneben können weitere zivilrechtliche Ansprüche nach dem Recht der Mitgliedstaaten bestehen, beispielsweise Abwehr-, Unterlassungs- oder auch Schadenersatzansprüche nach den §§ 823 ff., 1004, 253 ff. BGB. Zu Bedenken ist insoweit, dass neben dem Eigentum auch das allgemeine Persönlichkeitsrecht als sonstiges Recht vom Schutzbereich des § 823 BGB erfasst wird und zur Zahlung von Schmerzensgeld führen kann.[169]

Zudem kommen Gewährleistungsansprüche bei Sachmängeln in Betracht, zum Beispiel wenn die Kaufsache nicht die vereinbarte oder die übliche Beschaffenheit im Sinne des § 434 BGB aufweist. Denkbar wäre ein Sachmangel insbesondere dann, wenn Vorgänge im Kfz eine Datenverarbeitung ermöglichen, die unter Verletzung der Vorschriften der DSGVO zu einer Verletzung des Allgemeinen Persönlichkeitsrechts führt. So hat das OLG Hamm im Jahr 2015 zwar eine solche Negativabweichung (noch) nicht festgestellt. Es hat aber angedeutet, dass *„wenn eine nicht beeinflussbare Weiterleitung personenbezogener Daten von dem Fahrzeug an unbefugte Dritte zu befürchten stünde“* [170], eine negative Abweichung von der üblichen Beschaffenheit i.S.d. § 434 Abs. 1 S. 2 Nr. 2 BGB vorliegen könnte, die einen Sachmangel begründet.

2.3.3.2.2 Mittelbare Haftung der Hersteller

Die Haftung des Verantwortlichen kann auch auf den Hersteller des eingesetzten Softwareprodukts zurückfallen. Der Hersteller eines Softwareprodukts haftet zwar nicht unmittelbar nach der DSGVO, wenn er nicht auch zugleich datenschutzrechtlich verantwortlich ist. Eine Haftung kann sich aber nach den Maßgaben der Produzentenhaftung aus § 823 BGB oder dem Produkthaftungsgesetz ergeben. Ferner kommt eine mittelbare Haftung des Herstellers – etwa bei kaufrechtlichen oder werkvertraglichen Gewährleistungs- und Regressansprüchen entlang der Produktions- oder Lieferkette – in Betracht.

Die Hersteller sind daher nicht nur mittelbar über ihre Auftraggeber an die Grundsätze zur datenschutzfreundlichen Technikgestaltung in Artikel 25 DSGVO gebunden, besonders wenn sie bei Ausschreibungen weiterhin berücksichtigt werden möchten. Im Eigeninteresse sollten sie diese Grundsätze auch beachten, um zivilrechtliche

[169] Vgl. OLG Köln, Urteil vom 30.09.2016, - 20 U 83/16 -, Rn. 69 ff.,Rn. 88.

[170] Vgl. OLG Hamm, Beschluss vom 02.07.2015, - 28 U 46/15-, Rn.46f.

Regressansprüche oder gar Strafverfahren sowie damit verbundene Vertrauensverluste zu vermeiden.

2.4 Grundsätze der Verarbeitung

Die bereits skizzierten Pflichten des Verantwortlichen werden nachfolgend eingehender betrachtet. Zunächst ist der Verantwortliche für die Umsetzung und Einhaltung der essentiellen Grundsätze der Verarbeitung in Art. 5 Abs. 1 DSGVO verantwortlich.

Nach Art. 5 Abs. 1 lit. a Var. 1–3 DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die Person nachvollziehbaren Weise verarbeitet werden. Die zusammenhängende Nennung dieser drei Voraussetzungen verdeutlicht, dass Wechselwirkungen zwischen ihnen bestehen. So kann sich der Verantwortliche auch nicht mithilfe einer Einwilligung jeglichen Bindungen entziehen. Selbst mit Zustimmung der betroffenen Person darf er die auf sie beziehbaren Daten nur nach Treu und Glauben für festgelegte Zwecke verarbeiten.[171]

2.4.1 Rechtmäßigkeit

Rechtmäßigkeit, die erste Variante von Art. 5 Abs. 1 lit. a DSGVO, bedeutet, dass personenbezogene Daten nur auf Basis einer Rechtsgrundlage verarbeitet werden dürfen.[172] Wie bereits unter der alten Rechtslage konstituiert die DSGVO mit dem Rechtmäßigkeitsprinzip die Notwendigkeit einer Einwilligung der betroffenen Person oder einer gesetzlich vorgesehenen Rechtfertigung.[173]

Die möglichen Rechtsgrundlagen sind in Art. 6 Abs. 1, DSGVO abschließend aufgezählt. Bei der Auslegung und Anwendung der Rechtsgrundlagen sind die grundrechtlichen Vorgaben aus Art. 8 Abs. 2 S. 1 GRCh, die wie bereits ausgeführt dem Leitbild der Selbstbestimmung folgen, zu beachten.[174] Selbstbestimmung setzt Entscheidungsfreiheit voraus. Eine freiwillige Entscheidung erfordert, dass strukturelle Informations- und Machtasymmetrien ausgeglichen werden.

Die für die Integration von Diensten in das Ökosystem des vernetzten und automatisierten Fahrens in Betracht kommenden Rechtsgrundlagen werden nachfolgend näher betrachtet.

---

[171] Brink/ Wolff–*Stemmer*, DSGVO, Art. 7, Rn. 26.

[172] Vgl. Artt. 8 Abs 2; 52 Abs. 1 GRCh.

[173] Brink/ Wolff–*Stemmer*, DSGVO, Art. 7, Rn. 24.

[174] Oberlandesgericht Köln, Urteil v. 30.09.2016, –20 U 83/16–, DE:OLGK:2016:0930.20U83.16.00, Rn. 69 (m.w.N.).

2.4.1.1 Einwilligung

Denkbar ist zunächst die Rechtsgrundlage der Einwilligung in einen oder mehrere bestimmte Zwecke. Das umfasst insbesondere auch die besonderen Bedingungen für die Einwilligung gemäß Artt. 5, 6, 7 und 9 DSGVO (vgl. Art. 83 Abs. 5 lit. a DSGVO).

Die Einwilligung ist der zentrale Baustein im Datenschutzrecht und Ausdruck eines selbstbestimmten Menschenbildes, das den Bestimmungen der GRCh, der EMRK und dem GG zugrunde liegt, und stark von der Achtung eines selbstbestimmten Lebensentwurfes geprägt ist. [175] Diesem Wertesystem muss das sekundäre einfachgesetzliche Recht im Spiegel technologischen Fortschritts und Kommerzialisierung folgen. [176] Die Artikel 29-Datenschutzgruppe hat bereits 2014 gefordert, dass Verfahren für die Einholung der Einwilligung auf Informationen ausgerichtet werden müssen, die für den Nutzer verständlich sind und beispielweise nicht auf allgemeine Datenschutzbestimmungen auf der Website des für die Verantwortlichen beschränkt werden dürfen.[177] Die DSGVO setzt das nun in erhöhten Anforderungen um.

Die Einwilligung muss gemäß Artt. 6 Abs. 1 lit. a, 4 Nr. 11 DSGVO informiert und freiwillig für bestimmte Zwecke und durch eine eindeutig bestätigende Handlung abgegeben werden. Sie darf nach dem sog. Kopplungsverbot in Art. 7 Abs. 4 DSGVO nicht von der Erfüllung eines Vertrages abhängig gemacht werden. Die betroffene Person muss eine echte Wahl haben. Die Einwilligung gilt nicht als freiwillig, wenn die betroffene Person bei einer Weigerung oder einem Widerruf Nachteile befürchten muss.[178] So wäre im Kontext vernetzter Fahrzeuge nach den Vorgaben der DSGVO eine Freiwilligkeit zu verneinen, wenn der Fahrzeugstart von der Erteilung der Einwilligung abhängig gemacht wird, oder der Fahrzeugkaufvertrag von der Erteilung einer Einwilligung abhängt.

Die Wirksamkeit der Einwilligung setzt ferner voraus, dass die betroffene Person ausreichende Informationen über die beabsichtigte Verarbeitung (Erhebung, Übermittlung, Speicherung usw.) erhält. Auch muss darüber aufgeklärt werden, dass die Abgabe der Einwilligung freiwillig ist, und welche Folgen eine Verweigerung oder ein Widerruf hat. So muss die betroffene Person vor der Erteilung der Einwilligung mindestens wissen, wer der Verantwortliche ist und welche ihrer Daten für welche bestimmten Zwecke verarbeitet werden sollen.[179] Die betroffene Person muss auch vor

---

[175] Maunz/Dürig–*Herdegen*, GG, Art. 1 Abs. 1, Rn. 28.

[176] Tinnefeld/ Conrad, ZD 2018, S. 392.

[177] Artikel 29-Datenschutzgruppe, WP 259 rev. 01, S. 4.

[178] ErwG 42 S. 5 DSGVO.

[179] ErwG 42 S. 4 DSGVO.

der Einwilligung nach Art. 7 Abs. 3 S. 3 DSGVO über ihr Recht, die Einwilligung jederzeit für die Zukunft zu widerrufen, informiert werden.

Je nach Fallgestaltung setzt eine informierte Entscheidung zusätzliche Informationen voraus. So sind die Anforderungen bei Profiling aufgrund der Komplexität der Verarbeitung hoch gesetzt, um echtes Verständnis zu ermöglichen. Die eine freie Entscheidung hindernde Informationsasymmetrie muss durch weitere Informationen ausgeglichen werden.[180] Folgende Informationen sind je nach Fall für eine ausreichende Information erforderlich: [181] Das Recht aus Art. 22 Ab. 2 lit. c DSGVO, bei einer ausschließlich automatischen Entscheidung mit erheblicher Auswirkung. [182] Bei Übermittlungen in Drittstaaten die Information gemäß Art. 49 Abs. 1 lit. a DSGVO. Soweit besondere Kategorien personenbezogener Daten verarbeitet werden sollen, sind die Vorgaben der von Art. 9 Abs. 1, Abs. 2 lit. a, ErwG 51 DSGVO zusätzlich zu beachten.

Die Einwilligung kann auch elektronisch, etwa durch Anklicken eines Kästchens oder die Auswahl technischer Einstellungen erfolgen. [183] Allerdings stellen Stillschweigen, vorangekreuzte Kästchen oder Untätigkeit keine Einwilligung dar. [184] Es besteht insbesondere Forschungsbedarf hinsichtlich der technischen Machbarkeit der Einholung von Einwilligungen am Maßstab von Art. 7, ErwG 42 DSGVO. Ungeachtet dieser Frage erscheint die Einholung von Einwilligungen aufgrund der unbekannten Vielzahl möglicher betroffener Personen (weitere Fahrzeugnutzer, Verkehrsteilnehmer, …) im Kontext von C-ITS nicht praktikabel. Die Erbringung von Diensten kann nur dann auf eine Einwilligung gestützt werden, wenn sichergestellt ist, dass die Verarbeitung sich nur auf Daten des Einwilligungsgebers bezieht und nur die Daten des Einwilligungsgebers verarbeitet werden.

Besondere Grenzen sind bei der Einholung von Einwilligungen von Arbeitnehmern gegenüber dem Arbeitgeber oder bei Kindern zu beachten. [185]

Besonders schwierig gestaltet sich die Abgrenzung zur Rechtsgrundlage der Erforderlichkeit zur Vertragserfüllung in Art. 6 Abs. 1 lit b DSGVO, wenn in Nutzer-AGBs zugleich datenschutzrechtliche Einwilligungen eingeholt werden sollen. Aus dem Kopplungsverbot folgt dann regelmäßig die Unwirksamkeit der Einwilligung.

---

[180] Notwendige Informationen werden in ErwG 42 S. 4 und ErwG71 DSGVO benannt.

[181] Artikel 29-Datenschutzgruppe, WP 259 rev. 01, S.13.

[182] ErwG 71 DSGVO.

[183] ErwG 32 S. 1, S.2 DSGVO.

[184] ErwG 32 S. 3 DSGVO.

[185] Artikel-29-Datenschutzgruppe, WP 252, S. 12.

Dient die Verarbeitung mehreren Zwecken, muss für jeden dieser Zwecke eine Einwilligung erteilt werden, da sie verschiedene Verarbeitungen darstellen und jeder Verarbeitungsvorgang einer separaten Einwilligung bedarf.[186] Sollen etwa neben dem Hauptzweck weitere Zwecke, wie Zusatzdienste, Produktbeobachtung oder Maschinelles Lernen zur Fortentwicklung der Algorithmen verfolgt werden, muss sich die Einwilligung auch auf die weiteren bestimmten Zwecke ausdrücklich beziehen. Eine Sammlung auf Vorrat zu unbestimmten oder noch bestimmbaren Zwecken ist hingegen unzulässig.[187]

Die Einwilligung ist jederzeit für die Zukunft frei widerrufbar, worauf bei den Rechten der betroffenen Personen näher eingegangen wird. Nach Art. 7 Abs. 3 S. 4 DSGVO muss der Widerruf der Einwilligung so einfach sein wie die Erteilung der Einwilligung. Wird z.B. die Einwilligung über das Infotainmentsystem des Fahrzeugs oder das Smartphone eingeholt, muss der Widerruf auf die gleiche Weise erklärt werden können.

2.4.1.2 Erforderlich zur Vertragserfüllung

Nach Art. 6 Abs. 1 lit. b Var. 1 DSGVO ist die Verarbeitung gerechtfertigt, soweit sie für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich ist.

Da regelmäßig eine gemeinsame Verantwortung im Ökosystem des vernetzten Verkehrs naheliegt, ist zunächst eine Beurteilung der unterschiedlichen Funktionen im Hinblick auf die jeweils verfolgten Zwecke und Mittel erforderlich, bevor eine vertragliche Rechtsgrundlage geschaffen werden kann.[188]

Die Norm setzt voraus, dass ein wirksamer Vertrag mit der betroffenen Person und die Erforderlichkeit zu dessen Erfüllung vorliegen.

2.4.1.2.1 Vertragsverhältnis mit der betroffenen Person

Nach dem klaren Wortlaut gilt diese Rechtsgrundlage nur dann, wenn die von der Verarbeitung betroffene Person mit dem unmittelbaren Vertragspartner personenidentisch ist. Gegenüber Drittbetroffenen begründet die Vorschrift hingegen keine Rechtsgrundlage. Verträge zu Lasten Dritter sind unzulässig, und können gegenüber anderen Fahrzeugnutzern, Verkehrsteilnehmern und sonstigen betroffenen Personen keine Rechtswirkungen begründen. Damit kann diese Rechtsgrundlage eine Datenverarbeitung gegenüber anderen Fahrzeugnutzern als dem Vertragspartner sowie Personen außerhalb des Fahrzeugs nicht legitimieren.

---

[186] ErwG 42 S. 4 , ErwG 43 DSGVO.

[187] BVerfG, Urteil vom 14.07.1999, -1 BvR 2226/94, Rn. 179.

[188] Artikel-29-Datenschutzgruppe, WP 252, S. 6, 13.

2.4.1.2.2 Wirksame Vertragsgrundlage

Die vertragliche Grundlage muss darüber hinaus wirksam sein. Fraglich ist insoweit, ob die Voraussetzung der wirksamen Vertragsgrundlage sich nach einer unionsrechtlichen Definition oder nach den vertragsrechtlichen Vorgaben der Mitgliedstaaten, hier des Bürgerlichen Gesetzbuchs (BGB) richtet.

Für eine unionsrechtliche Auslegung spricht zunächst, dass sich auf EU-Ebene zunehmend ein autonomes Vertragsverständnis etabliert.[189] Bei der Konturierung des unionsrechtlichen Vertragsbegriffs ist jedoch zu beachten, dass das Unionsrecht eng mit dem mitgliedstaatlichen Recht verzahnt ist. Das Unionsrecht regelt nur bestimmte schuldrechtliche Aspekte (z.B. im Verbraucher-, Finanzdienstleistungs- und Wirtschaftsvertragsrecht), die grundlegenden Fragen, wie das Zustandekommen des Vertrages, unterliegen hingegen dem mitgliedstaatlichen Privatrecht.[190]

Die Frage eines wirksamen Vertragsschlusses richtet sich daher auch weiterhin (noch) nach dem nationalen Recht der Mitgliedstaaten, wobei der europarechtliche Rahmen in Form von Richtlinien und Verordnungen als höherrangiges Recht bei der Vertragsauslegung zu berücksichtigen ist.

Art. 6 Abs. 1 lit. b DSGVO erfasst die Erfüllung der vertraglichen Leistungs- und Nebenpflichten und die diesbezüglichen gesetzlichen Verpflichtungen. [191] Der Vertragsinhalt ist anhand der Auslegungsregeln der §§ 133, 145ff, 157 BGB am Maßstab von Treu und Glauben zu ermitteln. Verträge werden von den Gerichten anhand der Vertragszwecke und unter Beachtung der rechtlichen Gestaltungsgrenzen ausgelegt, um die Haupt- und Nebenleistungspflichten zu ermitteln. Der Vertragsinhalt kommt nur in diesem ermittelten Umfang zustande. Er ist darüber hinaus nur wirksam, wenn er die Grenzen der Vertragsautonomie, insbesondere der §§ 134, 138, 307 ff BGB beachtet. Nach dem Bundesverfassungsgericht ist das Datenschutzrecht als Konkretisierung des allgemeinen Persönlichkeitsrechts auch bei der Anwendung und Auslegung dieser zivilrechtlichen Normen zu beachten: *„Das allgemeine Persönlichkeitsrecht […] entfaltet als objektive Norm seinen Rechtsgehalt auch im Privatrecht und strahlt so auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus. Verkennt ein Gericht, das eine privatrechtliche Streitigkeit entscheidet, in grundsätzlicher Weise den Schutzgehalt*

[189] Lüttringhaus, 2018, S. 64 ff (m.w.N.).

[190] Vgl. nur die Erwägungsgründe 14, 42 und Art. 3 Abs. 5 der Verbraucherrechtrichtlinie.

[191] BGH, Urteil v. 12.07.2018, -III ZR 183/17-, DE:BGH:2018:120718UIIIZR183.17.0, Rn. 71.

des allgemeinen Persönlichkeitsrechts, verletzt es durch sein Urteil das Grundrecht des Bürgers in seiner Funktion als Schutznorm."[192]

Lassen sich Dienste vertraglich weitere Verarbeitungsrechte als für die Zweckerreichung notwendig einräumen, dürfte dies regelmäßig bereits wegen Verstoßes gegen die zivilrechtlichen Auslegungsgrenzen, insbesondere verbraucherschützende Vorschriften, oder auch im Falle einer zugleich eingeholten Einwilligung gegen das Kopplungsverbot, zur Unwirksamkeit der vertraglichen Bestimmung führen. Diese Grenzen sollten Veranlassung sein, sich bei der Ausgestaltung der Verträge und insbesondere der Formulierung der vertraglichen Pflichten auf das zur Erfüllung der Hauptleistungspflichten erforderliche Maß an Datenverarbeitung zu begrenzen.

2.4.1.2.3 Erforderlichkeit

Ist die Datenverarbeitung nicht ausdrücklich im Vertrag vereinbart, kommt es auf die Erforderlichkeit der Datenverarbeitung an. Die Erforderlichkeit verlangt, dass die erhobenen Daten für die Vertragsdurchführung unbedingt notwendig sind. Hierfür ist eine bloße Zweckdienlichkeit nicht ausreichend. Was unbedingt notwendig ist, hängt vom Vertragsinhalt und der vertragscharakteristischen Leistung des jeweiligen Schuldverhältnisses ab.[193]

So benötigen Dienste, die Verkehrsinformationen empfangen, aufbereiten und anderen Verkehrsteilnehmern zur Verfügung stellen, keine identifizierenden Daten des Absenders der Verkehrsinformation. Um den Verkehrsfluss einzuschätzen, dürften aggregierte Daten einer Gruppe von Verkehrsteilnehmern in einem bestimmten Straßenabschnitt zu einem bestimmten Zeitpunkt bereits ausreichen.

2.4.1.3 Erforderlich zur Erfüllung einer rechtlichen Verpflichtung; Aufgabenerfüllung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

Durch die veränderte Handlungsform der Verordnung ändert sich auch die Bedeutung des nationalen Rechts und besonders der Fachgesetze: Maßgeblich für die Verarbeitung personenbezogener Daten ist nun stets die DSGVO[194], nur soweit diese den Mitgliedstaaten Handlungsspielräume eröffnet, darf auf einer zweiten Stufe geprüft werden, ob das nationale Gesetz die Vorgaben der DSGVO in zulässiger Weise umsetzt.[195]

---

[192] Oberlandesgericht Köln, Urteil v. 30.09.2016, –20 U 83/16–, DE:OLGK:2016:0930.20U83.16.00, Rn. 49; BVerfG, Beschluss v. 17.07.2013 – 1 BvR 3167/08, NJW 2013, 3086 m.w.N.

[193] BGH, Urteil v. 12.07.2018, -III ZR 183/17-, DE:BGH:2018:120718UIIIZR183.17.0, Rn. 71.

[194] Im Rahmen ihres Anwendungsbereichs, also z.B. nicht im Bereich der Polizei-Richtlinie (vgl. Art. 2 DSGVO).

[195] Vgl. Roßnagel, DuD 2018, 477 (480 f.).

Soweit die DSGVO sog. obligatorische (verpflichtende) Öffnungsklauseln enthält, muss der nationale Gesetzgeber tätig werden und diese Vorgaben umsetzen. Daneben existieren sog. fakultative Öffnungsklauseln, in deren Rahmen keine Umsetzungspflicht besteht, den nationalen Parlamenten aber ein gewisser Gestaltungsspielraum eingeräumt wird. Werden die Öffnungsklauseln überschritten gilt aufgrund des Anwendungsvorrangs des Unionsrechts die DSGVO vor[196].

Art.6 Abs. 1 lit.c, lit. e i.V.m. Abs. 2, Abs. 3 DSGVO eröffnen eine fakultative Regelungsmöglichkeit für die Union und die Mitgliedstaaten, bereichsspezifische Ausnahmen zur Erfüllung einer rechtlichen Verpflichtung, im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt zu schaffen (Art. 6 Abs. 1 lit. c, e DSGVO). Bei der Regelung muss es sich aufgrund von Art. 8 Abs. 2 GRCh und Artt. 2 Abs. 1., 1 Abs. 1 GG um ein formelles Parlamentsgesetz handeln.[197] Erforderlich ist, dass die nationale Rechtsgrundlage zur Datenverarbeitung im öffentlichen Interesse liegt. Gegebenenfalls müssen die bereichsspezifischen Vorgaben nach den Artt. 85 ff DSGVO zusätzlich erfüllt sein. Darunter fällt in Deutschland beispielsweise die Regelung des Straßenverkehrs oder die Lenkungsverwaltung.[198]

Die Norm erlaubt damit, präzise und spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO beizubehalten oder einzuführen. Diese allgemeinen Öffnungsklauseln sind von zentraler Bedeutung, um die breite Palette der Datenverarbeitung im öffentlichen Interesse im bereichsspezifischen Datenschutzrecht in Deutschland aufrechterhalten zu können.[199]

Allerdings können die Vorgaben der DSGVO nur präzisiert und nicht unterschritten werden.[200] Inwieweit die nationalen Regelungen Bestand haben können, weil sie den weiteren Anforderungen der DS-GVO genügen, wird sich erst nach und nach erweisen.[201] Zahlreiche datenschutzrechtliche Vorgaben in den Fachgesetzen (z.B. in der Strafprozessordnung oder den Sozialgesetzbüchern) werden aktuell überarbeitet und an die neuen europarechtlichen Vorgaben angepasst.

Datenschutz im Bereich vernetzter, automatisierter und kooperativer Fahrzeuge berührt eine Vielzahl unterschiedlicher Rechtsmaterien, namentlich das IVSG oder das BDSG n.F. Durch die Integration von Diensten im Bereich der mobilen Kommunikation,

---

196 Kühling/Sackmann, NVwZ 2018, 681 (682).

197 ErwG 41 2.Hs DSGVO.

198 Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 32.

199 Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 28.

200 ErwG 45 S. 5 DSGVO.

201 Paal/Pauly-*Frenzel*, DSGVO, Art. 6, Rn. 40.

elektronischen Bezahldienste oder Elektro-Mobilität treten weitere spezialgesetzliche Fragen hinzu. Daher ist zu prüfen, wann welches Gesetz für welchen Teilbereich nach den Maßgaben der DSGVO zur Anwendung kommt.

2.4.1.3.1 Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern

Das Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG) enthält keine bereichsspezifischen Vorschriften zum Datenschutz, sondern verweist in § 3 S. 2 IVSG allgemein auf bundesrechtliche Regelungen. Solche Regelungen existieren (noch) nicht.

2.4.1.3.2 Straßenverkehrsgesetz

Künftig dürfen Kraftfahrzeuge mit hoch- oder vollautomatisierten Fahrfunktionen[202] nach § 1a Straßenverkehrsgesetz (StVG) unter bestimmten Voraussetzungen betrieben werden. Neben der Zulassung zum Straßenverkehr bedarf es dazu auch einer Typengenehmigung der hoch- oder vollautomatisierten Fahrfunktionen. Ferner dürfen die Fahrfunktionen nur bestimmungsgemäß verwendet werden.

In § 1a Abs. 2 StVG sind konkrete Anforderungen an die Fahrzeugsysteme formuliert. Datenschutzrechtliche Vorgaben gehören jedoch nicht dazu. Das ist dann problematisch, wenn der Gesetzgeber nach dem Wesentlichkeitsvorbehalt verpflichtet ist, die Belange im beabsichtigten Gesetz selbst festzulegen. Das ist bei wesentlichen grundrechtserheblichen Belangen der Fall, wenn bei datenintensiven Verarbeitungssystemen mit der technischen Systemeinführung auch eine gesetzliche Speicherpflicht einhergeht. Solche Speicherpflichten werden in § 63a StVG festgelegt.

Der neu eingeführte § 63 a StVG legt Speicherpflichten sowohl im öffentlichen als auch im privaten Beweisführungsinteresse fest. Die Norm dient der Einführung der Fahrzeugautomatik. [203] Besonders umstritten sind in diesem Zusammenhang der Adressat der Speicherpflicht, die normierten Übermittlungsbefugnisse und die ungenügende Eingrenzung der Zweckbestimmung.[204]

Um Beweisproblemen zu begegnen, schreibt § 63a StVG künftig vor, dass die Fahrzeuge die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben speichern müssen, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt, der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische

---

[202] Zum Begriffsverständnis: WD BT, autonomes und automatisiertes Fahren.

[203] Zu den weiterhin bestehenden Pflichten das Fahrzeugführers vgl. König, NVZ 2017, 123 (124 ff.).

[204] Schmid/ Wessels, NVZ 2017, 357.

Störung des Systems auftritt. Nach § 63a Abs. 4 StVG müssen die Daten sechs Monate, bei Unfällen im Sinne des § 7 Abs. 1 StVG drei Jahre gespeichert werden. Eine vorherige Löschung ist nach der Gesetzesbegründung nicht zulässig.[205]

2.4.1.3.2.1 Datenzugang und Adressat der Speicherpflicht

Vorgaben zum Adressaten der Speicherpflicht, zur technischen Ausgestaltung, zu Ort, Art und Weise der Speicherung sowie der Datensicherung bei Verkauf des Fahrzeugs sollen gemäß § 63b StVG im Wege von Rechtsverordnungen erlassen werden. Mit der Norm geht eine Erweiterung der Verordnungsermächtigungen, darunter sind insbesondere die Fahrerlaubnisverordnung (FeV), die Straßenverkehrs-Zulassungsverordnung (StVZO), die Fahrzeugzulassungsverordnung (FZV) und die Straßenverkehrsordnung (StVO) zu nennen, einher.[206] Die Gesetzesbegründung verweist zudem auf internationale Verhandlungen.[207] Entsprechende Änderungen werden derzeit auf der Ebene der Wirtschaftskommissionen der Vereinten Nationen für Europa (UN-ECE) abgestimmt.[208]

Nach der Gesetzesbegründung sollen die Daten gesondert aufgezeichnet und nur bei Erforderlichkeit zugänglich gemacht werden.[209] Das erfordert, dass der Speicher funktional abgegrenzt sein muss und dass beim Auslesen und Übertragen des Unfalldatenspeichers nicht auf den gesamten Datenbestand im Fahrzeug zugegriffen werden kann. Die verschiedenen Funktionsbereiche müssen konsequent getrennt werden.

Die wesentliche Frage nach dem Speicherort der Daten lässt § 63a StVG unbeantwortet. Gleichwohl geht der Gesetzgeber jedenfalls auch von einer lokalen Speicherung im Fahrzeug selbst aus. Nach der Gesetzesbegründung soll das zentrale Fahrzeugregister nämlich um das eindeutige Identifikationsdatum des Speichermediums (Speicher-ID) jedes Kraftfahrzeugs mit hoch- oder vollautomatisierter Fahrfunktion ergänzt werden.[210] Ferner sollen Polizei und Zulassungsbehörden mit Datenauslesegeräten ausgestattet und entsprechend geschult werden.[211]

Die zum Teil geforderte (zusätzliche) Speicherung bei einem Dritten bedarf als eigenständiger Grundrechtseingriff auch einer eigenen Rechtsgrundlage, die hohen

---

[205] BT-Drs. 18/11776,.12.

[206] König, NVZ 2017, 123 (126).

[207] BT-Drs. 18/11776, 12.

[208] BT-Drs. 18/113006, 15.

[209] BT- Drs. 18/11300, 25.

[210] BT-Drs. 18/11300, 2, 28f.

[211] BT-Drs. 18/11300, 2, 28f.

Anforderungen an die Verhältnismäßigkeit genügen muss. Zum Teil wird vertreten, ein Treuhandmodell setze implizit voraus, dass die Automobilindustrie Inhaber der Datenrechte sei.[212]

Die verpflichtende Einbindung eines Datentreuhänders birgt darüber hinaus aufgrund der mit dieser Position verbundenen Vertrauensstellung bei Interessenskonflikten erhebliche Missbrauchspotentiale. Interessenkonflikte liegen insbesondere dann auf der Hand, wenn der jeweilige Hersteller diese treuhänderische Position ausfüllen soll. Die Interessenkonflikte liegen auf der Hand: Er könnte sich bei Fehlfunktionen berechtigten Produkthaftungsansprüchen oder sogar zulassungs- oder strafrechtlichen Konsequenzen zu entziehen versuchen oder sich beispielsweise bei aufbereiteten Datensätzen auf den Schutz von Gebrauchsmustern oder Geschäftsgeheimnissen berufen. Hinzu kommt das Risiko technischer Schwachstellen bei der Datenverwaltung. Das Bundesverfassungsgericht hat zu gesetzlichen Speicherpflichten Privater ausgeführt: *„Auch die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, verschärfen deren belastende Wirkung. […] Verstärkt wird dies dadurch, dass die Anforderungen an die Datenverwaltung ein hohes Maß an Technikbeherrschung voraussetzen, womit sich zwangsläufig die Gefahr von Schwachstellen und das Risiko von Manipulationen durch interessierte Dritte verbinden.“* [213] Dem gesteigerten Missbrauchsrisiko steht ein hoher Schutzbedarf der Fahrzeugdaten gegenüber. Sie enthalten in der Regel Zeit- und Standortangaben und wecken daher vielfältige Begehrlichkeiten, da sie die Ableitung von Bewegungs- und Verhaltensprofilen ermöglichen. Darüber hinaus ist absehbar, dass die Frage nach dem Datenzugang in naher Zukunft einen großen Personenkreis betreffen wird. Der Grundsatz der Datenminimierung, der nach der höchstrichterlichen Rechtsprechung den Verhältnismäßigkeitsgrundsatz konkretisiert, dürfte daher einer zusätzlichen Speicherung bei einem Dritten entgegenstehen.

Die Frage des Datenzugangs bestimmt wirkst sich zudem wesentlich auf die Art und Weise der Datenverarbeitung aus und hat damit erhebliche Auswirkungen auf das Grundrecht auf Schutz der personenbezogenen Daten. Daher dürfte eine Festlegung durch den Gesetzgeber selbst erforderlich sein.

Bei der Übermittlung muss, wie bereits dargelegt, zur Wahrung der Verhältnismäßigkeit für jedes Datum dargelegt werden, warum das konkrete Datum im Verfahren benötigt wird. § 63a Abs. 2 S. 2 StVG bekräftigt den Grundsatz der Erforderlichkeit. In der Gesetzesbegründung wird explizit darauf hingewiesen, dass es insbesondere unstatthaft

[212] Hoeren, NVZ 2018, 153 (153).

[213] BVerfG, Urteil v. 02.03.2010, - 1 BvR 256/08, Rn.212 (m.w.N.).

ist, zur Klärung der Verantwortlichkeit alle gespeicherten Daten oder bei einer allgemeinen verdachtsfreien Verkehrskontrolle überhaupt die aufgezeichneten Daten zu übermitteln.[214]

2.4.1.3.2.2 Zweckbindung und Verwendungsregelungen

Welchem Zweck die in § 63a Abs. 1 StVG geregelte Pflicht zur Speicherung der Daten dient, ist im Gesetz selbst nicht geregelt. Aus der Gesetzesbegründung ergibt sich aber, dass die Speicherpflicht sicherstellen soll dass der Fahrzeugführer sich nicht pauschal auf ein Versagen des automatisierten Systems berufen kann.[215] Der Wortlaut des § 63a Abs. 2 StVG sowie die Gesetzesbegründung legen daher nahe, dass der Zweck der Speicherpflicht der Nachweis der Verantwortlichkeit für die Bedienvorgänge bei Regelverstößen im Zusammenhang mit dem Straßenverkehr sein soll.

Allerdings fehlt im Gesetzeswortlaut eine Begrenzung auf diesen Zweck. Zudem verweist § 63a Abs. 2 S. 3 StVG auf die allgemeinen Regelungen zur Verarbeitung personenbezogener Daten, die von § 63a StVG unberührt bleiben. Danach ist die Möglichkeit zu zweckändernden Verarbeitungen i.S.d. BDSG n. F. eröffnet, obwohl der hohe Schutzbedarf aufgrund der sensiblen Datenmengen, die in großem Umfang Standortdaten, die feste Speicher-ID und Zeitstempel enthalten können, eine strenge Zweckbindung erfordern dürften.

Die unklare Bestimmung und Begrenzung der Zwecke der Datenerhebung und -verwendung führt bereits zu entsprechenden Diskussionen[216] und wird, wie schon die Erfahrungen im Zusammenhang mit der Lkw-Maut gezeigt haben, auch die Staatsanwaltschaften und Gerichte beschäftigen: Obwohl das Autobahnmautgesetz von Beginn an eine ausdrückliche Zweckbestimmung und -begrenzung enthielt, wurde von einem Gericht die Beschlagnahme der Daten für einen anderen als den im Autobahnmautgesetz genannten Zweck als zulässig angesehen. Daraufhin verankerte der Gesetzgeber klarstellende Regelungen zur ausnahmslosen Zweckbindung im Autobahnmautgesetz (jetzt § 4 Abs. 3 S. 4 und 5 Bundesfernstraßenmautgesetz).[217]

Vor dem Hintergrund dieser unklaren Zweckbegrenzung ist die Bestimmtheit und Verhältnismäßigkeit der Speicherpflicht nach § 63a StVG äußerst fraglich. Datenverarbeitungen zu anderen Zwecken, die in Anbetracht der mit den Speicherungen verbundenen Eingriffstiefe unverhältnismäßig wären, sind durch das Gesetz nicht hinreichend ausgeschlossen.

---

[214] BT-Drs. 18/11300, 25.

[215] BT-Drs. 18/11300, 15.

[216] Berndt, NZV 2018, 249 ff.; DAV, Stellungnahme 24/2017, S. 10.

[217] Vgl. LG Magdeburg, Beschluss v. 3.2.2006 – 25 Qs 7/06 –; WD BT, Mautdaten, S. 5.

Der Verhältnismäßigkeitsgrundsatz stellt bei gesetzlichen Speicherpflichten aber erhöhte Anforderungen auf und verlangt nach normenklaren sowie bereichsspezifischen Verwendungsregeln. Das Bundesverfassungsgericht hat im Rahmen der Pflicht zur Vorratsdatenspeicherung bereits ausgeführt: *„Eine Speicherung kann nicht als solche abstrakt gerechtfertigt werden, sondern nur insoweit sie hinreichend gewichtigen, konkret benannten Zwecken dient. Demgegenüber ist es unzulässig, unabhängig von solchen Zweckbestimmungen einen Datenpool auf Vorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt. In einem solchen Fall könnte die Verfassungsmäßigkeit der Speicherung mangels hinreichend vorhersehbarer und begrenzter Zwecke zum Zeitpunkt des in der Speicherung liegenden Eingriffs noch nicht beurteilt werden. Auch wäre ihre Tragweite für den Bürger weder vorhersehbar noch nach Maßgabe des Verhältnismäßigkeitsgrundsatzes begrenzt.“*[218]

Auch die weitere Verwendung der Daten bei den in § 63a Abs 2 S. 1 StVG genannten Empfängern ist im Gesetz in keiner Weise eingeschränkt. Stattdessen eröffnet der Verweis auf die allgemeinen Regeln die Möglichkeit zweckändernder Verwendungen außerhalb des konkreten Verfahrens, für das die Daten erhoben wurden. Die Verwendung unterliegt somit nur den allgemeinen Schranken für eine zweckändernde Verarbeitung. Ob § 63a StVG dem besonderen Schutzbedarf der nach § 63a Abs. 1 StVG gespeicherten Daten genügt, ist auch in dieser Hinsicht äußerst zweifelhaft.

2.4.1.3.3 Ausblick auf die ePrivacy-Verordnung

Geplant war, dass zeitgleich mit der DSGVO auch eine Spezialregelung für den Bereich des Schutzes der Privatsphäre in der elektronischen Kommunikation in Kraft treten sollte, der die DSGVO insoweit um bereichsspezifische Regelungen präzisiert und ergänzt. Motive für eine Übererarbeitung der bislang für den Bereich der elektronischen Kommunikation geltenden ePrivacy-Richtlinie sind die unterschiedlichen Umsetzungen und unterschiedliche Interpretationen der Richtlinie in den Mitgliedstaaten, die durch die Wahl einer Verordnung als in den Mitgliedstaaten unmittelbar geltendes Recht harmonisiert werden sollen.

Die Entwürfe zur ePrivacy-VO müssen zwischen dem Europäischen Parlament, der EU-Kommission und dem europäischen Rat abgestimmt werden. Nachdem am 10.01.2017 die Gesetzesinitiative durch die Europäische Kommission gestartet wurde,[219] erfolgten

[218] BVerfG, Urteil v. 02.03.2010, –1 BvR 256/08–, Rn. 266 (m.w.N).

[219] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische

bis Mitte 2017 zunächst verschiedene Stellungnahmen, insbesondere von der Artikel 29–Datenschutzgruppe [220] und vom Europäischen Datenschutzbeauftragten (EDPS)[221]. Am 26.10.2017 wurde der Entwurf einer legislativen Entschließung des Europäischen Parlaments verabschiedet. [222]

Nach erneuten Stellungnahmen, insbesondere im Mai 2018 vom Europäischen Datenschutzausschuss (EDSA) [223] , dem Nachfolgegremium der Artikel 29–Datenschutzgruppe, ist der Standpunkt des europäischen Rates weiterhin offen. Derzeit werden weitreichende Änderungsvorschläge im Rat diskutiert,[224] ohne dass sich die EU-Mitgliedstaaten bislang auf eine gemeinsame Position einigen konnten.[225]

Der Schutz bei elektronischer Kommunikation soll nach den vorliegenden Entwürfen der Europäischen Kommission und des Europäischen Parlaments nicht nur für die klassische Telekommunikation gelten, sondern auch auf sog. „over the top" (OTT)-Dienste ausgeweitet werden, die Bedeutung der Einwilligung stärker hervorheben, neben Inhaltsdaten auch die Metadaten stärker schützen, Pflichten für Softwarehersteller nach den Grundsätzen Data Protection by Design und by Default normieren, sowie Regelungen zur M2M–Kommunikation enthalten.[226] Ferner soll die ePrivacy-Verordnung detaillierte Regelungen zum Webtracking und anderen Profilbildungsmöglichkeiten bei der elektronischen Kommunikation vorhalten.[227] Die bislang bezogenen Standpunkte weisen jedoch erhebliche Unterschiede auf, so dass eine Einigung derzeit nicht absehbar ist. Besonders umstrittene Punkte sind die Weiterverarbeitung durch den Endnutzer/ in dessen Auftrag nach Art. 5 VO-E, die Verarbeitung pseudonymisierter Standortdaten ohne Einwilligung nach Art. 6 VO-E, der Katalog zulässiger Verarbeitungen, für die keine

---

Kommunikation), COM/2017/010 final - 2017/03 (COD), abrufbar: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0010 (letzter Abruf: 04.12.2018).

220 Artikel 29-Datenschutzgruppe, WP 247.

221 EDSB, Stellungnahme ePrivacy–VO.

222 Vgl. European Parliament, Legislative Observatory, 2017/0003(COD), Respect for private life and the protection of personal data in electronic communications, abrufbar: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0003(OLP) (letzter Abruf: 04.12.2018).

223 EDSA, Erklärung zur ePrivacy-VO.

224 Die einzelnen Ratsdokumente sind abrufbar unter: https://eur-lex.europa.eu/procedure/DE/2017_3 (letzter Abruf: 04.12.2018).

225 Zusammenfassend: Rat der Europäischen Union, Interinstitutionelles Dossier: 2017/0003(COD), 23.11.2018, abrufbar: http://data.consilium.europa.eu/doc/document/ST-14491-2018-INIT/de/pdf (letzter Abruf: 04.12.2018).

226 Ausführlich: BayLDA, Synopse ePrivacy-VO.

227 Paal/Pauly-*Martini*, DSGVO, Art. 22, Rn. 22.

Einwilligung erforderlich ist nach Art. 8 VO-E, die Pflichten von Software-Anbietern, insbesondere Data Protection by Design und by Default durch Voreinstellungen, Nutzerinformation bei der Erstinstallation sowie die Möglichkeiten zur Einholung einer Einwilligung nach Art. 10 VO-E.

Sowohl der europäische Datenschutzausschuss als auch der Europäische Datenschutzbeauftragte betonen insoweit den gestiegenen grundrechtlichen Schutzbedarf und dass der Schutz der geplanten ePrivacy-Verordnung nicht hinter dem Schutz der ePrivacy-Richtlinie zurückbleiben darf.[228]

Durch die Verzögerung im Gesetzgebungsverfahren stellt sich die Frage, welches Recht in der Zwischenzeit Geltung beansprucht. Art. 95 DSGVO bestimmt insoweit, dass nur solche nationalen Umsetzungsakte, die auf der ePrivacy-RL 2002/58/EU (ergänzt durch die sog. „Cookie-RL“ 2009/136/EU) beruhen, anwendbar bleiben, die das gleiche Ziel verfolgen wie die DSGVO. Damit existieren zwei Anforderungen: Das nationale Gesetz muss auf der ePrivacy-Richtlinie beruhen und es muss dasselbe Ziel verfolgen wie die DSGVO.

Insoweit ist im Folgenden zu untersuchen, inwieweit das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) die ePrivacy-Richtlinie umsetzen und dabei dasselbe Ziel verfolgen wie die DSGVO.

2.4.1.3.4 Telekommunikationsgesetz

Soweit Telekommunikationsdienstleistungen erbracht werden, ist die Anwendung des Telekommunikationsgesetzes (TKG) zu prüfen.

Hinsichtlich der datenschutzrechtlichen Bestimmungen im TKG bestehen keine Bedenken, dass diese Angaben auch unter der DSGVO wirksam bleiben. Die Regelungen des TKG beruhen auf den Regelungen der ePrivacy–Richtlinie und es ist nicht erkennbar, dass der Schutzmaßstab der DSGVO unterschritten werden könnte, da das TKG die Vorgaben der ePrivacy-Richtlinie umsetzt. Die DSGVO dürfte nach der Sonderregel in Art. 95 DSGVO daher keine erhöhten Anforderungen aufstellen, der Schutzmaßstab der DSGVO darf aber auch nicht abgesenkt werden.

Im Bereich der Telekommunikation besteht ein gegenüber der DSGVO erhöhter Schutzbedarf, da bei der Erhebung personenbezogener Daten über Telekommunikationsnetze das Telekommunikationsgeheimnis aus Art. 10 GG bzw. Art. 7 GRCh berührt wird, vgl. § 88 Abs. 2 TKG. Aus dem Fernmeldegeheimnis folgt ein grundsätzliches Kenntnisnahmeverbot sämtlicher Telekommunikationsinhalte und der näheren Umstände der Kommunikation über die bei der Kommunikation anfallenden

[228] EDSA, Erklärung zur ePrivacy-VO; EDSB, Stellungnahme ePrivacy-VO, S. 2 f.

Verkehrsdatensätze, die Aufschluss über die äußeren Kommunikationsumstände geben können und damit auch Rückschlüsse auf Kommunikationsinhalte zulassen. Dabei sind auch juristische Personen nach dem TKG geschützt, soweit sie personenbezogene Daten über Telekommunikationsnetze übermitteln. Die erhöhten Vorgaben an den Datenschutz im Bereich der Telekommunikation sind in den §§ 91 ff. TKG bereichsspezifisch geregelt.

Adressaten der Datenschutzvorschriften des TKG sind Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, die in der Übertragung von Signalen über Telekommunikationsnetze (einschließlich Rundfunknetzen) gemäß § 3 Nr. 24 TKG bestehen. Telkommunikationsanbieter dürfen Informationen, die dem Fernmeldegeheimnis unterliegen, grundsätzlich nur für den Zweck der Erbringung der Telekommunikationsdienstleistung und für den Schutz der technischen Systeme im dazu erforderlichen Maß nach § 88 Abs. 3 DSGVO verwenden. Welche Kenntnisnahme konkret erforderlich ist, richtet sich nach den Umständen des Einzelfalls. Darüber hinaus besteht ein Kenntnisnahmeverbot.

2.4.1.3.4.1 Sensibilität von Standortdaten

Im Kontext vernetzter und automatisierter Fahrzeuge ist § 98 TKG besonders relevant. Danach dürfen Standortdaten zur Bereitstellung von Diensten mit Zusatznutzen nur im erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat.

2.4.1.3.4.2 M2M-Kommunikation

Im Kontext vernetzter und automatisierter Fahrzeuge wirft insbesondere die Maschine-zu-Maschine (M2M)-Kommunikation spezifische Fragstellungen auf, die in der geplanten ePrivacy-Verordnung geregelt werden sollen. Zumindest für die Übergangszeit muss jedoch anhand der bekannten Grundsätze unter Beachtung der verfassungsrechtlichen Vorgaben nach angemessenen Lösungen gesucht werden.

Abgrenzungsfragen ergeben sich dadurch, dass die M2M-Kommunikation neue Geschäftsmodelle ermöglicht und dabei die tradierte trennscharfe Unterscheidung zwischen dem Erbringen der (inhaltlichen) Dienstleistung und dem Erbringen der Übertragungsleistung zunehmend verwischt. Bei der M2M-Kommunikation sind regelmäßig mehrere Dienstleister eingebunden. Neben dem Dienstleister selbst, der die inhaltliche Dienstleistung erbringt, und dem Telekommunikationsanbieter, der die benötigte Telekommunikationsinfrastruktur bereitstellt, wird oftmals ein Dritter Dienstleister eingebunden, der die jeweilige Plattform betreibt. Der Betreiber kann aber auch mit dem Dienstleister in einer Person zusammenfallen. Bei Plattformbetreibern ist daher im Einzelfall zu klären, ob im Schwerpunkt der Übermittlungsvorgang im Vordergrund steht, und damit die jeweilige M2M-Leistung als Telekommunikationsdienstleistung anzusehen ist, die den Vorgaben des TKG bzw.

künftig der ePrivacy-Verordnung unterfällt, oder ob der Schwerpunkt auf der inhaltlichen Ebene der Dienstleistung liegt. Die Abgrenzung erfordert technisches Verständnis. Orientierung bei der Einordnung der jeweiligen Dienstleistung kann das ISO/OSI-Schichtenmodell bieten, das sich als Referenzmodell aus sieben Schichten zusammensetzt, von denen die ersten vier Schichten transportorientiert und die darüber liegenden Schichten fünf bis sieben als anwendungsorientiert und damit inhaltsbezogen eingeordnet werden.[229] Die verbindliche Klärung der Frage, ob auch internetbasierte Kommunikationsdienste (sog. OTT-Dienste), die selbst keinen Internetzugang vermitteln, in den Anwendungsbereich der Richtlinie 2002/21/EG (ePrivacy-Richtlinie) und damit unter das TKG fallen, liegt dem Europäischen Gerichtshof zur Klärung vor[230] und ist auch rechtspolitisch im Rahmen der geplanten ePrivacy-Verordnung umstritten.

2.4.1.3.4.3 Embedded SIM

Künftig wird auch genau zu prüfen sein, ob der Autohersteller, der eine sogenannte Embedded SIM (eSIM) verbaut und als Serviceleistung anbietet, Telekommunikationsdienstleistungen erbringt, den Vorgaben des TKG unterliegt und gemäß § 88 Abs. 2 TKG das Telekommunikationsgeheimnis beachten muss. Die Meldung an die Bundesnetzagentur kann dabei aber nur ein Anhaltspunkt sein, da die neuen Telekommunikationsdienstleistungsangebote auch von den Anbietern nur zögernd als solche erkannt und entsprechend an die Bundesnetzagentur gemeldet werden. [231] Indiz kann dabei sein, ob die Übertragungsleistung in der Abrechnung eingeschlossen ist und ob sie pauschal oder individuell abgerechnet wird.

Soweit keine Kommunikationsdienstleistungen erbracht werden, unterfallen auch die M2M-Dienste nicht den datenschutzrechtlichen Sonderbestimmungen des TKG. Vielmehr gelten die allgemeinen datenschutzrechtlichen Regeln Das sind derzeit die DSGVO, ergänzend das BDSG und ggf. bereichsspezifische (vgl. § 1 TMG; § 2 Nr. 12 a.E. IVSG). sowie ggf. länderspezifische Datenschutzbestimmungen.

2.4.1.3.5 Telemediengsetz

Ob die datenschutzrechtlichen Vorgaben der §§ 11 ff. Telemediengsetz (TMG) weiterhin anwendbar sind oder nach Art. 95 DSGVO verdrängt werden, bedarf weiterer Klärung. Der Gesetzgeber hat selbst den Anpassungsbedarf des TMG an die DSGVO erkannt, ist bislang aber untätig geblieben.[232]

---

[229] Grünwald/Nüßing, MMR 2015, 378 (380f.).

[230] Vgl. OVG Nordrhein-Westfalen, Beschluss v. 26.2.2018, - 13 A 17/16 -.

[231] Stender-Vorwachs/ Steege, MMR 2018, 212 (214 f.).

[232] OLG Frankfurt, Beschluss v. 06.09.2018, -16 W 27/18-, DE:OLGHE:2018:0906.16W27.18.00, Rn. 43 (m.w.N).

Besonders umstritten ist die Frage, ob das TMG insgesamt, oder nur die Bestimmungen des § 15 Abs. 3 TMG vom Anwendungsbereich der DSGVO verdrängt werden. Es spricht vieles dafür, dass die datenschutzrechtlichen Sonderbestimmungen der §§11-15a TMG seit dem 25.05.2018 insgesamt von der DSGVO verdrängt werden.[233] Sie beruhen nämlich nicht auf der ePrivacy-Richtlinie.[234]

Der Wegfall des TMG wirkt sich vor allem bei der Anwendung von § 15 Abs. 3 TMG aus. Nach dem Wortlaut dieser Vorschrift darf der Telemedienanbieter pseudonyme Nutzungsprofile ohne Einwilligung des Nutzers mit Widerspruchsmöglichkeit (sog. Opt-out) erstellen. Nach den grundrechtlichen Vorgaben der GRCh und den Vorgaben der ePrivacy-Richtlinie ist eine Opt-Out-Bestimmung jedoch europarechtswidrig und damit unanwendbar.[235] Der BGH teilt diese Bedenken und hat die Frage, ob eine Opt-out-Regelung in Form eines vorangekreuztes Kästchen den Vorgaben der ePrivacy-Richtlinie und der DSGVO entspricht, dem EuGH vorgelegt.[236]

Ferner fällt mit dem Wegfall des TMG auch die begriffliche Unterscheidung zwischen Bestands- und Nutzungsdaten weg, die einen deutschen Sonderweg darstellte und in der ePrivacy-Richtlinie keine Grundlage hat. Nutzungsdaten können je nach Einzelfall auch sensible Inhaltsdaten enthalten. Im Zuge der Einführung der ePrivacy-Verordnung soll daher künftig der Begriff der Metadaten eingeführt werden.

Da Telemediendienste auch dem besonders sensiblen Telekommunikationsgeheimnis verpflichtet sind, ist der Gesetzgeber gehalten, schnellstmöglich bereichsspezifische Regelungen zum Datenschutz zu erlassen, die den erhöhten Anforderungen der DSGVO und dem zusätzlich berührten Telekommunikationsgeheimnis durch konkrete Regelungen gerecht werden. Jedenfalls in der Übergangszeit müssen die bestehenden Normen grundrechtskonform ausgelegt werden, und den erhöhten Schutzbedarf berücksichtigen. Unabhängig von der Frage, welches Gesetz zur Anwendung kommt, sind insofern die gleichen grundrechtlichen Erwägungen zu berücksichtigen.[237] Die DSGVO ist daher besonders streng anzuwenden. So ergibt sich das bisher in § 13 Abs. 6 TMG normierte Recht auf anonyme oder pseudonyme Nutzung bei hohem Schutzbedarf vergleichbar aus der grundrechtskonformen Auslegung der DSGVO. Der Dienstanbieter kann ferner bislang nur dann eine namentliche Registrierung verlangen, wenn es nach § 14 Abs. 1 TMG für das Vertragsverhältnis erforderlich ist. Auch diese Anforderung

[233] DSK, Positionsbestimmung TMG.

[234] DSK, Positionsbestimmung TMG; BGH, EuGH-Vorlage vom 05. Oktober 2017 – I ZR 7/16 –, DE:BGH:2017:051017BIZR7.16.0, Rn. 16 (m.w.N.), juris.

[235] DSK, Positionsbestimmung TMG;.Jandt, ZD 2018, 405 ff., Benedikt, DB 2018, 80 ff.

[236] BGH, EuGH-Vorlage v. 05.10.2017 – I ZR 7/16 –, DE:BGH:2017:051017BIZR7.16.0., Rn. 12 ff., 30.

[237] Vgl. VGH München, Beschluss v. 26.09.2018, – 5 CS 18.1157 –, BeckRS 2018, 25018, Rn. 30.

ergibt sich aus Art. 6 Abs. 1 lit. b DSGVO. Auch die nach § 13 Abs. 4 TMG geforderten technischen und organisatorischen Maßnahmen sind in den Artt. 25, 32 DSGVO vorgeschrieben. Schließlich ist auch eine elektronische Einwilligung nach der DSGVO wie bisher nach dem TMG möglich.

2.4.1.3.6 eCall-Verordnung

Die flächendeckende Vernetzung ist eine notwendige Voraussetzung für das automatisierte Fahren und wird aktuell durch die eCall-Verordnung[238] vorangetrieben. Die eCall-Verordnung gilt seit April 2018 in den europäischen Mitgliedstaaten unmittelbar und schreibt für die Typenzulassung von Pkws und leichter Nutzfahrzeuge innerhalb der EU eine automatische Notrufeinheit vor. Das eCall-System beinhaltet neben einem GPS-Empfänger auch eine Telemetrie-Einheit und einen Unfalldatenspeicher. In der eCall-Verordnung ist zwar ausdrücklich festgeschrieben, dass die Unfalldaten nur im Falle eines Unfalls gespeichert und ausschließlich zu Zwecken des Notrufs verarbeitet werden dürfen, Art. 6 eCall-Verordnung. Eine anderweitige Nutzung ist verboten und nicht genutzte Daten müssen gelöscht werden. Damit stehen die Daten weder für Private noch für staatliche Organe außerhalb der engen Zweckbestimmung der Notrufbearbeitung zur Verfügung und dürfen für andere Zwecke weder erhoben noch verwertet werden. Ferner sind die Vorgaben der eCall-Verordnung künftig Bestandteil der EU-Typenzulassung.

Nach den Vorgaben der eCall-Verordnung ist es aber zulässig, auch ein von einem Privatanbieter angebotenes Notrufsystem zu verwenden. Die Nutzung dieses privaten Notrufsystems durch andere Dienste wird in der eCall-Verordnung weder ausgeschlossen noch reguliert, daher können auch datengetriebene Dienste ihre Geschäftsmodelle kostengünstig auf dieser neuen Schnittstelle zwischen Auto und Internet aufsetzen.[239] In Zukunft ist daher eine Angebotszunahme datengetriebener und besonders ortsbasierter Dienste auch abseits von Mobilitätsdiensten zu erwarten. Beispiele sind auf die individuelle Fahrweise bezogene Pay-as-you-drive Versicherungstarife oder das ortsbezogene Anzeigen von freien Parkplätzen, interessanten Sehenswürdigkeiten oder das Anbieten von Carsharing-Angeboten. Bislang werden solche Dienste noch über Telematik-Boxen oder durch Einbindung von Smartphone-Apps über das Infotainment-System realisiert, wenn nicht herstellerseitig bereits eine fest verbaute sog. „embedded SIM“ (eSIM) integriert ist.

---

[238] Verordnung (EU) 2015/758 vom 29.04.2015 über Anforderungen für die Typengenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG.

[239] Krit. Lüdemann/ Sengstacken, RDV 2014, 177 (180).

2.4.1.3.7 Messstellenbetriebsgesetz

Für das Smart Grid bzw. die elektronische Ladeinfrastruktur der Ladesäulen gelten die datenschutzrechtlichen Vorschriften des Messstellenbetriebsgesetzes (MsbG). Es bestehen keine Anhaltspunkte dafür, dass die DSGVO das MsbG verdrängt, jedoch müssen die einschlägigen Normen des MsbG im Lichte der DSGVO angewendet werden.

Im Bereich der E-Mobilität wurde das Rollout der Smart Grids („intelligente Netze“) bereits begonnen. Smart Grids sind mithilfe der durch Smart Meter („intelligente Zähler“) erstellten Messdaten an den Einspeise und Verbrauchspunkten in der Lage, Energieerzeugung und Energiebedarf zu koordinieren. Insbesondere durch die Messdaten können Lastprofile und damit auch Nutzungs- und Bewegungsprofile erstellt werden.[240] Hierfür enthält das MsbG spezifische Datenschutzvorschriften.

Das Verhältnis zwischen dem Endkunden, der sein E-Fahrzeug an der Ladesäule aufladen möchte, und dem Ladesäulenbetreiber gelten nicht die Vorschriften des MsbG, sondern die allgemeinen datenschutzrechtlichen Vorgaben. Daher findet die Vorschrift des § 40 EnWG, der Vorgaben an die Abrechnung aufstellt und datenschutzfördernden Bezahlverfahren entgegenstehen könnte, insoweit keine Anwendung. Soweit ein Dienst auf die sensiblen Lastdaten zu Abrechnungszwecken zugreifen möchte, sind insbesondere die Risiken der Verkettung, die mit der Anbindung an die Smart-Metering-Infrastruktur einhergehen, gebührend zu berücksichtigen.

2.4.1.3.8 Rundfunkstaatsvertrag

Der Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag, RStV) soll Datenschutz und Medienprivileg bei Anbietern von Rundfunkinhalten in einen angemessenen Ausgleich bringen. Der einundzwanzigste Rundfunkänderungsstaatsvertrag ist zeitgleich mit der DSGVO in Kraft getreten, um den dem nationalen Gesetzgeber gemäß Art. 85 DSGVO eröffneten weiten Umsetzungsspielraum auszufüllen. § 47 Abs. 1 RStV, der bislang auf die allgemeinen Regeln verwies, wurde dabei durch eigene bereichsspezifische Regelungen zum Datenschutz ersetzt. So unterliegen die Verarbeitungstätigkeiten zu journalistischen Zwecken dem Datengeheimnis und dürfen nach § 9c Abs. 1 S. 1-3 RStV nicht zu anderen Zwecken verarbeitet werden. Die allgemeinen Regeln der DSGVO gelten im Übrigen aber nur sehr eingeschränkt, vgl. § 9c Abs. 1 S. 4 RStV.

Rundfunk bzw. Broadcast ist dadurch gekennzeichnet, dass das Sendesignal gleichmäßig in alle Richtungen abgestrahlt wird. Der Sender speist lediglich das Signal in das

[240] Ausführlich: Lüdemann/Ortmann/Pokrant, RDV 2016, 125 ff.

Trägermedium ein und hat danach keinen Einfluss mehr darauf, insbesondere, durch wen das Signal empfangen wird (sog. One-to-Many-Aussendung ohne Rückkanal).[241]

Das Gegenstück zum Broadcast ist der Unicast, bei dem eine individuelle Verbindung zwischen Sender und Empfänger hergestellt wird. Darunter fällt beispielweise die Individualkommunikation ebenso wie die tradierte Übertragung von Datenpaketen im Internet, bei der Inhalte auf die Anfrage eines Clients vom Server, dem Sender, an die vom Client mitgeteilte Adresse zu einem anderen Client, dem Empfänger, geschickt werden. Das ist aber keinesfalls zwingend, so sieht IPv6 grundsätzlich auch eine Multicast-Übertragungsweise vor, bei der beide Ansätze kombiniert werden.[242]

Die Datenübermittlung im Rahmen von C-ITS mittels DAB+ sowie die speziellen WiFi-Technologie zum Austausch von V2V-Messages dürften dem Rundfunkbegriff unterfallen, da sie die genannten Merkmale von Broadcast erfüllen. Allerdings dient V2V zumindest teilweise der Übermittlung von Individualkommunikation über ad hoc Netze[243]. Auch die flächendeckende Datenerhebung von Echtzeitverkehrsinformationen via V2X ist datenschutzrechtlich besonders sensibel, weil damit die Möglichkeit zu einer seriellen Erfassung einer Vielzahl von Standortdaten einhergeht.[244]

Allerdings ist zweifelhaft, ob der Rundfunkstaatsvertrag auch geeignet ist, die Interessen der an der Verarbeitung Beteiligten angemessen auszugleichen. Denn die C-ITS-Kommunikation dient nicht journalistischen Zwecken, sondern soll unter anderem automatisierte Fahrfunktionen und damit andere Zwecke ermöglichen. Damit ist die Hoffnung verbunden, die Verkehrsunfälle zu senken, Effizienz und Nachhaltigkeit zu steigern, sowie einen Zugewinn an Komfort für den Nutzer zu erreichen. Demgegenüber stehen die Schutzbedürfnisse der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Grundrechtsträger auf Wahrung ihrer Grundrechte aus Artt. 7, 8 GRCh bzw. aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und ggf. Art. 10 GG. Daher ist eine spezialgesetzliche Regelung erforderlich, um diese Interessenlage angemessen auszugleichen.

2.4.1.3.9 Bundesdatenschutzgesetz n.F.

Der nationale Gesetzgeber hat von der Möglichkeit, ergänzende Bestimmungen zu erlassen, Gebrauch gemacht. Das überarbeitete Bundesdatenschutzgesetz (BDSG n. F.)

---

[241] Assion, 2015, S.44, S.102.

[242] Ausführlich zu IPv6 vgl. DSK, AK Technik 2012.

[243] Artikel-29-Datenschutzgruppe, WP 252, S. 10.

[244] Vgl. zum dadurch erhöhten Schutzbedarf: BVerfG, Urteil v. 11.03.2008, , - 1 BvR 2074/05 -, - 1 BvR 1254/07 -, http://www.bundesgerichtshof.de, Rn 71, 73.

ist Kernbestandteil des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU [245] (DSAnpUG-EU) und ist zeitgleich mit den neuen europäischen Bestimmungen am 25.05.2018 in Deutschland in Kraft getreten. Das BDSG n. F. enthält Regelungen für öffentliche und nichtöffentliche Stellen des Bundes und der Länder. Mit ihm sollen die neuen europäischen Vorgaben, insbesondere der Polizei-Richtlinie, umgesetzt werden und an einigen Stellen die Vorgaben der DSGVO spezifiziert werden. Inwieweit die teilweise vorgenommenen Einschränkungen, insbesondere zu Zweckänderungen und Ausnahmen von den Informations- und Auskunftspflichten den Vorgaben der DSGVO genügen, ist noch nicht abschließend beurteilbar.

In Art. 88 DSGVO i.V.m. § 26 BDSG n. F. finden sich besondere Bestimmungen für die Verarbeitung personenbezogener Daten von Beschäftigten durch den Arbeitgeber. Besondere Grenzen sind bei der Einholung von Einwilligungen von Arbeitnehmern gegenüber dem Arbeitgeber zu beachten. [246] Nach ErwG 155 DSGVO ist die Einwilligung im Arbeitsverhältnis nicht grundsätzlich ausgeschlossen, sondern kann von den Mitgliedstaaten ausgestaltet werden. Dabei ist aber das besondere Abhängigkeitsverhältnis des Arbeitnehmers, der mit dem Arbeitsverhältnis seine Existenzgrundlage sichern muss, in die Betrachtung einzubeziehen und schonend auszugleichen.[247] Der Bundesgesetzgeber hat hierzu eine Regelung in § 26 BDSG n.F. erlassen.

Ferner besteht nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz ein Mitbestimmungsrecht des Betriebsrates, wenn technische Einrichtungen, die dazu bestimmt sind, das Verhalten der Beschäftigten zu überwachen, eingesetzt werden sollen. Diese Vorschrift dürfte bei dem Einsatz von smart cars in Firmenflotten oder bei der Gebrauchsüberlassung von Firmenwagen an Arbeitnehmer relevant werden.

2.4.1.3.10 Landesdatenschutzgesetze

Die einzelnen Landesdatenschutzgesetze der Bundesländer stellen für die Verarbeitung personenbezogener Daten durch ihre öffentlichen Stellen spezifische Bestimmungen bereit, auf deren Details vorliegend nicht näher einzugehen ist.

2.4.1.4 Wahrnehmung berechtigter Interessen

Der Verantwortliche kann sich gem. Art. 6 Abs. 1 lit. f DSGVO auf die Wahrnehmung seiner berechtigten Interessen berufen, soweit die Verarbeitung dazu erforderlich ist

[245] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BGBl. I 2017, S. 2079 ff.

[246] Artikel-29-Datenschutzgruppe, WP 252, S. 12.

[247] Vgl. Artikel 29-Datenschutzgruppe, WP 249.

und die Interessen, Grundrechte und Grundfreiheiten der von der Verarbeitung betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Die Rechtsgrundlage in Art. 6 Abs. 1 lit.f DSGVO ist aus Art. 7 lit. f der Datenschutzrichtlinie 95/46/EG übernommen worden, weshalb die bisherigen Grundsätze und Ziele der Richtlinie, einschließlich der EuGH-Rechtsprechung auch unter der DSGVO fortgelten.[248]

Der EuGH hat 2017 klargestellt, dass die Norm drei Voraussetzungen enthält, die kumulativ vorliegen müssen.[249] Das berechtigte Interesses, die Erforderlichkeit und die vorzunehmende Abwägung werden nachfolgend näher untersucht.

2.4.1.4.1 Berechtigtes Interesse des Verantwortlichen

Zunächst muss beim Verantwortlichen ein berechtigtes Interesse vorliegen. Vor dem teleologischen Hintergrund der Norm, wonach ein Ausgleich durch eine Abwägung der involvierten Interessen angestrebt wird, ist der Begriff der berechtigten Interessen weit zu verstehen und kann neben rechtlich geschützten Interessen auch wirtschaftliche oder ideelle Interessen des Verantwortlichen oder eines Dritten erfassen.[250] Das Interesse, eine persönliche Information über eine andere Person zu erlangen, muss dabei aber von der Rechtsordnung anerkannt werden bzw. rechtlich zulässig sein. [251] Der Verantwortliche ist befugt, aber nicht verpflichtet, Daten an einen Dritten zur Verwirklichung dessen berechtigter Interessen zu übermitteln.[252]

2.4.1.4.2 Erforderlichkeit

Nach dem EuGH ist die Voraussetzung der Erforderlichkeit in Art. 6 Abs. 1 lit. f DSGVO so auszulegen, dass „*sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen*.“[253] Der EuGH versteht den Rechtsbegriff der Erforderlichkeit also mit demselben Inhalt, wie er ihn auch in Art. 51 Abs. 1 GRCh im Rahmen der Verhältnismäßigkeit definiert und wie es aus Gründen der Rechtssicherheit und Fairness auch geboten ist. Diese Rechtsgrundlage

[248] ErwG 9 DSGVO; BGH, Urteil v. 12.07.2018, -III ZR 183/17-, DE:BGH:2018:120718UIIIZR183.17.0, Rn. 75, 94.

[249] EuGH, Urteil v. 04.05.2017,– C-13/16 –, ECLI:EU:C:2017:336, BeckRS 2017, 108615, Rn. 28.

[250] OLG München, Teilurteil v. 24.10.2018, –3 U 1551/17–, DE:OLGMUEN:2018:1024.3U1551.17.0A, Beck RS 2018, 27477, Rn. 30.

[251] Artikel 29-Datenschutzgruppe, WP 217, S. 32, 35 f.; EuGH, Urteil v. 04.05.2017,– C-13/16 –, ECLI:EU:C:2017:336, BeckRS 2017, 108615, Rn. 29.

[252] EuGH, Urteil v. 04.05.2017,– C-13/16 –, ECLI:EU:C:2017:336, BeckRS 2017, 108615, Rn. 26.

[253] EuGH, Urteil v. 04.05.2017,– C-13/16 –, ECLI:EU:C:2017:336, BeckRS 2017, 108615, Rn. 30 (m.w.N.).

darf damit nicht zu einer unangebracht weit gefassten Auslegung der Datenverarbeitung führen, wobei geprüft werden muss, ob zur Zweckerreichung andere, weniger einschneidende Maßnahmen zur Verfügung stehen[254].

2.4.1.4.3 Abwägung mit den Rechten der betroffenen Person

Sodann ist in einem dritten Schritt eine umfangreiche Abwägung der jeweiligen gegenüberstehenden Rechte und Interessen vorzunehmen, die von den konkreten Umständen des jeweiligen Einzelfalls abhängt.[255] Dabei ist maßgeblich, ob die betroffene Person nach Treu und Glauben mit der Weitergabe rechnen kann, und inwieweit der Verantwortliche die Informationen auch auf anderem Wege, beispielsweise durch Einholung einer Einwilligung, beschaffen kann.[256] Ferner können nach dem EuGH die Grundrechte der betroffenen Person durch die Datenverarbeitung unterschiedlich stark beeinträchtigt sein, je nachdem, ob die in Rede stehenden Daten öffentlich zugänglich sind oder nicht.[257] Der BGH stellt insoweit heraus, dass sich die Abwägung nach dem Schutzbedarf und insbesondere nach ErwG 47 DSGVO richten muss, wonach die *„vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“* ebenso zu berücksichtigen sind, wie der Umstand, ob die betroffene Person zum Erhebungszeitpunkt und angesichts der Verarbeitungsumstände vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.[258]

2.4.1.4.3.1 Erfordernis einer speziellen Rechtsgrundlage bei hohem Risiko

Der EuGH betont, das bei potentiell schwerwiegenden bzw. persönlichkeitsrelevanten Eingriffen allein ein wirtschaftliches Interesse nicht ausreicht, um den Eingriff in Form der Verknüpfung von für das Privatleben sensiblen Informationen mit dem Namen zu rechtfertigen.[259] Auch die Artikel 29–Datenschutzgruppe betont die wichtige Unterscheidung zwischen öffentlichen und geschäftlichen Interessen und die besondere Sensibilität von Standortdaten.[260]

[254] Artikel 29-Datenschutzgruppe, WP 217, S. 37.

[255] EuGH, Urteil v. 04.05.2017,– C-13/16 –, ECLI:EU:C:2017:336, BeckRS 2017, 108615, Rn. 31.

[256] VGH München, Beschluss v. 26.09.2018, – 5 CS 18.1157 –, BeckRS 2018, 25018, Rn. 27, 29.

[257] EuGH, Urteil v. 04.05.2017,– C-13/16 –, ECLI:EU:C:2017:336, BeckRS 2017, 108615, Rn. 32.

[258] BGH, Urteil v. 12.07.2018, -III ZR 183/17-, DE:BGH:2018:120718UIIIZR183.17.0, Rn. 84 ff., 87.

[259] Vgl. EuGH, Google, NVwZ 2014, 857 (863, 864), Rn. 81, Rn. 97, Rn 98, beck-online.

[260] Artikel-29-Datenschutzgruppe, WP 252, S. 14.

Auch nach der Rechtsprechung des BVerfG bedarf es nur dann keiner speziellen Rechtsgrundlage, wenn nur geringfügig in die Grundrechte eingegriffen werden soll.[261] Das Grundrecht auf informationelle Selbstbestimmung ist hingegen dann in erheblicher Weise betroffen und es bedarf einer spezialgesetzlichen Grundlage, wenn die angefragten Daten aussagekräftige Rückschlüsse auf die betroffene Person zulassen. Nach dem Bundesgerichtshof ist das insbesondere dann der Fall, wenn aus den angeforderten Daten (wenn auch nur grobgranulare) Bewegungsprofile ableitbar sind.[262] Bei Fahrzeugdaten, die Orts- und Zeitangaben beinhalten und damit Bewegungsprofile ermöglichen, oder die Rückschlüsse auf die Fahrweise oder vergleichbare Profilbildungen zulassen, überwiegt daher in den meisten Fällen das schützenswerte Interesse der betroffenen Person, dass die auf sie beziehbaren Daten nur dann verarbeitet werden dürfen, wenn sie ihre Einwilligung erteilt hat.

Die Rechtsgrundlage aus Art. 6 Abs. 1 lit. f DSGVO ist daher nur für nicht-eingriffsintensive Verarbeitungen geeignet. Die Norm besitzt damit insbesondere keine Auffangfunktion und greift keinesfalls immer dann ein, wenn eine andere Rechtsgrundlage nicht einschlägig ist.[263]

Im Kontext vernetzter Fahrzeuge dürfte die Norm aufgrund der zahlreichen Profilbildungsmöglichkeiten bei umfangreichen Datensammlungen oder der Verwendung von Standortdaten, die bei dem Betrieb anfallen, daher nur einen äußerst geringen Anwendungsbereich aufweisen. Jedenfalls dürfte das Interesse der betroffenen Person dann überwiegen, wenn das hohe Risiko nicht zugleich durch technische und organisatorische Maßnahmen, wie eine wirksame Pseudonymisierung, wirksam begrenzt wird. Daher hat das Ergreifen geeigneter Schutzmaßnahmen auch direkte Auswirkungen auf die Rechtmäßigkeit und damit die Legitimationsgrundlage der Verarbeitung.

Die betroffene Person hat bei dieser Rechtsgrundlage zudem nach Art. 21 Abs. 1 DSGVO ein jederzeitiges Widerspruchsrecht, auf das der Verantwortliche nach Art. 21 Abs. 4 DSGVO spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich hinweisen muss.

---

[261] BVerfG, Beschluss v. 17.2.2009 - 2 BvR 1372/07, Rn. 31 (m.w.N.), Rn. 26 f.

[262] Vgl. zum Eingriffsgewicht von Standortdaten und damit ermöglichten Bewegungsprofilen: BGH, Beschluss v. 8.2.2018, - 3 StR 400/17 -, Rn. 6.

[263] Robrahn/Bremert, ZD 2018, 291 (291).

2.4.1.4.3.2 Produktbeobachtungspflichten und Maschinelles Lernen

Fraglich ist im Kontext vernetzter und automatisierter Fahrzeuge, ob die Produktbeobachtungspflichten des Herstellers auf die Rechtsgrundlage von Art. 6 Abs. 1 lit. f DSGVO gestützt werden können.

Dem Produkthersteller obliegen unter anderem Instruktions- und Produktbeobachtungspflichten, um solche Gefahren aufzudecken, die aus der Verbindung seines Produktes mit Produkten anderer Hersteller entstehen können.[264] Die Produktbeobachtungspflicht erstreckt sich auch auf die mit dem Produkt verbreitete Software und ihre Kombinationsmöglichkeiten mit anderen Produkten.

Um die Software zu pflegen, erhält der Hersteller daher oftmals Zugriffsmöglichkeiten auf die Software. Das kann dem Hersteller die Möglichkeit eröffnen, eine weitere Schnittstelle für eine Fernwartung einzurichten die einen Datenzugriff ermöglicht.

Allerdings erstreckt sich die Produktbeobachtungspflicht nur auf öffentlich verfügbare Informationen.[265] Sie verlangt lediglich eine Marktbeobachtung. Daher fehlt es bereits an der Voraussetzung der Erforderlichkeit.

Der Fahrer wird darüber hinaus regelmäßig keine Erwartung in der Richtung haben, dass eine Beobachtung von potentiell gefährlichen Produkten auch zur Sammlung seiner personenbezogenen Daten dient. Insoweit ist zu berücksichtigen, dass die relevanten Fahrzeugdaten, wie beim Personenbezug ausführlich dargestellt, regelmäßig auch Aufschluss über ein Nutzungsverhalten geben können und damit eine Profilbildung möglich ist, wenn nicht eine Identifikation wirksam verhindert wird. Es kann dann auch nicht ausgeschlossen werden, dass einmal vorliegende Daten zu Beweiszwecken in Zivil- oder Strafverfahren zur Klärung der Schuldfrage z.B. im Rahmen eines Schadensfalls verwendet werden, oder um erhobene Garantie- oder sonstige Ansprüche des Fahrers abzuwehren. Daher überwiegen die Interessen der betroffenen Person und es bedarf einer expliziten Einwilligung, wenn ein Rückbezug auf das Individuum weiterhin möglich ist.

Auch der Zweck, Daten zur Fortentwicklung der Algorithmen zum Maschinellen Lernen zu verwenden, bedarf als personenbezogen einer Rechtsgrundlage, sofern nicht ausschließlich vollständig anonymisierte Daten verarbeitet werden.[266]Wie bereits beim Personenbezug dargestellt, sind sowohl die Erhebung in Anonymisierungsabsicht als auch der Anonymisierungsvorgang selbst als Verarbeitung personenbezogener Daten

[264] Vgl. BGH NJW 1987, 1009 ff.

[265] Vgl. BGHZ 80, 199 (202 f.); BGH NJW 1990, 906 (907 f.); Spindler 2007, S. 59.

[266] ErwG 26 S. 5 DSGVO (argumentum e contrario).

einzuordnen. Bei der Einzelfallabwägung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO ist zu beachten, dass bei Anonymisierungsmaßnahmen aufgrund der Vielzahl der Daten schon anhand weniger bekannter Parameter die Gefahr der Re-Identifizierung besteht, und das, wie zuvor dargestellt, erhebliche Auswirkungen auf die betroffenen Personen haben kann.

Daher dürfte das Interesse der betroffenen Person, dass keine Profile von ihr erstellt werden, jedenfalls dann überwiegen, wenn keine risikomindernden technischen und organisatorischen Maßnahmen zur Verhinderung der Identifikation, die auch praktisch wirksam sind, ergriffen werden.[267]

2.4.1.5 Notwendigkeit bereichsspezifischer Regelungen

Im dynamischen Gebiet des vernetzten, automatisierten und kooperativen Verkehrs entsteht zunehmend weiterer gesetzlicher Regelungsbedarf. Nachfolgend wird daher untersucht, wann der grundrechtliche Schutzbedarf bereichsspezifische Regelungen erfordert.

Nach der bereits genannten Auffassung der Artikel 29-Datenschutzgruppe wird im C-ITS-Kontext langfristig eine bereichsspezifische Rechtsgrundlage i.S.d. Art. 6 Abs. 1 lit. c DSGVO erforderlich werden, soweit dies dem öffentlichen Interesse zur Erhöhung der Verkehrssicherheit, der Förderung der Verkehrseffizienz und der ökologischen Nachhaltigkeit dienlich ist.

Nach den bereits dargestellten Vorgaben des BVerfG reichen immer dann, wenn ein besonders hohes Risiko für die Grundrechte besteht, allgemeine Rechtsgrundlagen wie die in der DSGVO enthaltenen, die für alle möglichen Verarbeitungskontexte allgemein gehaltene Regeln aufstellt, nicht mehr aus, um dem hohen Schutzbedarf gerecht zu werden. Vielmehr sind nach dem Bestimmtheitsgrundsatz spezielle gesetzliche Regelungen erforderlich, die dieses spezifische Risiko auch angemessen adressieren, indem sie die speziellen beteiligten Interessen grundrechtskonform ausgleichen und somit ein höheres Maß an Rechtssicherheit erzeugen können.

Hoch- und vollautomatisierte Fahrfunktionen benötigen ein möglichst genaues Abbild der Umwelt, um die originäre Aufgabe des Fahrers zuverlässig übernehmen zu können. Um den Nahbereich einschätzen zu können, kommen unterschiedliche intelligente Sensoren zum Einsatz, die mit Aktorik und Steuergerät verbunden sind. Zum Einsatz kommen aufgrund der benötigten hohen Zuverlässigkeit unterschiedliche Techniken wie Kamera, Infrarot, Radar und Lidar. Zusätzlich tauscht das Fahrzeug mit der Verkehrsinfrastruktur und anderen Verkehrsteilnehmern Nachrichten aus (V2X-

[267] Vgl. ErwG 47, ErwG 49 DSGVO

Kommunikation), um Verkehrsmeldungen zu erhalten oder an der Grünphasenprediktion teilzunehmen. Auch mit anderen Fahrzeugen werden Nachrichten (V2V-Kommunikation) ausgetauscht, um sich bei plötzlich auftretenden Gefahren zurechtzufinden. Die Kommunikation ist hybrid angelegt und vollzieht sich neben infrastrukturloser Kommunikation zudem auch über das mobile Internet.

Die Grundrechtsrelevanz, die Neuartigkeit, die Kombination der eingesetzten Technologien und die Komplexität des Gesamtsystems des vernetzten, automatisierten und kooperativen Fahrens machen insoweit bereichsspezifische Regelungen zum Datenschutz erforderlich, die aber noch nicht erlassen ist.

Wie bereits bei der Bestimmung der Verantwortung dargelegt, wird zudem angestrebt, dass im Kontext von intelligenten Verkehrssystemen in Zukunft Verkehrsmanagementzentralen und verschiedene Mobilitätsdienste – beispielsweise in den Bereichen Straßenverkehrssicherheit, Verbindung zwischen Fahrzeug und Verkehrsinfrastruktur oder Verkehrs- und Frachtmanagement – mit den Datenanbietern von Verkehrsinformationen kooperativ und vernetzt zusammenwirken sollen.[268] Im Gesetzgebungsverfahren müssen im Hinblick auf das Gesamtsystem die dadurch eröffneten Risiken ebenfalls klaren gesetzlichen Regelungen unterliegen.

Der Gesetzgeber ist daher aufgefordert, bereichsspezifische Regelungen zu erlassen, auch soweit Risiken dadurch entstehen, dass private Dienstanbieter in die fahrsicherheitsrelevante Gesamtarchitektur einbezogen sind, wie beispielsweise Anbieter von Fahrerassistenzsystemen. Die datenschutzrechtlichen Belange müssen dabei einer sorgfältigen Verhältnismäßigkeitsprüfung unterzogen werden.

2.4.1.5.1 Pflichteinführung von Fahrerassistenzsystemen über die Vorschriften zur Typengenehmigung

Den Fahrerassistenzsystemen wird eine wichtige Funktion bei der Einführung automatisierter Fahrfunktionen zugeschrieben, da automatisierte Fahrzeuge als Zusammenfassung verschiedener Assistenzfunktionen betrachtet werden können.[269] Mit ihrer Einführung wird daher ein evolutiver Weg hin zum automatisierten Fahren beschritten.[270] Eine Einführung ist dabei nur über die Änderung der Vorgaben zur Typengenehmigung von Fahrzeugen möglich.[271]

---

[268] Vgl. ausführlich BMVI, IVS-Aktionsplan „Straße“, S. 27 ff.

[269] BMVI, Strategie automatisiertes und vernetztes Fahren, S. 5; Europäische Kommission, COM(2016) 766 final, S. 14.

[270] Jourdan/Matschi, NZV 2015, 26 (28).

[271] Zu den zulassungsrechtlichen Rahmenbedingungen vgl. Arzt/ Ruth-Schumacher, NZV 2017, 57 ff.

Aktuell wird hierzu auf EU–Ebene eine Verordnung zur Änderung der Typengenehmigung abgestimmt, die in Artikel 6 eine Reihe von nichtabschaltbaren Fahrerüberwachungsdiensten zwingend vorschreiben will (z.B. intelligenter Geschwindigkeitsassistent; Systeme zur Schläfrigkeits- und Aufmerksamkeits-überwachung des Fahrers, zur Erkennung von Ablenkungen; Rückwärtsfahrt-Erkennung; Erleichterung des Einbaus von Sperren zur Verhinderung von Alkoholfahrten)[272] In dem Verordnungsentwurf heißt es, dass die Grundrechte aus Artt. 7, 8 GRCh nicht berührt werden, da die Vorgaben der DSGVO von den Dienstanbietern zu beachten sein werden. Datenschutzrechtliche Erwägungen finden sich darüber hinaus nicht in dem Entwurf.

Der EuGH hat aus Art. 8 GRCh eine Pflicht der Gesetzgebungsorgane der EU hergeleitet, die Grundrechte der Betroffenen im Gesetzgebungsverfahren umfassend gegen die kollidierenden öffentlichen Belange abzuwägen. [273] Auch der europäische Datenschutzbeauftragte hebt die sorgfältige Prüfung des unionsrechtlichen Grundsatzes der Verhältnismäßigkeit bei Erlass eines Gesetzes hervor und hat dafür ein Toolkit zur Erforderlichkeitsprüfung für die Organe der EU zusammengestellt.[274] Der Schutzbedarf wird im Hinblick auf Artt. 8, 7 GRCh [275] gleichwohl vielfach übersehen. Der Verordnungsentwurf ist hierfür ein Beispiel und der bloße Verweis auf die DSGVO unzureichend.

Die gesetzliche Verpflichtung zum Einbau und damit auch zum Führen eines Fahrzeugs mit nicht abschaltbaren Assistenzsystemen zur Fahrer- und/oder Umfeldüberwachung muss vielmehr auch selbst einen verhältnismäßigen Eingriff in die Grundrechte der betroffenen Personen aus Artt 7, 8 GRCh darstellen.

Mit dem Verweis auf die DSGVO überträgt die Europäische Kommission die angezeigte Verhältnismäßigkeitsprüfung von Art. 6 des Verordnungsentwurfs auf den einzelnen Anbieter. Sie ist aber selbst unmittelbar an die GRCh gebunden und sollte bereits im Gesetzgebungsverfahren die notwendigen Vorrkehrungen für den Schutz der personenbezogenen Daten gemäß den Artt. 7, 8 GRCH bei der Pflichteinführung der datenintensiven Verarbeitungen bereichspezifisch festschreiben.

---

[272] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates 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 Verordnung (EU) 2018/… und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009, Brüssel, Mai 2018, 2018/0145 (COD), COM(2018) 286 final, S. 13.

[273] EuGH, MMR 2011, 122 – Schecke und Eifert.

[274] EDPS, Toolkit Erforderlichkeit, 6 f., 9, 13.

[275] Vgl. zu C-ITS: Artikel-29-Datenschutzgruppe, WP 252, S. 10.

Mit Blick auf die Artt. 7, 8 GRCh ist besonders problematisch, dass mit Einführung dieser Verordnung die Einbeziehung der datenintensiven Technologien in den Straßenverkehr faktisch zur zwingenden Vorschrift wird.

Die Artikel-29-Datenschutzgruppe betont im Kontext von C-ITS die Notwendigkeit, eine gesetzliche Regelung einer umfassenden Verhältnismäßigkeitsprüfung zu unterziehen und stellt zu Recht dem Aufzwingen einer „allgegenwärtigen Verfolgung“ eine freie Teilnahme an C-ITS gegenüber, die den Menschen die Freiheit der Entscheidung überlässt.[276]

Die Verpflichtung zum Einbau nicht abschaltbarer Assistenzsysteme über das Zulassungsrecht führt jedoch genau zu diesem Ergebnis. Es steht faktisch einer Pflichteinführung gleich, da nur noch Fahrzeuge, die mit diesen nicht mehr abschaltbaren, teilweise datenintensiven Assistenzsystemen ausgestattet sind, am Markt verfügbar wären. Fahrzeuge sind für den Betrieb im Straßenverkehr bestimmt, wozu es zwingend auch einer Typengenehmigung bedarf. Betroffenen Personen wäre bei der faktischen Einführung daher ein informationeller Selbstschutz nur noch durch die Nichtteilnahme am motorisierten Straßenverkehr und damit praktisch unmöglich.

Daher sind die absoluten Grenzen gesetzlicher Gestaltungsmöglichkeiten eingehender zu betrachten.

2.4.1.5.2 Absolute Grenzen gesetzlicher Gestaltungsmöglichkeiten

Nachfolgend wird untersucht, inwieweit die rechtlichen Gestaltungsmöglichkeiten im Kontext der Einbindung von Dienstleistern in das Gesamtsystem des automatisierten, vernetzten und kooperativen Fahrens durch die ethischen gesellschaftlichen Grundentscheidungen, die in den Grundrechten auf Datenschutz der Artt. 7, 8 GRCh bzw. Artt. 2 Abs. 1, 1 Abs. 1 GG zum Ausdruck kommen, beeinflusst und begrenzt werden. Aufgrund der begrenzten Zuständigkeiten der EU und der engen Verzahnung von europäischem und nationalem Recht dürfen dabei die nationalen grundrechtlichen Vorgaben nicht außer Betracht bleiben.

Die vom Bundesministerium für Verkehr und digitale Infrastruktur mit der Erstellung ethischer Leitlinien beauftragte Ethik-Kommission betont, dass es Wesentlich auf die Bedingungen und Ausgestaltungen der autonomen Systeme ankommen wird und stellt klar: *„Die technische Entwicklung gehorcht dem Prinzip der Privatautonomie im Sinne eigenverantwortlicher Handlungsfreiheit.“*[277] *„Die eigenverantwortliche Entscheidung des Menschen ist Ausdruck einer Gesellschaft, bei der der Mensch mit seinem*

[276] Artikel-29-Datenschutzgruppe, WP 252, S. 11 f.

[277] Ethik–Kommission, S. 10, ethische Regel Nr. 1.

Entfaltungsanspruch und seiner Schutzbedürftigkeit im Zentrum steht. Jede staatliche und politische Ordnungsentscheidung dient deshalb der freien Entfaltung und dem Schutz des Menschen." [278] *„Eine gesetzlich auferlegte Pflicht zur Nutzung vollautomatisierter Systeme oder die Herbeiführung einer praktischen Unentrinnbarkeit ist ethisch bedenklich, wenn damit die Unterwerfung unter technische Imperative verbunden ist."*[279]

Auch das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass *„das allgemeine Persönlichkeitsrecht gewährleistet, dass in der Rechtsordnung gegebenenfalls die Bedingungen geschaffen und erhalten werden, unter denen der Einzelne selbstbestimmt an Kommunikationsprozessen teilnehmen und so seine Persönlichkeit entfalten kann. Dazu muss dem Einzelnen ein informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein. […] Die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht gebietet den zuständigen staatlichen Stellen vielmehr, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen."* [280] *„Hierfür müssen der betroffenen Person datenschutzfreundliche Alternativen derart zur Verfügung stehen, dass ihr Möglichkeiten zu informationellem Selbstschutz geboten werden, die sie auch ausschlagen können muss."*[281]

Die Freiheit des Einzelnen, sich unerkannt, unbeobachtet und frei von A nach B bewegen zu können, darf nach dem Bericht der Ethik-Kommission zudem nicht einer auf Effizienz beruhenden, zentralisierten digitalen Verkehrsinfrastruktur geopfert werden; Das könnte zu einer Totalüberwachung der Verkehrsteilnehmer führen.[282] *„Autonomes Fahren ginge zu Lasten autonomen Alltagshandelns. Der Zugewinn an Komfort und Verkehrssicherheit könnte dann nicht den Verlust an Freiheit und Autonomie rechtfertigen. Einer solchen Entwicklung ist daher durch die Förderung datenschutzfreundlicher Innovationen (Privacy by Design) sowie durch normative Ausgestaltungen entgegenzuwirken."*[283]

„Erlaubte Geschäftsmodelle, die sich die durch automatisiertes und vernetztes Fahren entstehenden, für die Fahrzeugsteuerung erheblichen oder unerheblichen Daten zunutze machen, finden ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer.

---

[278] Ethik–Kommission, S. 10, ethische Regel Nr. 4.

[279] Ethik–Kommission, S. 11, ethische Regel Nr. 6.

[280] BVerfG, Beschluss v. 23.10.2006, –1 BvR 2027/02–,Rn. 33, https://www.bundesverfassungsgericht.de.

[281] BVerfG, Beschluss v. 23.10.2006, –1 BvR 2027/02–,Rn. 61, https://www.bundesverfassungsgericht.de.

[282] Ethik–Kommission, S. 24.

[283] Ethik–Kommission, S. 24.

Fahrzeughalter oder Fahrzeugnutzer entscheiden grundsätzlich über Weitergabe und Verwendung ihrer anfallenden Fahrzeugdaten. Die Freiwilligkeit solcher Datenpreisgabe setzt das Bestehen ernsthafter Alternativen und Praktikabilität voraus. Einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, sollte frühzeitig entgegengewirkt werden."[284]

2.4.1.5.3 Berücksichtigung datenschutzrechtlicher Vorgaben in der Typengenehmigung

Neben der Frage der Verhältnismäßigkeit der Pflichteinführung als solcher stellt sich die Frage, ob in einem zweiten Schritt bei der Pflichteinführung datenintensiver Technologien datenschutzrechtliche Vorgaben jedenfalls bereits bei der Typengenehmigung berücksichtigt werden müssen. Insofern kann auf die Ausführungen zur Schaffung bereichsspezifischer Regelungen verwiesen werden.

Die Ethik-Kommission stellt, wie bereits dargestellt, fest, dass es als Ausdruck seiner Autonomie dem eigenverantwortlichen Menschen freistehen müsse, technische Möglichkeiten wahrzunehmen. Die Bundesregierung zieht daraus in einem kürzlich veröffentlichten Maßnahmenplan die Konsequenz, dass Niemand zur Nutzung automatisierter Fahrsysteme gezwungen werden dürfe. [285] Die Förderung datenschutzfreundlicher Innovationen (Privacy by Design) sowie normative Ausgestaltungen sollen das sicherstellen.[286]

Es liegt ein unauflösbarer Wertungswiderspruch nahe, wenn sich die Bundesregierung auf der einen Seite klar dazu bekennt, das die Zulassung autonomer Systeme entscheidend von der datenschutzfreundlichen Gestaltung by Design abhängt, andererseits aber auf EU-Ebene über das Zulassungsrecht eine Pflichteinführung ohne jede Vorgabe zur datenschutzrechtlichen Gestaltung erfolgt.

Auch aus Verbraucherschutzaspekten sollten datenschutzrechtliche Vorgaben in der Typengenehmigung berücksichtigt werden. So hat das OLG Nürnberg bei der Frage, ob ein Fahrzeug wegen mangelhafter Software zurückgegeben werden kann, entscheidend darauf abgestellt, ob dies die Typenzulassung beeinträchtigt.[287] Hintergrund ist, dass Gewährleistungsrechte von dem Vorliegen eines Mangels abhängen. Ein Mangel setzt wiederum voraus, dass der bestimmungsgemäße Gebrauch der Sache nicht nur unerheblich beeinträchtigt ist. Fehlen datenschutzrechtliche Vorgaben in der Typengenehmigung, müssten die Käufer insofern mit großen Rechtsunsicherheiten

[284] Ethik–Kommission, S. 12, ethische Regel Nr. 15.

[285] BMVI, Maßnahmenplan Ethik-Kommission, S. 2 f.

[286] Bericht der Ethik–Kommission, S. 24.

[287] OLG Nürnberg, Urteil vom 24.4.2018, – 6 U 409/17–, NZV 2018, 315 ff.

leben. Dieses Ergebnis ist mit der Wichtigkeit einer datenschutzfördernden Gestaltung, die wesentlich ist für die ethische Verantwortbarkeit der Zulassung autonomer Systeme, nicht vereinbar. Damit bedarf es datenschutzrechtlicher Vorgaben bei der Typengenehmigung aus Gründen der Rechtssicherheit im Hinblick auf zivilrechtliche Gewährleistungs- oder Produkthaftungsansprüche.

2.4.1.6 Besondere Kategorien personenbezogener Daten

Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Besonderen Kategorien sind solche Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten oder biometrischen Daten zur eindeutigen Identifizierung oder von Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Damit wird dem aus dem Grundrecht auf Nichtdiskriminierung folgenden besonderen Schutzbedarf, insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung oder der Staatsangehörigkeit in Art. 21 GRCh Rechnung getragen.

Ausnahmen von diesem Verbot sind nur unter den strengen Voraussetzungen in Art. 9 Abs. 2 DSGVO möglich.

2.4.2 Grundsatz der Fairness (Treu und Glauben)

Der zweite in Art. 5 Abs 1 lit. a DSGVO genannte Grundsatz verlangt, dass auch die Verarbeitung personenbezogener Daten, die auf einer Rechtsgrundlage beruhen, das Gebot der Fairness beachten müssen. Daher kann auch eine formal rechtmäßige Datenverarbeitung als rechtswidrig zu qualifizieren sein, wenn sie unfair ist, indem beispielsweise Vertrauen missbraucht wird.[288] Der Grundsatz ist insbesondere im Zusammenhang mit den anderen Varianten des Art. 5 Abs. 1 lit. a DSGVO zu sehen. So kann eine Verarbeitung nach dem Wortlaut des Art. 6 Abs. 1 DSGVO zwar auch auf mehrere Rechtsgrundlagen gestützt werden. Dabei müssen aber Transparenz sowie Treu und Glauben beachtet werden. So muss die betroffene Person erkennen können, wenn noch eine andere Rechtsgrundlage greift, da sich dadurch auch ihre Rechte ändern können. Widersprüchliches Verhalten wäre es, wenn eine Einwilligung eingeholt wird,

[288] Roßnagel, ZD 2018, 339 (340).

und für den Fall der Unwirksamkeit auf einen gesetzlichen Erlaubnistatbestand zurückgegriffen werden soll.[289]

2.4.3 Transparenzgrundsatz

Die Verarbeitung muss schließlich nach dem dritten in Art. 5 Abs. 1 lit. a DSGVO genannten Verarbeitungsgrundsatz *„in einer für die betroffene Person nachvollziehbaren Weise erfolgen*." Der Grundsatz der Transparenz umfasst alle Informationen und Informationsmaßnahmen, die erforderlich sind, damit die betroffene Person die Rechtmäßigkeit der Verarbeitung überprüfen und ihre Rechte wahrnehmen kann.[290] Dieser Grundsatz ist nun in der DSGVO ausdrücklich normiert.

Der Grundsatz verlangt, dass die betroffene Person Verständnis darüber erlangen kann, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang diese verarbeitet und künftig noch verarbeitet werden.[291] Er umfasst insbesondere die Pflicht, alle Informationen und Mitteilungen an die betroffene Person leicht zugänglich und verständlich und in klarer und einfacher Sprache bereitzustellen.[292]Das betrifft insbesondere die Informationen über die Identität des Verantwortlichen, die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung für die betroffene Person gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten.[293] Ferner müssen die betroffenen Personen über die Risiken, Vorschriften, Garantien und Rechte informiert und darüber aufgeklärt werden, wie sie diese Rechte geltend machen können.[294]

Der Grundsatz der Transparenz ist in den Informations- und Auskunftsrechten der Artt. 12 ff. DSGVO weiter ausdifferenziert.

2.4.4 Zweckbindung

Personenbezogene Daten dürfen gemäß Art. 5 Abs. 1 lit. b DSGVO nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Der Verantwortliche muss die Zwecke der Verarbeitung bei der Erhebung eindeutig festlegen und ist an diese Zwecke

---

289 Kühling/ Buchner – *Buchner/ Kühling,* DSGVO, Art. 7, Rn. 5 ff.

290 BVerfGE 65, 1 (46, 59); Roßnagel, ZD 2018, 339 (340).

291 ErwG 39 S. 2 DSGVO.

292 ErwG 39 S.3 DSGVO.

293 ErwG 39 S. 4 DSGVO.

294 ErwG 39 S.5 DSGVO.

gebunden. [295] Der Grundsatz der Zweckbindung ist Kernelement des verfassungsrechtlichen Datenschutzes[296] und notwendige Voraussetzung für die Prüfung der weiteren Zulässigkeit der Verarbeitung. Ohne die Zweckfestlegung kann die Zulässigkeit der Verarbeitung nicht beurteilt werden, nicht zuletzt weil die gesetzlichen Erlaubnisvoraussetzungen je nach zulässigem Zweck unterschiedlich ausgestaltet sind. Die Einhaltung der gesetzlichen Vorgaben im Sinne des gebotenen wirksamen Grundrechtsschutzes wäre nicht gewährleistet, wenn der rechtfertigende Zweck erst im Nachhinein alternativ bestimmt werden könnte.[297]

Ein besonderes Problem stellt der derzeit ungeregelte Zugang zu den Fahrzeugdaten dar. Das Interesse an den Fahrzeugdaten ist immens und geht von Werbeagenturen über Automobilherstellern bis zu Versicherungsgesellschaften. Die Artikel 29-Datenschutzgruppe betont zu Recht die mit einem ungeregelten Zugang einhergehenden Gefahren der missbräuchlichen Ansammlung individueller Bewegungsprofile und der „Datifizierung“ von Fahrverhalten, die nicht nur zur Beeinflussung von Konsumverhalten dienen können, sondern auch einem über den Zweck des automatisierten Fahrens hinausgehenden Zweck der Verfolgung von Straftaten und Verkehrsvergehen. [298] Damit steht die Erforderlichkeit und Verhältnismäßigkeit der potentiellen Nutzung der Daten für andere Zwecke in Frage.[299] Die Zweckbindung führt dazu, dass bei der Verfolgung weiterer Zwecke, beispielweise zum Machine Learning zur Fortentwicklung automatisierter Fahrzeuge, eine von der ursprünglich verfolgten Zweckverarbeitung eigenständige Verarbeitung stattfindet, bei der die Vorgaben der DSGVO zu beachten sind.[300]

In engen Ausnahmen kann eine unter Umständen mit dem ursprünglichen Zweck vereinbare Weiterverarbeitung zu statistischen Zwecken gemäß Art. 5 Abs. 1 lit. b, Art. 89 Abs. 1 DSGVO vorliegen. Sie darf aber nicht zu Entscheidungen gegenüber einzelnen Personen verwendet werden und es dürfen keine personenbezogenen Daten sein, vgl. Art. 6 Abs. 4, ErwG 162 a.E. DSGVO. Aufgrund des bereits dargelegten hohen Identifizierungsrisikos unterfallen Fahrzeugdaten ohne gebührende Schutzmaßnahmen nicht dieser Ausnahme.

---

[295] ErwG 39 S. 6 DSGVO.

[296] BVerfGE 65, 1ff, Rn. 185, (openjur).

[297] OLG Köln, Urteil vom 30.09.2016, - 20 U 83/16 -, Rn. 69.

[298] Artikel 29-Datenschutzgruppe, WP 252, S. 10.

[299] Artikel 29-Datenschutzgruppe, WP 252, S. 10.

[300] Vgl. IWGDP, vernetzte Fahrzeuge, S. 13

2.4.5 Datenminimierung

Die Datenverarbeitung muss gemäß Art. 5 Abs. 1 lit. c DSGVO *„dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein*“. Der Grundsatz drückt damit die nach Artt. 8 Abs. 2, 52 GRCh gebotene Verhältnismäßigkeitsforderung aus, aus der sich auch der Grundsatz der Nichtverkettung ableiten lässt. Der Grundsatz der Datenminimierung konkretisiert den Grundsatz der Erforderlichkeit, wonach die personenbezogenen Daten als Mittel zur Zweckerreichung unbedingt notwendig sein müssen.[301] Das ist nicht der Fall, wenn schonendere Mittel zur Zweckerreichung zur Verfügung stehen. Ferner trägt die Rechtsgrundlage nur die für ihre Zwecke unbedingt notwendigen Verarbeitungstätigkeiten.

Eine besondere Herausforderung stellt die Gefahr der zweckü̈berdehnenden Sammlung von Fahrzeugdaten aufgrund der durch die zahlreichen Sensoren generierten Echtzeitdaten dar. Bereits die Gestaltung der Datenerhebung durch die Fahrzeugsysteme selbst muss daher dem Grundsatz der datenschutzfreundlichen Systemgestaltung aus Art. 25 DSGVO zur Durchsetzung der Zweckbindung und Datenminimierung entsprechen.[302]

2.4.6 Richtigkeit

Die verarbeiteten personenbezogenen Daten müssen gemäß Art. 5 Abs. 1 lit. d DSGVO „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.“ Die geforderte Datenqualität betrifft solche durch die Daten vermittelten Informationen, die sich auf Tatsachenangaben beziehen und folglich einem empirischen Beweis zugänglich sind.[303] Unrichtige Daten müssen im Rahmen des Vertretbaren gelöscht oder berichtigt werden.[304]

2.4.7 Speicherbegrenzung

Personenbezogene Daten müssen zudem gemäß Art. 5 Abs. 1 lit. e DSGVO *„in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur solange ermöglicht, wie es für die Zwecke, für die sie verarbeitet wurden, erforderlich ist*.“ Ist der Zweck erreicht oder ist der Zweck auch ohne Personenbezug erreichbar, sind die personenbezogenen Daten zu löschen.[305] Die Speicherfrist muss auf das unbedingt

[301] Roßnagel, ZD 2018, 339 (341).

[302] IWGDPT, vernetzte Fahrzeuge, S. 9.

[303] Roßnagel, ZD 2018, 339 (341).

[304] ErwG 39 S. 11 DSGVO.

[305] ErwG 39 S. 9 DSGVO.

erforderliche Mindestmaß beschränkt bleiben und erfordert Löschfristen oder regelmäßige Überprüfungen.[306]

2.4.8 Integrität und Vertraulichkeit

Nach Art. 5 Abs. 1 lit. f DSGVO dürfen personenbezogene Daten nur *„in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch technische und organisatorische Maßnahmen*“. Der Grundsatz zielt damit auf einen umfassenden Systemdatenschutz und schließt Zugangs- und Zugriffsschutz mit ein.[307]

2.5 Transparente Information und Kommunikation mit betroffenen Personen

Die DSGVO stellt gegenüber der alten Rechtslage erhöhte Anforderungen an die Transparenz der Verarbeitung, vgl. Art. 5 Abs. 1 lit. a, Artt. 12, 13, 14, ErwG 39, 60, 61 DSGVO. Als Ausprägung des Transparenzgrundsatzes treffen den Verantwortlichen in den Artt. 13 ff. DSGVO Informations- und Auskunftspflichten. Die betroffene Person muss dabei in einer Art und Weise über die Existenz der Verarbeitungsvorgänge, die damit verbundenen Gefahren für ihre Privatsphäre und ihre Einwirkungsmöglichkeiten informiert werden, die es ihr ermöglicht, auch tatsächlich Verständnis und Problembewusstsein zu entwickeln.

Der Verantwortliche ist nach Art. 5 Abs. 1 lit. a Var. 3, Art. 12 Abs. 1 DSGVO verpflichtet, alle ihm nach Artt. 13, 14 DSGVO obliegenden Informations- und Auskunftspflichten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, besonders wenn Kinder betroffen sind.

Eine bestimmte Form ist nicht vorgeschrieben, sondern richtet sich nach den Umständen, wobei der Verantwortliche gemäß Artt. 12 Abs. 1, 24 Abs. 1 DSGVO nachweispflichtig ist. Die Form der Darstellung muss aber leicht wahrnehmbar, verständlich und klar nachvollziehbar sein.

Nach Art. 12 Abs. 7, ErwG 60 DSGVO besteht die Möglichkeit der Kombination mit standardisierten Bildsymbolen, um einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Die Informationen können in elektronischer Form bereitgestellt werden.[308] Die elektronische Form muss maschinenlesbar sein.[309]

---

[306] ErwG 39 S. 8, S. 10 DSGVO.

[307] Roßnagel, ZD 2018, 339 (341).

[308] ErwG 58 S.1, S. 2 DSGVO.

2.5.1 Betroffene Personen

Die Transparenzpflichten sind gegenüber jeder betroffenen Personen zu erfüllen. Von der Verarbeitung der Fahrzeugdaten können insoweit unterschiedliche Personen betroffen sein. Der Personenbezug der Fahrzeugdaten liegt zunächst nicht nur in Bezug auf den Halter, sondern auch in Bezug auf jeden Fahrzeugnutzer, wie den Fahrer und die weiteren Fahrzeuginsassen vor.[310] Damit können auch Mitfahrer wie Familienmitglieder, Freunde oder sonstige Dritte von der Datenverarbeitung betroffen sein, wenn Rückschlüsse auf ihre Person möglich sind.

Es existieren zahlreiche rechtliche Möglichkeiten, sowohl den Fahrer, als auch Mitfahrer zu ermitteln, beispielsweise über Halterfeststellungen, Auskünfte der Mobilfunkanbieter oder Zeugenvernehmungen in Straf-, Bußgeld- oder Zivilverfahren. So könnten der Fahrer oder sonstige Zeugen auch die Identität von Beifahrern offenlegen.

Auch lässt sich aus den Wegstrecken auf Mitfahrer schließen, z.B. Umwege auf dem Arbeitsweg zur Schule, dem Kindergarten oder der Privatadresse von anderen Mitarbeitern. Hat ein Mitfahrer beim selben Dienstanbieter einen Vertrag, sind dessen Adressdaten bekannt und es besteht eine weitere Verknüpfungsmöglichkeit.

Daneben können weitere Sensoren im Fahrzeuginnenraum sowie Video- und/oder Tonaufnahmen des Innenraums eine Identifikation der Mitfahrer ermöglichen.

2.5.2 Elektronische Bereitstellung über das HMI/Infotainmentsystem

Die Informationen sollen unter anderem dann elektronisch bereitgestellt werden, wenn die große Zahl der Beteiligten und die Komplexität der Technologien es der jeweils betroffenen Person schwer machen, die Verarbeitung zu erkennen und nachzuvollziehen.[311] Im Kontext vernetzter und automatisierter Fahrzeuge, bei denen unterschiedliche Mobilitätsdienste auf die Fahrzeugdaten zugreifen möchten, muss der Verantwortliche geeignete Maßnahmen zur Gewährleistung der transparenten Information und Kommunikation ergreifen. So können über die HMI/Infotainment-Systeme mehrschichtige, erweiterte Informationsangebote angeboten werden, die Informationen gebündelt und leicht auffindbar darstellen und visualisieren und ein nutzerbezogenes Privatsphärenmanagement ermöglichen.[312]

---

[309] ErwG 60 DSGVO.

[310] BVerfG, Urteil v. 11.03. 2008,– 1 BvR 2074/05, 1 BvR 1254/07–, NJW 2008, 1505 (1507 f.), Rn.72, Rn. 86; OVG Münster, Urt. v. 19.10.2017,–16 A 770/17–, NVwZ 2018, S. 742 ff (744).

[311] ErwG 58 DSGVO.

[312] Weiterführend: Artikel 29-Datenschutzgruppe, WP 260 rev.01

2.5.3 Informationspflichten

Den Verantwortlichen treffen Informationspflichten gegenüber der betroffenen Person. Art. 13 DSGVO regelt die Informationspflichten, wenn die personenbezogenen Daten direkt bei der betroffenen Person erhoben werden. Art. 14 DSGVO ist hingegen anwendbar, wenn die Informationen aus anderen Quellen nicht direkt bei der betroffenen Person erhoben werden.

Bei der Erhebung bei der betroffenen Person müssen gemäß Art. 13 Abs. 1 DSGVO die Informationen auch zum Zeitpunkt der Erhebung gegeben werden.[313] Der Zeitpunkt gilt gemäß Art. 13 Abs. auch bei der rechtmäßigen Offenlegung gegenüber Dritten. Bei einer beabsichtigten Weiterverarbeitung für andere Zwecke muss die betroffene Person vorher unterrichtet werden.[314] Die Unterrichtung der betroffenen Person bei der Erhebung aus anderen Quellen verlangt gemäß Art. 14 Abs. 1 DSGVO eine nach den Umständen des Einzelfalls angemessene Frist und kann im Einzelfall die Information bereits bei der Erhebung erforderlich machen.[315]

Die wesentlichen Informationen umfassen die Unterrichtung über die Existenz des Verarbeitungsvorgangs, die Zwecke der Verarbeitung, die Essentia der Artt. 12 ff. DSGVO, die Betroffenenrechte, sowie alle weiteren für eine faire und transparente Verarbeitung im Einzelfall erforderlichen Informationen.[316] Im Einzelfall erforderliche Informationen umfassen Informationen über ein erfolgendes Profiling und dessen Folgen[317], bestehende Widerspruchsrechte nach Art. 21 Abs. 1, Abs. 4 DSGVO bzw. Widerrufsmöglichkeiten nach Art. 7 Abs. 4 DSGVO, das Bestehen einer automatisierten Entscheidungsfindung und aussagekräftige Informationen über die involvierte Logik, ihre Tragweite und ihre Auswirkungen nach Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g DSGVO sowie bestehende Interventionsrechte nach Art. 22 Abs. 3 DSGVO. Zu dem genauem Umfang der Auskunftspflicht über die involvierte Logik ist bereits seit dem Jahr 2014 noch unter Geltung der Datenschutzrichtlinie 95/46/EG eine Verfassungsbeschwerde beim BVerfG anhängig.[318]

Insoweit ist eine Information auf einem beim Fahrzeugkauf mitübergebenen Datenschutzblatt nur dann ausreichend, wenn nicht die besonders unübersichtliche Zahl der Datenverarbeitungsvorgänge eine zeitgerechtere Information erfordert.

---

[313] ErwG 61 DSGVO.

[314] ErwG 61 DSGVO.

[315] ErwG 61 S. 3 DSGVO.

[316] ErwG 61 DSGVO.

[317] ErwG 60 DSGVO.

[318] Vgl. BVerfG - 1 BvR 756/14 (anhängig).

Informationen werden möglicherweise nur an den Fahrzeughalter weitergegeben und nicht zum richtigen Zeitpunkt, sondern nur bei Kauf bzw. Übergabe. Den Default-Einstellungen kommt insoweit eine wichtige Bedeutung zu, um gegenüber den weiteren Fahrzeugnutzern eine unrechtmäßige Datenerhebung zu verhindern. Bei einer Umsetzung im Fahrzeug beispielweise über die Borddokumentation ist darauf zu achten, dass die Informationen nicht zur Unzeit gegeben werden und dadurch eine Ablenkung von der Fahraufgabe stattfindet.

Aktuell stellt sich die Frage, ob bei den komplexen, für den Nutzer oftmals verborgenen Datenverarbeitungsvorgängen im vernetzten Fahrzeug dem Nutzer die aktuell stattfindende Datenverarbeitung überhaupt bewusst ist. Mögliche Gründe für Zweifel können darin begründet liegen, dass die Information lange zurückliegt, sie dem Nutzer kein echtes Verständnis über Art, Umfang und Zwecke der Verarbeitung vermittelt hat, z.B. durch intransparente Datenschutzerklärungen (zu lange Texte, unpräzise und juristische Formulierungen und damit nicht adressatengerecht) oder weil die Information nur dem Vornutzer oder Fahrzeugeigentümer erteilt wurde. Besonders hohe Anforderungen gelten bei erhöhter Schutzwürdigkeit beispielsweise gegenüber älteren Menschen, Kindern, Arbeitnehmern, Leasingnehmern oder Mietern.

2.5.4 Heimliche Datenabflüsse an die Hersteller

Im Kontext vernetzter Fahrzeuge ist entgegen dieser Vorgaben zu beobachten, dass vielfach die Hersteller, je nach Hersteller und Modellreihe in unterschiedlichem Umfang über die Default-Einstellungen Daten erheben ohne dass – abgesehen von der fehlenden Rechtsgrundlage – eine Information der betroffenen Personen über die Datenerhebung und die anschließende Verwendung erfolgt.[319] Eine strafgerichtliche Entscheidung des Landgerichts Köln[320] offenbart die Brisanz dieser Problematik: Der Hersteller eines Fahrerassistenzsystems mit Telematik-Einheit erhielt ohne Kenntnis der betroffenen Personen automatisierte Datenrückflüsse, die nicht der Fahrsicherheit zuzurechnen waren und die erst durch eine staatsanwaltliche Beschlagnahme im Strafverfahren offengelegt wurde.[321]

Heimliche Datenerhebungen sind besonders eingriffsintensiv, da den betroffenen Personen zugleich die Möglichkeit, ihre Rechte geltend zu machen, von vornherein unmöglich gemacht wird. Den Gesetzgeber treffen insoweit besondere Schutz- und

[319] Nürnberger, DuD 2018, 79 ff.; Weichert NZV 2017, 507 (508).

[320] LG Köln, Urteil v. 23.5.2016, -113 KLs 34/15-, Rn. 80, 86 ff, juris.

[321] Vgl. zur zunehmenden Relevanz der Fahrzeugdaten im Ermittlungsverfahren: LG Berlin, Urteil v. 27.2.2017, -(535 Ks) 251 Js 52/16 (8/16); LG Köln, Urteil v. 23.5.2016, -113 KLs 34/15-; LG Köln, Urteil v. 14.4.2016 -117 KLs 19/15-. AG Emmendingen, Urteil v. 3.11.2014, -5 Cs 500 Js 21795/13-.

Beobachtungspflichten, die ihn dazu verpflichten, einen angemessenen Schutz für die Grundrechte herzustellen, der auch wirksam ist.[322] Insbesondere sind die staatlichen Organe verpflichtet, *„dem Einzelnen Schutz davor zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf die seine Individualität kennzeichnenden Daten nehmen. Dies gilt grundsätzlich selbst dann, wenn der Zweck […] von einem grundrechtlich geschützten Kenntnisinteresse getragen wird. Die in solchen Fällen vorliegende Grundrechtskollision kann nicht von einem der Grundrechtsträger nach seinem Gutdünken bewältigt, sondern nur durch den Gesetzgeber gelöst werden.“*[323]

Betroffene Personen müssen im Kontext vernetzter Fahrzeuge in die Lage versetzte werden, ihre Rechte auszuüben und jederzeit die Kontrollmöglichkeit über ihre Daten innehaben. Andernfalls drohen Sanktionen und der Vertrauensverlust der Nutzer. Der Gesetzgeber und die staatlichen Organe sind zudem bei dem Anhalten dieser Entwicklung zu weitgehenderen und empfindlicheren Regulierungsmaßnahmen gehalten.

2.6 Modalitäten für die Ausübung der Betroffenenrechte

Die betroffene Person hat nach den Artt. 15 ff DSGVO weitere Rechte gegen den Verantwortlichen, mit denen sie Einfluss auf die Verarbeitung der auf sie bezogenen oder beziehbaren Informationen nehmen kann.

Der Verantwortliche ist nach Art. 12 Abs. 3 DSGVO verpflichtet, der betroffenen Person die Ausübung ihrer Rechte zu erleichtern. Auf Anträge muss er unverzüglich, was im deutschen Recht ohne schuldhaftes Zögern bedeutet, spätestens aber innerhalb eines Monats Informationen über die ergriffenen Maßnahmen zur Verfügung stellen. Dabei gilt die Pflicht zur transparenten Kommunikation aus Art.12 Abs. 1 DSGVO.

2.6.1 Auskunftsrechte

Die betroffene Person hat gemäß Art. 15 DSGVO das Recht, zunächst eine Bestätigung darüber zu erhalten, ob sie betreffende Daten verarbeitet werden. Ist das der Fall, hat sie einen Anspruch auf Auskunft über die zu ihrer Person gespeicherten Daten und die in Art. 15 Abs. 1 lit. a -lit. h, Abs. 2 DSGVO genannten Informationen.

Ferner hat die betroffene Person nach Art. 15 Abs. 3 DSGVO grundsätzlich den Anspruch auf Anfertigung einer Kopie, die auch grundsätzlich kostenlos sein muss.

---

[322] BVerfGE 88, 203 ff. (254); BVerfG, Urt. v. 13.02.2007, –1 BvR 421/05– ,Rn. 63;

[323] BVerfG, Urt. v. 13.02.2007, –1 BvR 421/05–, Rn. 67.

2.6.2 Widerspruchs- und Widerrufsrechte

Die betroffene Person hat nach Art. 7 Abs. 3 und Art. 21 DSGVO Widerspruchs- und Widerrufsrechte, wenn die Verarbeitung auf einer Einwilligung oder einer Rechtsgrundlage aus Art. 6 Abs. 1 lit. e oder lit f beruht.

Nach Art. 21 Abs. 5 DSGVO kann die betroffene Person bei Diensten der Informationsgesellschaft auch ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden. Denkbar ist beispielsweise ein standardisiertes Datenformat, welches gestattet, Widerspruch aber auch Einwilligungen und deren Widerruf elektronisch zu kommunizieren.[324]

Nach Art. 7 Abs. 3 DSGVO muss der Widerruf der Einwilligung so einfach sein wie die Erteilung der Einwilligung.

Mobilitätsdienste, die auf diesen Rechtsgrundlagen beruhen, sollten daher bei fehlendem Bezug zu Fahrsicherheitsfunktionen einfach deaktivierbar sein, etwa über einen Schalter im Infotainmentsystem, und zwar unabhängig davon, ob die Verarbeitung lokal im Fahrzeug oder außerhalb auf einem Server erfolgt.

2.6.3 Privilegierung bei wirksamer Pseudonymisierung

Nach Art. 11 DSGVO soll bei einer wirksamen Pseudonymiserung das Risiko nicht dadurch wieder erhöht werden, dass der Verantwortliche lediglich zur Erfüllung seiner Pflichten nach der DSGVO zusätzliche identifizierende Merkmale aufbewahren muss. Der Verantwortliche sollte daher personenbezogene Daten nicht allein zu dem Zweck speichern, um auf mögliche Auskunftsersuchen reagieren zu können.[325] Er muss aber zusätzliche Informationen durch die betroffene Person entgegennehmen, wenn diese ihre Rechte geltend machen will.[326]

Diese Privilegierung soll nicht den Verantwortlichen entlasten, sondern nach dem BVerfG das Identifizierungsrisiko für die betroffene Person minimieren und damit ihrem Schutz dienen: *„Eine Benachrichtigung würde daher erfordern, diesen Personenbezug zu ermitteln, was den Grundrechtseingriff noch vertiefen würde.“*[327] Daraus ergibt sich, dass die Privilegierung nur bei Datenverarbeitungen greift, die den vernünftigen Erwartungen der betroffenen Person entspricht und nicht nach Treu und Glauben ihre Einwilligung oder eine andere Rechtsgrundlage erfordert. Eingriffsintensive Verfahren unterfallen

[324] Vgl. die Bestrebungen der W3C Data Privacy Vocabularies and Controls CG, nähere Informationen abrufbar unter: https://www.w3.org/community/dpvcg/ (letzter Abruf: 20.12.2018).

[325] ErwG 64 S. 2 DSGVO.

[326] ErwG 57 s. 2 DSGVO.

[327] BVerfG, Beschluss v. 22.08.2006, –2 BvR 1345/03–, Rn. 77, juris (m.w.N.).

daher nicht der Privilegierungswirkung, wenn nicht zugleich wirksame Schutzmaßnahmen ergriffen werden, beispielweise wenn für maschinelles Lernen große Datensammlungen auf Vorrat und ohne Zweckbestimmung angelegt werden.[328]

Nur dann, wenn die Pseudonymsierung auch praktisch gem. Art. 4 Nr. 5 DSGVO sichergestellt ist, greift die Ausnahme des Art. 11 DSGVO zugunsten der betroffenen Person ein.

2.6.4 Rechte bei automatisierter Verarbeitung und Profiling

Bei automatisierten Entscheidungen stellt Art. 22 DSGVO ein Verbot von Entscheidungen auf, die ausschließlich auf automatisierter Verarbeitung – einschließlich Profiling – beruhen und die gegenüber der betroffenen Person rechtliche Wirkung entfalten oder sie in anderer Weise erheblich beeinträchtigen. Die betroffene Person hat in diesem Fall das Recht, nicht ausschließlich einer automatischen Entscheidung unterworfen zu werden.

Eine nicht ausschließlich automatische Entscheidung erfordert eine menschliche Intervention. Diese liegt nach dem Sinn und Zweck von Art. 22 DSGVO nur dann vor, wenn eine echte inhaltliche Prüfung erfolgt.[329] Die bloße Rechnungserstellung stellt keine Sachprüfung dar.

Ausnahmsweise darf von diesem Grundsatz gemäß Art. 22 Abs. 2 lit. a Variante 1 DSGVO abgewichen werden, wenn die Entscheidung für die Erfüllung eines Vertrages objektiv erforderlich ist. Nach dem klaren Wortlaut reicht diese Ausnahme nur, soweit die automatisierte Entscheidung zur Vertragsdurchführung erforderlich ist. Hierfür muss ein unmittelbarer Zusammenhang mit der Entscheidungs- und Kalkulationsgrundlage des Vertrages bestehen[330]. Der Verantwortliche muss dann aber ein Verfahren einrichten, dass der betroffenen Person nach Art. 21 Abs. 1 S. 1 DSGVO die Möglichkeit auf Einspruch gegen die Entscheidung einräumt und ihr die Möglichkeit des jederzeitigen Widerrufs nach Art. 14 Abs. 2 lit. c DSGVO mitteilen. Im vertraglichen Kontext bedeutet dies, dass wirksame Möglichkeiten zur Intervention bei der Vertragsdurchführung durch technische und organisatorische Maßnahmen vorgesehen werden müssen.

Enge Ausnahmen[331] bestehen nach Art. 22 Abs. 3 DSGVO bei Erforderlichkeit für den Abschluss oder die Erfüllung eines Vertrages sofern angemessene Schutzmaßnahmen getroffen werden, bei einer speziellen Rechtsvorschrift, die angemessene

---

[328] IWGDPT, vernetzte Fahrzeuge, S. 9, S. 13.

[329] ErwG 71 DSGVO.

[330] Kühling/Buchner-*Buchner,* DS-GVO, Art.22 Rn. 30.

[331] Vgl. Artikel 29-Datenschutzgruppe, WP 251 rev.01

Schutzmaßnahmen enthält oder bei der ausdrücklichen Einwilligung der betroffenen Person sofern angemessene Schutzmaßnahmen getroffen werden. Die Ausnahme greift aber nur, wenn keine Rückausnahme gemäß Art. 22 Abs. 4 i.V.m. Art. 9 Abs. 1 DSGVO eingreift. Danach dürfen ausschließlich auf automatisierter Verarbeitung beruhende Entscheidungen nicht auf besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO beruhen, aus denen Informationen über den besonders geschützten Lebensbereich betroffener Personen hervorgehen, wie zum Beispiel die ethnische Herkunft oder politische Orientierung, sofern keine Ausnahme nach Art. 9 Abs. 2 DSGVO vorliegt. Solche besonderen Kategorien sind besonders sensibel und verdienen einen besonderen Schutz. [332] Dann würde das Verbot aus Art. 22 Abs. 1 DSGVO wieder aufleben.

Diese zusätzlichen Anforderungen müssen neben den allgemeinen Anforderungen der DSGVO zusätzlich erfüllt werden.[333] Im Kontext des vernetzten, automatsierten und kooperativen Fahrens müssen die Dienstanbieter, beispielweise wenn Pay-As-You-Drive-Tarife angeboten werden, diese Vorgaben beachten.

2.6.5 Recht auf Berichtigung

Die betroffene Person hat nach Art. 16 DSGVO das Recht, unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen, wozu auch das Vervollständigen unvollständiger Daten gehört.

2.6.6 Recht auf Löschung

Die betroffene Person hat unter den Voraussetzungen des Art. 17 DSGVO das Recht auf unverzügliche Löschung, beispielsweise der nicht mehr notwendigen Daten.

Fraglich ist, wie die Löschbarkeit der Fahrzeugdaten durch den Fahrzeughersteller realisiert werden wird. Bedenken gegen die datenschutzrechtliche Zulässigkeit von Verarbeitungen bestehen dann, wenn in Herstellerangaben Einschränkungen der Löschbarkeit für solche Daten gemacht werden, die im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sein können. Insofern ist auf die Ausführungen bei der Rechtsgrundlage des berechtigten Interesses zu verweisen.

2.6.7 Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat das Recht, unter den Voraussetzung des Art. 18 DSGVO, die Einschränkung der Verarbeitung zu verlangen.

---

[332] Vgl. ErwG 51 DSGVO.

[333] ErwG 72 DSGVO.

2.6.8 Recht auf Datenübertragbarkeit und Datenzugang

Der neu eingeführte Art. 20 DSGVO soll der betroffenen Person im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine „bessere Kontrolle über die eigenen Daten“ ermöglichen.[334] Das darin festgelegte Recht auf Datenübertragbarkeit begründet einen Anspruch der betroffenen Person gegen den Verantwortlichen, sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt und die Rechtsgrundlage auf einer Einwilligung i.S.d. Art. 6 Abs. 1 lit. a, Art. 7; Art. 9 Abs. 2 lit. a DSGVO oder der Erfüllung eines Vertrages i.S.d. Art. 6 Abs. 1 lit. b DSGVO beruht. Der Anspruch auf Datenübertragbarkeit besteht nach Art. 20 Abs. 2 S. 1 DSGVO nicht, wenn die Verarbeitung auf einer anderen Rechtsgrundlage beruht. Im Kontext vernetzter und automatisierter Fahrzeuge betrifft das beispielweise die gesetzlichen Pflichtdatenspeicher nach der eCall-Verordnung oder nach § 63a StVG.

Das Recht auf Datenübertragbarkeit begründet den Anspruch, dass die von der betroffenen Person bereitgestellten Daten an sie selbst oder einen von ihr benannten Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden. Der Anspruch umfasst auch solche Daten, die allein durch die Nutzung des Dienstes von der betroffenen Person aufgezeichnet werden.[335]

Das Recht auf Datenübertragbarkeit korrespondiert gem. Art. 20 Abs. 2 S. 2 DSGVO nicht notwendigerweise mit dem Recht auf Löschung, wenn die Daten nach der Rechtsgrundlage noch benötigt werden.[336] Das Recht auf Datenübertragbarkeit kann im Umkehrschluss unabhängig vom Recht auf Löschung gesondert geltend gemacht werden.

2.6.8.1 Entgegenstehende Rechte und Freiheiten anderer Personen

Dem Anspruch können nach Art. 20 Abs. 4 DSGVO die Rechte und Freiheiten anderer Personen entgegenstehen. Der Verordnungsgeber stellt in der Begründung der Norm auf solche Fälle ab, bei denen im Fall eines bestimmten Datensatzes mehr als eine betroffene Person tangiert wird.[337] Das sind vor allem die Persönlichkeitsrechte von Mitbetroffenen, wie Fahrzeuginsassen, Personen aus dem Fahrzeugumfeld oder auch der Fahrer gegenüber dem personenverschiedenen Halter. Soweit dem Anspruch Geschäftsgeheimnisse oder Urheberrechte an der Software entgegengehalten werden[338], ist zu beachten, dass dies nicht dazu führen darf, dass jegliche Auskunft

[334] ErwG 68 S. 1 DSGVO.

[335] Artikel 29-Datenschutzgruppe, WP 242 rev.01, S. 11.

[336] ErwG 68 S. 8 DSGVO.

[337] ErwG 68 S. 8 DSGVO.

[338] Klink-Straub/ Straub, ZD 2018,459 (462 m.w.N.).

verweigert werden darf.[339] Geschäftsgeheimnis und Personenbezug stehen zudem in einem Exklusivitätsverhältnis, da personenbezogene Daten keinen kommerzialisierbaren Unternehmenswert [340] darstellen. Die Einschränkung aufgrund von Geschäftsgeheimnissen dürfte sich daher – wie bereits bei Art. 15 Abs. 1 lit. h DSGVO – auf die Frage beschränken, wie detailliert bei einer automatisierten Entscheidungsfindung einschließlich Profiling aussagekräftige Informationen über die involvierte Logik mitgeteilt werden müssen.

2.6.8.2 Gewährleistung des Datenzugangs

Fraglich ist, wie der Datenzugang für die betroffenen Personen gewährleistet werden wird. Der bislang gesetzlich ungeregelte Zugang zu den Fahrzeugdaten birgt aufgrund der zahlreichen Interessen an den Fahrzeugdaten, die von Werbeagenturen über Automobilhersteller bis zu Versicherungsgesellschaften reichen, ein datenschutzrechtlich hohes Risiko für die Grundrechte der betroffenen Personen.

Die Frage des Datenzugangs ist darüber hinaus bislang von Diskussionen um die Schaffung eines Dateneigentums überlagert worden.

2.6.8.2.1 Dateneigentum

Die mit dem Datenzugang eng verbundene Diskussion um die Schaffung eines Dateneigentums dürfte spätestens seit dem Bericht der Ethik-Kommission zugunsten der Grundrechte der betroffenen Personen beendet sein.[341] Die Ethik-Kommission hat Leitlinien erarbeitet, die den in den Grundrechten zum Ausdruck kommenden äußeren Rahmen unserer Rechtsordnung auf den automatisierten und vernetzten Verkehr angewendet hat. Danach ist ein veräußerliches Dateneigentum mit den Grundrechten nicht vereinbar und würde letztlich zu der grundrechtswidrigen Situation führen, in der der einzelne Bürger nicht mehr weiß oder erkennen kann, wer was wann und bei welcher Gelegenheit über ihn weiß.

2.6.8.2.2 Datenzugang im Fahrzeug selbst oder auf einer neutralen Plattform

Der Datenzugang zu den Fahrzeugdaten kann sowohl im Fahrzeug selbst, als auch außerhalb des Fahrzeugs auf einer Plattform realisiert werden.[342] Zum Teil wird angeführt, dass Argumente der Datensicherheit sowie Datenschutzgründe es erforderlich machen würden, dass die im Fahrzeug generierten und für

---

[339] Vgl. den Rechtsgedanken in ErwG 63 S. 5 f. DSGVO.

[340] Vgl. Goldhammer, NVwZ 2017, 1809 (1812).

[341] Ausführlich: Ethik-Kommission, S. 12, ethische Regel Nr. 15.

[342] Zu den bisherigen Zugangskonzepten und Analysen vgl. Europäische Kommission, Access to in-vehicle data.

Mobilitätsdienste benötigten Daten zunächst über eine verwaltete Schnittstelle zu den Backendservern des jeweiligen Automobilherstellers fließen, der insofern die Rolle eines Systemadministrators für diese Schnittstelle einnehmen solle, um die Daten aufzubereiten und an einen neutralen Server weiter zu verteilen.[343]

Dieser Ansicht ist entgegenzuhalten, dass die Rolle eines Systemadministrators mit erweiterten Zugriffsbefugnissen und Rechten funktional einer treuhänderischen Position gleichkommt, der damit zugleich die Rolle eines Gatekeepers einnimmt. Diese Rolle kann nur von einem Akteur ausgefüllt werden, der die geeignete Neutralität aufweist und bei dem keine Interessenskollisionen drohen. Zwischen dem Automobilhersteller und dem Fahrzeugnutzer besteht aber ein solcher Interessenskonflikt, da der OEM keine neutrale Instanz ist, sondern erhebliches Eigeninteresse an den generierten Daten hat. Er bietet eigene Services/Zusatzdienste an und ist damit zugleich potentieller Datenabnehmer. Im Streitfall haftet er darüber hinaus nach der Produzentenhaftung auf der Anspruchsgegenseite und möchte seine entgegengesetzten Interessen durchsetzen. Die Missbrauchsgefahr ist dadurch sehr hoch.

Der Datenzugang könnte auch orientiert am Vorbild des Messstellenbetriebsgesetzes (MsbG) umgesetzt werden, bei dem ein sternförmiges Kommunikationsmodell gesetzlich vorgegeben wurde. Ein solches Modell entspricht den Grundsätzen der Datenminimierung sowie der Zweckbindung und der Nichtverkettung, verhindert wirksam Datenschutzvorfälle i.S.d. Art. 33 f. DSGVO, da eine zentrale Datensammlung außerhalb des Fahrzeugs vermieden wird, und gewährleistet das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Zur Verwaltung der Schnittstelle sollte zudem eine nachweisbar vertrauenswürdige und sachkundige Instanz als Systemadministrator ausgewählt werden.

Wird der Datenzugang im Fahrzeug realisiert, kommt dem HMI/Infotainment-System eine wichtige Funktion zu. Hybride Endgeräte ermöglichen es, lineare und nichtlineare Inhalte, Broadcast- und Internetmedien auf einem Endgerät darzustellen, die damit um denselben Platz auf dem Bildschirm konkurrieren. Die Konzeption des Endgeräts spielt daher eine große Rolle, denn je nach Menüführung oder Gestaltung der Benutzeroberfläche kann die Nachfrage gelenkt werden. Das Recht auf Datenübertragbarkeit muss so umgesetzt werden, dass Lock-In-Effekte verhindert werden Ferner dürfen betroffenen Personen nicht durch eine komplizierte Menüführung die Ausübung ihrer Rechte erschwert werden.[344]

---

[343] Die Schnittstellen zwischen mobilen Kommunikationsgeräten und Fahrzeug sowie die Car2X–Kommunikation sollen davon unberührt bleiben, ebenso wie Reparatur- und Wartungsmaßnahmen über die OBD–2 Diagnoseschnittstelle, vgl. VDA, Zugang; VDA, Konzept NEVADA.

[344] Ausführlich: Weichert, SVR 2014, 241 (243).

Die Betroffenenrechte, wie das Recht auf jederzeitigen Widerruf in Art. 7 Abs. 3 DSGVO oder Widerspruch nach Art. 21 DSGVO erfordern auch eine Waffengleichheit äquivalent zur Verarbeitungssituation: Werden große Datenmengen vollautomatisiert verarbeitet, muss auch in diesen Vorgang technisch eingegriffen werden können. Denkbar wäre beispielsweise ein Aus-Schalter im Fahrzeug.

2.7 Datenschutzfreundliche Technikgestaltung und datenschutzfreundliche Voreinstellungen

Der Verantwortliche muss gemäß Art. 25 Abs. 1 DSGVO sowohl zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der eigentlichen Verarbeitung die Pflicht zur datenschutzfreundlichen Technikgestaltung „by Design“ durch Implementierung geeigneter technischer und organisatorischer Maßnahmen nachweisen können. Diese müssen darauf ausgelegt sein, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und Garantien enthalten, um der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen.

Ferner muss der Verantwortliche nach Art. 25 Abs. 2 DSGVO gewährleisten, dass durch datenschutzfreundliche Voreinstellungen „by Default“ nur diejenigen personenbezogenen Daten verarbeitet werden, die hinsichtlich der Menge, des Verarbeitungsumfangs, der Speicherfrist und der Zugänglichkeit für den bestimmten Verarbeitungszweck erforderlich sind.

Der Verantwortliche muss sowohl interne Strategien festlegen als auch geeignete technische und organisatorische Maßnahmen ergreifen, die den Grundsätzen von „Data Protection by Design“ und „Data Protection by Default“ genügen.[345] Solche Maßnahmen können sein: [346]

- Die Verarbeitung personenbezogener Daten wird minimiert.
- Personenbezogene Daten werden so schnell wie möglich pseudonymisiert.
- Transparenz wird in Bezug auf die Funktionen und die Verarbeitung hergestellt.
- Der betroffenen Person wird ermöglicht, die Verarbeitung zu überwachen.
- Der Verantwortliche wird in die Lage versetzt, Sicherheitsfunktionen zu schaffen und zu verbessern.

Der Verantwortliche ist dabei verpflichtet, nur solche Verarbeitungsmittel auszuwählen und einzusetzen, die datenschutzkonform betrieben werden können. Die Fahrzeughersteller sollten daher das Recht auf Datenschutz bereits bei der Produktion

[345] ErwG 78 S. 2 DSGVO.

[346] ErwG 78 S. 3 DSGVO.

gebührend berücksichtigen.[347] Insbesondere bei öffentlichen Ausschreibungen oder bei Firmenflotten können ihre Produkte andernfalls nicht berücksichtigt werden.[348]

2.8 Gewährleistung der Sicherheit der Verarbeitung

Der Verantwortliche muss auch technische und organisatorische Maßnahmen zur Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit umsetzen. Dabei gilt, wie zuvor, eine Abwägung unter Berücksichtigung des Risikos der Verarbeitung, des Stands der Technik, der Implementierungskosten, der Art, des Umfangs und der Umstände und Zwecke der Datenverarbeitung.

Durch Sicherheitslücken können nicht nur die Lebensgewohnheiten derjenigen, die das System regelmäßig nutzen, überwacht werden, sondern auch gezielt Aufbrüche oder Überfälle geplant und durchgeführt werden oder das Bewegungsverhalten manipuliert werden, etwa durch falsche Routenvorschläge.

In der DSGVO werden Pseudonymisierung und Verschlüsselung als beispielhafte Maßnahmen aufgeführt.

2.9 Datenübermittlung in Drittländer

Bei der Datenübermittlung in Drittländer muss der Verantwortliche nach Artt. 44 ff. DSGVO Garantien in Bezug auf die internationale Übermittlung von Daten vorhalten, die sicherstellen, dass das durch die DSGVO gewährleistete Schutzniveau nicht untergraben wird.

2.10 Verzeichnis von Verarbeitungstätigkeiten und Zusammenarbeit mit den Aufsichtsbehörden

Der Verantwortliche muss ein Verzeichnis aller seiner Verarbeitungstätigkeiten führen, dass die Angaben des Art. 30 Abs. 1 DSGVO enthält.

Ferner muss jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten führen, dass den Angaben des Art. 30 Abs. 2 DSGVO genügt.

Die Verzeichnisse sind nach Art. 30 Abs. 3 und Abs. 4 DSGVO schriftlich oder elektronisch zu führen und müssen auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt werden. Bei weniger als 250 Mitarbeitern besteht die Pflicht nicht, wenn nur ein geringes Risiko mit der Verarbeitungstätigkeit verbunden ist.[349]

---

[347] ErwG 78 S. 4 DSGVO.

[348] ErwG 78 S. 5 DSGVO.

[349] Weiterführend: DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten.

2.11 Datenschutzfolgenabschätzung

Nach Art. 35 DSGVO muss der Verantwortliche eine Datenschutzfolgenabschätzung (DSFA) durchführen, wenn die Verarbeitung voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden ist. Das Risiko bezieht sich dabei auf die Grundrechte der betroffenen Personen, die durch eine Datenverarbeitung tangiert werden können. Die DSGVO verlangt, dass solche Risiken durch geeignete technische und organisatorische Maßnahmen eingedämmt werden.

Für die Durchführung der DSFA kann auf die anerkannte Methodik des Standard-Datenschutzmodells (SDM) [350] zurückgegriffen werden. Das SDM wurde von der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) einstimmig angenommen [351] und wird von der Artikel 29-Datenschutzgruppe als Framework für die Durchführung einer Datenschutzfolgeabschätzung ausdrücklich anerkannt[352].

Die DSFA sollte entsprechend der in Art. 25, ErwG 78 DSGVO verankerten Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein Instrument angesehen werden, mit dem die Entscheidungsfindung vereinfacht wird. Die DSFA hilft dem Verantwortlichen nicht nur dabei, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten zu verstehen, sondern auch, die Pflichten nach der DSGVO umzusetzen und nachzuweisen.[353] Folglich sollte sie zum frühestmöglichen Zeitpunkt bereits in der Entwicklungsphase der Verarbeitungstätigkeiten als fortlaufender Prozess begonnen werden, selbst wenn einige Verarbeitungsvorgänge noch nicht bekannt sind.

Die Artikel 29-Datenschutzgruppe stellt darüber hinaus klar, dass die DSFA auch dann von Nutzen sein kann, wenn, wie vorliegend im Kontext moderner Fahrzeuge, die Auswirkungen eines Technologieproduktes, dass in verschiedenen Verarbeitungsvorgängen eingesetzt werden wird, auf den Datenschutz untersucht werden sollen.[354]

Die DSFA wird im Projektkontext in Deliverable 3.3 aus einer technischen Perspektive näher untersucht.

---

[350] DSK, SDM, V.1.1.

[351] Vgl. die Empfehlung auf der Homepage der Bundesdatenschutzbeauftragten, abrufbar: https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtiTec/Standard-Datenschutzmodell.html (zuletzt abgerufen: 15.02.2018).

[352] Artikel 29-Datenschutzgruppe, WP 248 rev.01, S. 21, S. 28.

[353] Weiterführende Hinweise: DSK, KP Nr. 5.

[354] Artikel 29-Datenschutzgruppe, WP 248 rev.01, S. 8.

2.12 Melde und Benachrichtigungspflichten bei Datenschutzvorfällen

Bei der Verletzung des Schutzes personenbezogener Daten bestehen nach den Artt. 33 ff DSGVO unverzügliche Melde- und Benachrichtigungspflichten gegenüber den Aufsichtsbehörden und bei hohem Risiko für Ihre Rechte gegenüber den betroffenen Personen.

2.13 Auswahl geeigneter technischer und organisatorischer Maßnahmen

Für den Rechtsanwender bestehen, wie bereits erläutert, Herausforderungen bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen, da die DSGVO keine konkreten Vorgaben enthält. Die systematische Ableitung von Anforderungen aus den abstrakten und komplexen Kriterien der DSGVO im Kontext der Einbindung von Dienstanbietern in den vernetzten, automatisierten und kooperativen Straßenverkehr mittels der Methodik des SDM, anhand der der datenschutzrechtliche Anforderungskatalog [355] entwickelt wurde, wurde bereits im Abschnitt 2.1.2.2 dargestellt. Nachfolgend werden der rechtliche Rahmen der DSGVO, den das SDM operationalisiert, und die Anforderungen an eine Pseudonymisierungslösung näher untersucht.

2.13.1 Beurteilungskriterien

In der DSGVO sind Kriterien vorgegeben, die bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen vom Verantwortlichen zu berücksichtigen sind. Danach soll die Maßnahmenauswahl unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen erfolgen. Bei Art. 25 und Art. 32 DSGVO sind ferner bei der Auswahl auch der Stand der Technik und die Implementierungskosten zu berücksichtigen. Ziel dieser Abwägung ist der Schutz der Grundrechte der betroffenen Personen durch ein angemessenes Schutzniveau.

In der DSGVO wird hierfür ein risikobasierter Ansatz verfolgt. Das durch die Verarbeitung eröffnete Risiko bezieht sich auf die betroffenen Schutzgüter, die Grundrechte der betroffenen Personen.[356] Das zu gewährleistende Schutzniveau orientiert sich daher am Schutzbedarf, der erforderlich ist, um Grundrechtsverletzungen wirksam zu verhindern. Der Schutzbedarf resultiert bereits aus der Datenverarbeitung als solcher und erhöht sich mit dem damit verbundenen Risiko eines Schadeneintritts.

---

[355] Bestandteil des iKoPA–Deliverable 1v2 (im Erscheinen), abrufbar: https://ikopa.de/de/arbeitsergebnisse/ (letzter Abruf:10.12.2018).

[356] ErwG 1, 2, 76 DSGVO.

Diese Risiken können zu physischen, materiellen oder immateriellen Schäden führen.[357] Immaterielle Schäden bestehen in der Verletzung der Grundrechte der betroffenen Personen.[358] Beispiele sind der Verlust der Vertraulichkeit bei der Telekommunikation, Art. 7 GRCh bzw. Art. 10 GG, der Bruch der Integrität und damit der Vertraulichkeits- und Integritätserwartung bei eigengenutzten IT-Systemen, oder nicht mehr zu wissen, wer was wann über einen weiß, Artt. 2 Abs. 1, 1 Abs. 1 GG bzw. Artt. 7, 8 GRCh. Mögliche immaterielle Schäden können ferner die Diskriminierung der betroffenen Person, die Aufhebung von Pseudonymen, fehlende Kontrollmöglichkeiten für die betroffenen Personen, Daten aus denen besondere Kategorien personenbezogener Daten hervorgehen oder die Bewertung persönlicher Aspekte der betroffenen Person sein.[359]

Die Eintrittswahrscheinlichkeit und Schwere des Risikos sind im Verhältnis zu Art, Umfang, Umständen und Zwecken der Verarbeitung anhand objektiver Kriterien zu ermitteln.[360] Ferner ist zu bewerten, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.[361] Der Schutzbedarf ist eng verbunden mit der Eingriffsintensität in die Grundrechte.[362] Mit zunehmendem Risiko steigt daher auch der Schutzbedarf. Je intensiver der durch das Risiko vermittelte Eingriff, umso höher ist der Schutzbedarf und desto strengere Anforderungen sind an die den Eingriff rechtfertigenden Gründe zu stellen.[363] Die Gewichtung des Risikos für die Grundrechte der betroffenen Personen hat daher Folgen für die Ausgestaltung der funktionalen Aspekte des Verfahrens und die umzusetzenden technischen und organisatorischen Schutzmaßnahmen. Je höher das mit der Verarbeitung gesetzte Risiko, umso mehr und aufwendigere technische und organisatorische Maßnahmen müssen zur Risikominimierung umgesetzt werden.

Welche technischen und organisatorischen Maßnahmen im Verhältnis zu dem, aus dem Risiko resultierenden Schutzbedarf angemessen sind, richtet sich nur bei Art. 25 und Art 32 DSGVO – nicht hingegen bei der allgemeinen Pflicht aus Art. 24 DSGVO – auch nach dem Technikstand und den Implementierungskosten. Auch hier gilt aber, dass an höhere Risiken auch höhere Anforderungen zu stellen sind.

---

357 ErwG 75 DSGVO.

358 Forum Privatheit, DSFA, S.32 f.

359 ErwG 75 DSGVO.

360 ErwG 90, 76 DSGVO.

361 ErwGe 74, 76 DSGVO.

362 Bieker/ Hansen/ Friedewald, RDV 2016, 188 (192 f).

363 zur Anwendung der sog. „Je-desto-Formel“: BVerfGE 119, 1ff. (30); NJW 2008, 39ff. (42).

Das Bundesverfassungsgericht betont besonders, dass solcher technische Aufwand und damit verbundene Kosten nicht ins Gewicht fallen können, die im Rahmen einer datenschutzfreundlichen technischen Gestaltung vermeidbar gewesen wären.[364] Diese Gewichtung ergibt sich nun unmittelbar aus dem Gesetzeswortlaut, vgl. Art. 24 Abs. 1 DSGVO.

Nach einer Betrachtung des Schutzbedarfs und der Gewichtung des Risikos wird die Geeignetheit einer Pseudonymiserungslösung für die Risikominderung untersucht.

2.13.2 Risikogewichtung und Schutzbedarf der Fahrzeugdaten

Die Fahrzeugdaten im Kontext des vernetzten, automatisierten und kooperativen Fahrens sind aufgrund der zahlreichen Identifizierungsmöglichkeiten, dem großen Umfang, den enthaltenen Standortdaten und der präzisen Echtzeiterfassung der Daten in der Regel hoch verknüpfbar und können leicht zur Erstellung von Bewegungs- oder/ und Verhaltensprofilen genutzt werden.

Aus den Fahrzeugdaten können vielfältige Schlüsse auf das Privatleben der Person gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderen Rhythmen erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Person und das soziale Umfeld. Die Bewegungsdaten können somit auch Aufschluss über den Besuch einer Kirche oder Moschee, einer Demonstration, intime Vorlieben oder häufige Arzt- oder Klinikaufenthalte und damit über den besonders geschützten inneren Lebensbereich der betroffenen Person offenbaren.

Die insweit bestehenden unterschiedlichen Verkettungsrisiken und der daraus resultierende Schutzbedarf wurden bereits bei der Untersuchung des Personenbezugs dargestellt.

Sind die von der Datenverarbeitung betroffenen Personen auch in ihrer Funktion als Verbraucher oder Arbeitnehmer betroffen, besteht aufgrund des Abhängigkeits-verhältnisses bzw. strukturellen Verhandlungsungleichgewichts ein zusätzlich erhöhter Schutzbedarf.[365] Insbesondere Standortdaten können eine unzulässige Arbeitnehmer-überwachung ermöglichen.[366]

Der Schutzbedarf von Fahrzeugdaten im Kontext des vernetzten, automatisierten und kooperativen Fahrens, ist insofern – vorbehaltlich der konkreten Ausgestaltung im Einzelfall– hoch und steigt darüber hinaus stetig an. Der Mobilitätsdienstanbieter, der

[364] BVerfG, Beschluss v. 27.10.2006, –1 BvR 1811/99–, Rn. 24 f., juris.

[365] Vgl. BVerfG, Beschluss v. 23.11.2006, –1 BvR 1909/06–, NJW 2007, 286 ff.

[366] Ausführlich: Hansen et al., Verkettung digitaler Identitäten, 197 ff.

einen daten- und/ oder ortsbasierten Mobilitätsdienst betreibt und dabei über eine in die Fahrzeugsysteme implementierte Kommunikationsplattform mit den Fahrzeugsystembetreibern, Infrastrukturanbietern und weiteren Anbietern von Mobilitätsdienstleistungen und anderen Dienstleistungen mithilfe unterschiedlicher Kommunikations- und Analysetechniken kooperiert, eröffnet ein hohes Risiko für die Grundrechte der betroffenen Personen. Auch wenn eine abschließende Bewertung nur in einem konkreten Einsatzszenario möglich ist, spricht das dafür, dass strenge Anforderungen an die Ausgestaltung des Verarbeitungsvorgangs zustellen sind.

2.13.3 Generelle Eignung einer Pseudonymisierungslösung im Fahrzeugkontext

In der DSGVO wird die Pseudonymisierung vielfach erwähnt, ohne dass sie verbindlich vorgeschrieben wird. Daher ist die Notwendigkeit einer Pseudonymisierung bei der Einbindung privater Dienstleister in den Kontext des vernetzten, automatisierten und kooperativen Fahrens näher zu untersuchen.

Eine Pseudonymisierung wird in der DSGVO zunächst bei einem dauerhaft auf ein geringes Maß abgesenkten Risiko an verschiedenen Stellen privilegiert. Zu nennen sind die Erleichterungen nach Art. 11 DSGVO. Zudem kann unter eng umgrenzten Umständen eine Weiterverarbeitung zu anderen Zwecken unter den erleichterten Voraussetzungen des Art. 6 Abs. 4 DSGVO in Betracht kommen, wenn der geänderte Zweck mit dem Ursprungszweck kompatibel ist. Das ist anhand einer umfassenden Einzelfallabwägung zu ermitteln, wobei gemäß Art. 6 Abs. 4 lit. e DSGVO insbesondere eine Pseudonymiserung positiv berücksichtigt werden kann. Auch bei der nach Art. 6 Abs. 1 lit. f DSGVO vorzunehmenden Abwägung der berechtigten Interessen kann sich die Pseudonymisierung auf das Abwägungsergebnis positiv auswirken. Beide Rechtsgrundlagen können allerdings eine Aufdeckung des Pseudonyms und damit einen Rückbezug auf die Person im Regelfall nicht rechtfertigen und sind insoweit in ihrer Legitimationswirkung begrenzt. Für die Aufhebung der Pseudonymiserung bedarf es, abseits spezialgesetzlicher (z.B. strafrechtlicher) Vorschriften, einer anderen Rechtsgrundlage, die regelmäßig in der Einwilligung gefunden werden muss.

Diese Ausführungen zeigen im Umkehrschluss, dass eine Pseudonymisierung das Risiko einer ansonsten unrechtmäßigen Verarbeitung auf ein zulässiges Maß begrenzen kann. Sie ist zwar nicht verpflichtend durchzuführen. Bei ihrem Fehlen kann jedoch ein Verarbeitungsverbot die Konsequenz darstellen.

Insbesondere kann ein wirksames Pseudonymisierungskonzept nicht nur im Sinne einer datenschutzfreundlichen Systemgestaltung „by Design“ nach Art. 25 DSGVO erforderlich sein, um eine frühe Identifikation betroffener Personen wirksam zu verhindern. Die Pseudonymiserung ist bei hohem Verarbeitungsrisiko – vorausgesetzt das Risiko wird wirksam minimiert – zugleich auch eine notwendige Bedingung dafür, dass die beabsichtigte Verarbeitung überhaupt erst die Voraussetzungen einer Rechtsgrundlage erfüllen kann. Unabhängig davon, ob eine spezialgesetzliche Regelung geschaffen wird, oder die Verarbeitung auf die Erlaubnistatbestände des Art. 6 DSGVO gestützt wird, wird

eine Datenverarbeitung aufgrund der grundrechtlichen Vorgaben nämlich nur dann erlaubt sein, wenn dem Risiko der Erstellung von Verhaltens- und Bewegungsprofilen wirksam begegnet wird.

Ohne eine wirksame Pseudonymisierung, oder vergleichbare Schutzmaßnahmen dürfte daher eine rechtmäßige Verarbeitung im Kontext des vernetzten, automatisierten und kooperativen Fahrens nicht zu erreichen sein.

2.13.4 Anforderungen an eine Pseudonymisierungslösung

Aus den dargestellten rechtlichen Vorgaben, insbesondere aus dem bereits im Rahmen der Rechtsgrundlage zu prüfenden Grundsatz der Erforderlichkeit, sowie den Grundsätzen der Zweckbindung und der Datenminimierung in den Artt. 5 , 6 DSGVO resultieren strenge Anforderungen an die Pseudonymisierung im Kontext des vernetzten, automatisierten und kooperativen Fahrens.

Ein geeignetes Pseudonymisierungskonzept kann einige der dargestellten Risiken bereits bei der Architekturgestaltung in wesentlichen Punkten adressieren (vgl. Abb. 2 und 3).

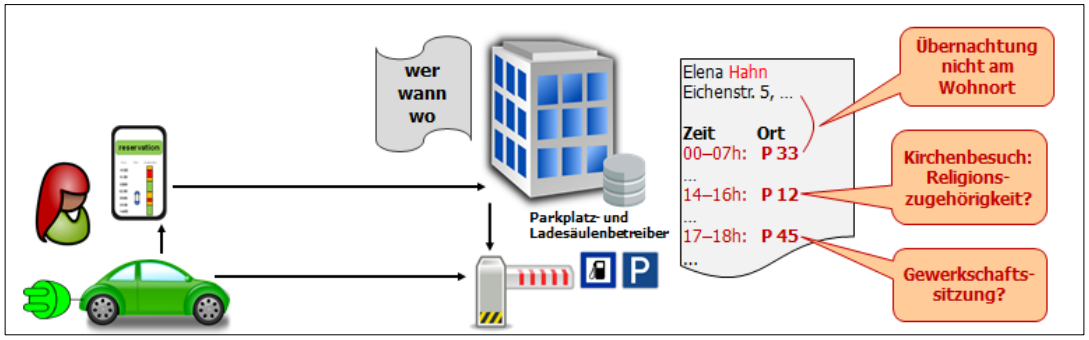

Abbildung 2: Hohes Risiko der Erstellung von Bewegungs- und Verhaltensprofilen bei der Reservierung von Parkplätzen ohne Pseudonymisierungskonzept

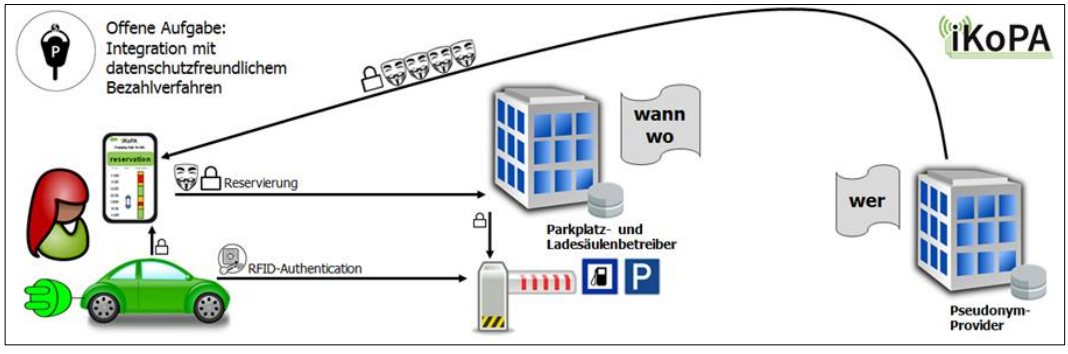

Abbildung 3: Entwicklung eines datenschutzfreundlichen Pseudonymisierungskonzepts „by Design“

Aufgrund der hohen Verkettungsrisiken und der zahlreichen Begehrlichkeiten ist bei der Implementierung eine starke Pseudonymisierung erforderlich, um eine unberechtigte Aufdeckung wirksam zu verhindern.

Zudem ist die Absicherung der Pseudonymisierung durch weitere technische und organisatorische Maßnahmen ebenso notwendig, wie die Sicherstellung der Einhaltung der Vorgaben der DSGVO insgesamt durch flankierende Maßnahmen.

Die unterschiedlichen, bereits beim Personenbezug dargestellten Risiken der Erstellung von Bewegungs- und Verhaltensprofilen sind unbedingt zu vermeiden. Dabei sind die zahlreichen Identifikationsmöglichkeiten und die Kombinationsmöglichkeiten mit anderen Produkten ebenso zu berücksichtigen wie die verschiedenen Möglichkeiten ihrer Kenntnisnahme.

Nachfolgend werden die wichtigsten Anforderungen an eine Pseudonymsierungslösung zusammengefasst dargestellt. [367]

2.13.4.1 Mehrstufige Pseudonymverfahren

Die benötigte starke Pseudonymisierung erfordert den kombinierten Einsatz von Rollen-Beziehungs-Pseudonyme [368] und Transaktionspseudonymen in gestuften Pseudonymisierungsverfahren.[369]

Die Pseudonymisierung ist insgesamt nur wirksam, wenn eine Aufdeckung der Pseudonyme zuverlässig verhindert werden kann. Wegen der leichten Wiedererkennbarkeit fester Merkmale dürfen feststehende Kfz- oder Nutzer-Pseudonyme nur der Ausgangspunkt weiterer Pseudonymisierungen sein und zudem nicht für die Individual-Kommunikation verwendet werden.

Bei der Individualkommunikation sollten Transaktionspseudonyme verwendet werden. Bei jedem Kommunikationsvorgang bzw. Transaktion wird dann ein neues Pseudonym eingesetzt.

Werden die Transaktionspseudonyme nicht lokal im Fahrzeug erzeugt, sondern müssen im Wege der Individualkommunikation bei einem Pseudonym-Provider angefragt werden, entstehen zusätzliche Verkettungsrisiken. So können beispielsweise Metadaten,

---

[367] Zu den umfassenden datenschutzrechtlichen Anforderungen an die Einbindung privater Dienstanbieter in das Gesamtsystem des vernetzten, automatisierten und kooperativen Verkehrs vgl. das iKoPA-Deliverable 1v2 (im Erscheinen), abrufbar: https://ikopa.de/de/arbeitsergebnisse/ (letzter Abruf:10.12.2018).

[368] Zur Terminologie vgl. Pfitzmann/ Hansen, Anon Terminology v.034, abrufbar: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (letzter Abruf: 10.12.2018).

[369] Weichert, SVR 2016, 361 (364).

die entstehen, wenn ein Fahrzeug vor jeder Kommunikation ein Pseudonym anfragt, Bewegungsprofile ermöglichen. Diese Risiken müssen erkannt und wirksam gemindert werden, z.B. durch die Aushändigung mehrerer Transaktionspseudonyme auf einmal, um über die nach außen sichtbare äußere Kommunikationsbeziehung möglichst wenig Rückschlüsse und damit Verkettungsmöglichkeiten zuzulassen.

Problematisch ist insoweit, dass in heutigen Kommunikationsnetzen, insbesondere bei der Kommunikation über das Internet, Nachrichten über unterschiedliche Metadaten oder auch Quasi-Identifikatoren verkettet und damit Pseudonyme aufgehoben werden können. Bei der Nutzung technischer Anwendungen werden oft zusätzliche Identifikatoren erzeugt, die Rückschlüsse auf eine Person zulassen. Auch bei mittels Aggregation pseudonymisierten Daten können Quasi-Identifikatoren erzeugt werden, wie beispielsweise bei der Methodik des Fingerprinting. Auch bei einer pseudonymen Konzeption bestehen daher bei einer praktischen Implementierung unterschiedliche ungewollte Identifikationsrisiken.[370] Insofern besteht in der Praxis ein inhärenter Konflikt zwischen Data Protection by Design und „Identifiability-by-Default“.[371]

Die Aussagekraft der Metadaten sinkt dann, wenn weniger Daten versendet werden. Es existieren im Rahmen von C-ITS vielversprechende Ansätze, die aber weiter erforscht werden müssen. So können Lösungsansätze zu Methoden der Datensparsamkeit bisher die Herstellung eines Personenbezugs nicht zuverlässig vermeiden.[372] Besonders problematisch ist die Adressierung des Verkettungsrisikos bei Pseudonymwechseln, beispielweise im Rahmen der V2V- oder V2X-Kommunikation. So können unterschiedliche orts- oder zeitbezogene Verknüpfungsmöglichkeiten zwischen einem verschwundenen und einem neu aufgetauchten Pseudonym bestehen bleiben, wodurch ein altes Pseudonym trotz des Wechsels wiedererkannt werden kann. Bislang erforschte Pseudonymisierungslösungen (Mix-Zonen oder häufige Pseudonymwechsel) funktionieren noch nicht zuverlässig.[373]

2.13.4.2 Public–-Key–-Infrastruktur

Eine zentrale Frage ist die Ausgestaltung der Verwaltung der verwendeten Schlüssel im Rahmen der Public-Key-Infrastruktur. Sie ist zugleich „*Erfolgsbedingung und Achillesferse*“[374] einer wirksamen Pseudonymisierungslösung.

---

[370] Artikel 29-Datenschutzgruppe, WP 252; IWGDP, vernetzte Fahrzeuge, S. 8.

[371] Strauß, DuD 2018, 497 (498 m.w.N.).

[372] Hansen, DuD 2015, S. 371; Troncoso et al., 2011, 3199 ff.

[373] Troncoso et al., 2011, 3199 ff.

[374] Zu C-ITS vgl. Weichert, SVR 2016, 361 (364).

2.13.4.2.1 Vermeidung zentraler Instanzen

Mit der Einrichtung zentraler Instanzen steigt auch die Missbrauchsgefahr, der mit der Rechtsordnung nicht zu vereinbarenden Gefahr einer Überwachungsinfrastruktur. [375] Da ein absoluter Schutz nicht zu erreichen ist, ist das Risiko bei einer verteilten Infrastruktur gegenüber einer hierarchischen deutlich geringer und daher zu bevorzugen.[376] Bei der Frage, ob der Betrieb der Infrastruktur zentralisiert oder dezentral organisiert werden sollte, gelten die gleichen Erwägungen. Große Datensammlungen an zentralen Stellen sind zu vermeiden. Da absolute Sicherheit nicht zu erreichen ist und der technologische Fortschritt stetig neue Analysemöglichkeiten hervorbringt, können Angriffe beispielsweise in Form von Identitätsdiebstahl selbst bei maximalem Aufwand nicht verhindert werden.

Die Motivation potentieller Angreifer kann durch eine dezentrale Wissensansammlung deutlich gesenkt werden. Insbesondere interner Missbrauch kann vermieden werden, wenn die Aufdeckung nur über das Zusammenwirken mehrerer unabhängiger Stellen, die sich gegenseitig kontrollieren, möglich ist. Insofern bedarf es institutioneller Maßnahmen, die das Risiko des internen und auch des organisationsübergeifenden kollusiven Zusammenwirkens kontrollieren und begrenzen.

Die Artikel-29-Datenschutzgruppe weist im Rahmen von C-ITS darauf hin, dass nach dem derzeitigen Kenntnisstand keine technischen Einzelheiten zur PKI-Infrastruktur bekannt sind, die gewährleisten, dass die ausgetauschten Daten auch praktisch pseudonymisiert sind. [377] Eine wirksame Risikominderung bei C-ITS sei insoweit derzeit nicht erkennbar.[378] Diese Erwägungen gelten entsprechend bei einer Pseudonymisierungslösung, mit der dritte Dienstanbieter in die Kommunikationsarchitekturen der vernetzten und kooperativen Fahrzeugsysteme eingebunden werden sollen.

2.13.4.2.2 Absicherung der Datentrennung durch ergänzende Maßnahmen

Ob Nachrichten, die das Fahrzeug verlassen, auch praktisch als wirksam pseudonymisiert angesehen werden können, ist von zusätzlichen Sicherungen abhängig.[379]

Die Pseudonymisierung ist nur dann rechtssicher, wenn sie als Bestandteil eines Bausteinkonzepts von weiteren ergänzenden technischen und organisatorischen Maßnahmen zur Datentrennung und zur Einhaltung der weiteren Vorgaben der DSGVO

---

[375] Vgl. Ethik–Kommission, S. 24.

[376] Weichert, SVR 2016, 361 (364).

[377] Artikel 29-Datenschutzgruppe, WP 252, 5.

[378] Artikel 29-Datenschutzgruppe, WP 252, 5.

[379] Rossnagel, ZD 2018, 243 ff.

flankiert wird. Nach Art. 4 Nr. 5 DSGVO liegt eine risikominimierende Pseudonymisierung nämlich nur dann vor, wenn die Umsetzung der DSGVO insgesamt gewährleistet ist, wobei besonders sicherzustellen ist, dass die identifizierenden Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die eine Identifizierung wirksam verhindern.[380]

Bei der organisatorischen Trennung durch Auslagerung an einen Auftragsverarbeiter liegt keine wirksame Datentrennung vor. Der Auftragsverarbeiter ist nämlich ausnahmslos verpflichtet, die Weisungen des Verantwortlichen zu befolgen und der Verantwortlich ist jederzeit befugt, die Weisungen an den Verarbeiter nach Belieben zu ändern, neu zu erteilen, oder zurückzuziehen, vgl. Art. 28 Abs. 3 lit. a, lit. g, Art. 29 DSGVO. Er kann also jederzeit nach Belieben Kenntnis von den Daten nehmen. Daher dürfte regelmäßig eine gemeinsame Verantwortung mit entsprechenden vertraglichen Absicherungen bzw. Kenntnisnahmeverboten notwendig sein.

Sofern gemeinsam Verantwortliche eine wirksame Datentrennung erreichen möchten, ist die verbindliche und klare Festlegung der jeweiligen Verantwortungsbeiträge und Festlegung der rechtssicheren Datentrennung eine Grundvoraussetzung.

2.13.4.2.3 Besonders abgesichertes Aufdeckungsverfahren

Die Aufdeckung der Identität darf nur dann erfolgen, wenn und soweit sie für die Zweckerreichung tatsächlich notwendig ist. Vorliegend kann in gewissen Fällen eine Identifizierung erforderlich sein, beispielsweise um innerhalb des Systems Angreifer zu identifizieren und Systemmissbrauch zu verhindern. Allerdings sind diese bestimmten Zwecke festzulegen, zu dokumentieren und spezifisch zu begrenzen. Die zahlreichen Begehrlichkeiten und der technologische Fortschritt verlangen hier ein besonders abgesichertes Aufdeckungsverfahren, um eine missbräuchliche oder auch vorschnelle Aufdeckung zu verhindern.

Durch den Einsatz von Attribute–-based Credentials for Trust (Privacy ABCs) [381] können die mit der Schaffung zentraler Pseudonymisierungsinstanzen einhergehenden Missbrauchsmöglichkeiten und die Gefahr der unberechtigten Aufdeckung von Pseudonymen vermieden, sowie Vertrauen in die Wirksamkeit der Pseudonymisierung geschaffen werden. Zugleich können aber auch Missbräuche und Angriffe verhindert oder auch aufgedeckt werden, indem verschiedene Mechanismen zusammenwirken müssen, die einer vorschnellen, gegebenenfalls unberechtigten Aufdeckung bzw. dem

[380] ErwG 29 DSGVO.

[381] Weiterführend: Hansen et al, in: ABC4Trust, 143 ff.

Entzug des Pseudonyms wirksam entgegenwirken können.[382] Über diese Mechanismen kann zudem die Unterrichtung der betroffenen Person nach einer Aufdeckung gewährleistet werden.

Sofern die Schaffung von Vertrauen über einen zentralen PKI–-Mechanismus erreicht werden soll, weist die Artikel 29–Datenschutzgruppe darauf hin, dass in der Schaffung einer mit einer PKI-–Infrastruktur verbundenen zentralen Instanz auch ein erhebliches Missbrauchspotential liegen kann.[383] Insbesondere, wenn die PKI–-Infrastruktur keinen Durchsetzungsmechanismus zur Feststellung der tatsächlichen Absichten der Zertifikatsinhaber oder Ausstellers vorsieht, sind weitere Mechanismen und Kontrollen zur Herstellung von Vertrauen erforderlich.[384] Diese Aussagen im Kontext von C-ITS sind auch auf andere PKI–-Infrastrukturen zu übertragen.

2.13.4.3 Lokale Verarbeitung und frühzeitige Löschung bzw. Aggregation im Fahrzeug

Daten sind grundsätzlich anonym zu erheben bzw. frühestmöglich zu anonymisieren, wenn nicht ausnahmsweise eine Notwendigkeit für eine pseudonyme Verarbeitung besteht. Technische Lösungen sind organisatorischen Maßnahmen gegenüber zu bevorzugen. Insbesondere wenn der Verantwortliche eine vollautomatisierte Verarbeitung anstrebt, folgt dies bereits aus dem Gebot der Fairness aus Art. 5 Abs. 1 DSGVO.

Das Risiko der ungewollten Aufhebung der Pseudonymisierung ist in einem dynamischen Gebiet wie dem vernetzten Verkehr besonders schwer kontrollierbar. In einem vernetzten und kooperativen Kommunikationssystem, das zahlreiche Technologien und Akteure verbindet, verschwimmen auch die Systemgrenzen, so dass nicht mehr zuverlässig überprüft werden kann, ob eine Annahme noch gilt. Aus der Kooperation entstehen zahlreiche Verkettungs-, Analyse und damit Trackingmöglichkeiten, z.B. bei der Koppelung eines Smartphone an die Fahrzeugsysteme; bei der Anbindung von E-–Autos an die Ladeinfrastruktur; bei der Einbindung weiterer zentraler Akteure wie einem zentralen Reservierungsservice; oder bei der Integration von Bezahlverfahren in die Gesamtarchitektur des vernetzten, automatisierten und kooperativen Straßenverkehrs. Die Pseudonymisierung muss insoweit auch praktisch wirksam sein. Dabei müssen die Risiken, die in einem Gesamtsystem durch den kombinierten und kooperativen Einsatz unterschiedlicher Technologien entstehen, auch anwendungsübergreifend adressiert und gemindert werden.

---

[382] Vgl. Hansen et al, in: ABC4Trust, 143 (155 ff.).

[383] Vgl. die übertragbaren Erwägungen zu C-ITS der Artikel-29-Datenschutzgruppe, WP 252, S. 15 (m.w.N.).

[384] Artikel-29-Datenschutzgruppe, WP 252, S. 15.

Daher sollte auch verbindlich festgeschrieben werden, wie festgestellt werden kann, inwieweit bei mehreren, für sich untersuchten Garantien oder Einzelmaßnahmen auch eine Gesamtaussage bezüglich des gesamten Systems möglich ist, und wie die gemeinsam Verantwortlichen diesen Risiken begegnen müssen. Das umfasst die verbindliche und klare Festlegung der jeweiligen Verantwortung, des Umfangs der Kooperation und der Gesamtverantwortung für die Risiken, die aus der Kooperation resultieren und wirksame Maßnahmen zur Risikominderung.

Den zahlreichen denkbaren Angriffs- und Missbrauchsszenarien und der hohen Identifikationskraft der bei der Nutzung von Telekommunikationsmitteln anfallenden Metadaten kann durch eine lokale Verarbeitung der Fahrzeugdaten im Fahrzeug selbst begegnet werden.

Daten, die für die Zweckerreichung nicht mehr benötigt werden, sind frühestmöglich zu löschen oder wirksam und vollständig zu anonymisieren. Das fortdauernde Speichern personenbeziehbarer Daten über den Zweckfortfall hinaus ist ein eigenständiger Grundrechtseingriff und bedarf einer neuen Rechtfertigung, insbesondere einer eigenen Rechtsgrundlage und der Einhaltung der weiteren Verarbeitungsgrundsätze.

Daher muss technisch sichergestellt werden, das Standort- und Umfelddaten im Fahrzeug bei Zweckfortfall unverzüglich wieder überschrieben oder vollständig gelöscht werden, sofern keine andere Rechtsgrundlage die fortdauernde Speicherung ausnahmsweise rechtfertigt. Gleiches gilt bei Daten über die Fahrzeugumgebung und den Fahrzeuginnenraum zum Schutz anderer Verkehrsteilnehmer und von Mitfahrern. Bei berechtigter Speicherung sollten frühzeitige Aggregationsverfahren eingesetzt und die Rohdaten, soweit überhaupt nötig, nur lokal im Fahrzeug gesichert werden. So kann der Verantwortliche seiner Pflicht zur Datenminimierung und Nichtverkettung gerecht werden und das Risiko von Datenpannen gering halten.

Bei der Aggregation sollten die Ausführungen der Art. 29-Datenschutzgruppe, die in dem Zusammenhang die datenschutzrechtlichen Implikationen unterschiedlicher Anonymisierungstechniken dargestellt hat, beachtet werden.[385] Ferner ist zu bedenken, dass auch bei Aggregationsverfahren Quasi-Identifikatoren entstehen können, die eine Profilbildung und damit eine Personenbeziehbarkeit ermöglichen.[386]

[385] Artikel 29-Datenschutzgruppe, WP 216.

[386] Strauß, DuD 2018, 497 (499).

2.13.4.4 Gewährleistung von Transparenz und Intervenierbarkeit

Datenschutz durch Technikgestaltung erfordert zudem stärkere Transparenz für die betroffenen Personen.[387] Transparenz und Intervenierbarkeit sind für das Verfahren insgesamt und die betroffene Person ebenso wie der Schutz der personenbezogenen Daten einschließlich der Kommunikationsverbindungen sicherzustellen. Insbesondere müssen die Voreinstellungen zuverlässig verhindern, dass personenbezogene Daten nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden, Art. 25 Abs. 2 S. 2 DSGVO.

Ein besonderes Risiko geht insoweit von nicht abschaltbaren oder nicht kontrollierbaren datenverarbeitenden Systemen aus, etwa wenn die Fahrzeugsysteme im Rahmen von C–ITS über Broadcast-Technologien Informationen austauschen bzw. weiterleiten oder sich via RFID-Technologie authentifizieren. Die Verbreitung von Meldungen via Broadcast-Technologien an unbestimmte und nicht kontrollierbare Empfänger durch ein identifizierbares Fahrzeug bietet neue Trackingmöglichkeiten. Es entsteht, anders als bei der Individualkommunikation, die nur zwischen Sender und Empfänger stattfindet, eine Informationsasymmetrie zu Lasten des Absenders, da er bei Broadcast die Empfänger nicht kontrollieren kann. Diese Informationsasymmetrie muss durch ein höheres Niveau der Kontrolle der personenbezogenen Daten wieder ausgeglichen werden. Die Deaktivierungsmöglichkeit der entsprechenden Hardware im Fahrzeug kann, bei fehlendem Bezug zu fahrsicherheitsrelevanten Fahrfunktionen, eine geeignete Schutzmaßnahme darstellen.

2.13.4.5 Datenschutzfreundliche Bezahlverfahren

Ein Pseudonymisierungskonzept zur pseudonymen Reservierung von Diensten, wie Ladesäulen oder Parkplätzen, darf auch nicht durch die Kooperation von Dienstanbietern bzw. der Kombination mit weiteren Verarbeitungsvorgängen und die damit einhergehenden Verkettungsmöglichkeiten aufgehoben werden. Aus der Kooperation entstehen neue Verkettungsmöglichkeiten, z.B. bei der Koppelung eines Smartphone an die Fahrzeugsysteme; bei der Anbindung von E-Autos an die Ladeinfrastruktur; bei der Einbindung weiterer zentraler Akteure wie einem zentralen Reservierungsservice; oder bei der Integration von Bezahlverfahren in die Gesamtarchitektur des vernetzten, automatisierten und kooperativen Straßenverkehrs. Die Pseudonymisierung muss auch insoweit praktisch wirksam sein.

Erforderlich ist beispielsweise eine Integration datenschutzfördernder Bezahlverfahren in das Gesamtsystem. Die Nutzung eines Dienstes sollte auch datensparsam bezahlt

[387] IWGDP, vernetzte Fahrzeuge, S. 7, Nr. 24.

werden können, wenn der Nutzer dies wünscht.[388] Neben datenintensiven Abrechnungsmodellen über die exakte Anbindung an einen Rahmenvertrag müssen daher auch datenschutzfreundliche Bezahlverfahren angeboten werden. Zu denken ist neben der altbewährten Barzahlung auch an Prepaid-Lösungen auf Basis von attribute-based Credentials oder die pauschale Abrechnung zu einem Festpreis. Attributbasierte Berechtigungsnachweise bieten einen vielversprechenden Lösungsansatz.[389]

2.13.4.6 Flankierende Maßnahmen zur Einhaltung der Vorgaben der DSGVO insgesamt

Die Pseudonymisierung ist wie bereits dargelegt nur dann rechtssicher, wenn sie als Bestandteil eines Bausteinkonzepts von weiteren ergänzenden technischen und organisatorischen Maßnahmen zur Datentrennung und zur Einhaltung der weiteren Vorgaben der DSGVO flankiert wird.

Datenschutz durch Technikgestaltung gemäß Art. 25 Abs. 1 DSGVO verlangt zudem, dass sowohl zum Zeitpunkt der Konzeption und der Festlegung der Mittel, als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen ergriffen werden. Neben der datenschutzfördernden Gestaltung eines Pseudonymisierungskonzepts auf Architekturebene bedarf es daher auf dem Weg zu einer praktischen Implementierung weiterer technischer und organisatorischer Maßnahmen, die sicherstellen, dass die Pseudonymisierung auch praktisch wirksam wird und die Vorgaben der DSGVO insgesamt eingehalten werden.

Die regelmäßige Überprüfung des Risikos im Wege der Datenschutzfolgenabschätzung, die bei hohem Risiko nach Art. 35 DSGVO verpflichtend durchgeführt werden muss, bietet sich als Instrument an, den Verarbeitungsvorgang den dynamischen technischen Entwicklungen anzupassen, um am Ende der Entwicklung einen datenschutzfördernden Mobilitätsdienst „by Design“ anbieten zu können.

---

[388] Vgl. zu aggregierten Abrechnungsmodellen beim Smart Metering: Lüdemann/Ortmann/Pokrant, RDV 2016, 125 (131).

[389] Weichert, SVR 2016, 361 (364).

3 LITERATURVERZEICHNIS

Artikel 29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, 11.04.2018, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (letzter Abruf: 14.11.2018). [zitiert: Artikel 29-Datenschutzgruppe, WP 260 rev.01]

Artikel 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 10.04.2018, online: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (letzter Abruf: 09.11.2018). [zitiert: Artikel 29-Datenschutzgruppe, WP 259 rev.01]

Artikel 29-Datenschutzgruppe, Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS), WP 252, 04.10.2017, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171 (letzter Abruf: 24.10.2018). **[**zitiert: Artikel 29-Datenschutzgruppe, WP 252]

Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP 251 rev.01, 06.02.2018, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (letzter Abruf: 14.11.2018). [zitiert: Artikel 29-Datenschutzgruppe, WP 251 rev.01]

Artikel 29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, WP 249, 08.06.2017, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (letzter Abruf: 14.11.2018). [zitiert: Artikel 29-Datenschutzgruppe, WP 249]

Artikel 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 rev.01, 04.10.2017, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (letzter Abruf: 14.11.2018). [zitiert: Artikel 29-Datenschutzgruppe, WP 248 rev.01]

Artikel 29-Datenschutzgruppe, Stellungnahme 01/2017 zum Vorschlag für eine Verordnung über die Privatsphäre (Opinion on the Proposed Regulation for the ePrivacy Regulation 2002/58/EG), WP 247, 04.04.2017, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140

(letzter Abruf: 14.11.2018).
[zitiert: Artikel 29-Datenschutzgruppe, WP 247]

Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev01, 05.04.2017, abrufbar: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (letzter Abruf: 14.11.2018).
[zitiert: Artikel 29-Datenschutzgruppe, WP 242 rev.01]

Artikel 29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der RL/95/46/EG, 09.04.2014, WP 217, abrufbar: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf (letzter Abruf: 14.11.2018).
[zitiert: Artikel 29-Datenschutzgruppe, WP 217]

Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10.04.2014, abrufbar: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf (letzter Abruf: 24.10.2018).
[zitiert: Artikel 29-Datenschutzgruppe, WP 216]

Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, abrufbar: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf (letzter Abruf: 14.11.2018).
[zitiert: Artikel 29-Datenschutzgruppe, WP 169]

Arzt, Clemens/ Ruth-Schumacher, Simone, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, in: Neue Zeitschrift für Verkehrsrecht (NZV) 2017, 57-62.
[zitiert: Arzt/ Ruth-Schumacher, NZV 2017]

Assion, Simon, Must Carry: Übertragungspflichten auf digitalen Rundfunkplattformen, Hamburg 2015, abrufbar unter: https://www.telemedicus.info/uploads/150408-SAS-DoktorarbeitinVerffentlichungsfassung.pdf (letzter Abruf: 23.10.2018).
[zitiert: Assion, 2015].

Balzer, Thomas/ Nugel, Michael, Das Auslesen von Fahrzeugdaten zur Unfallrekonstruktion im Zivilprozess, in: Neue Juristische Wochenschrift (NJW) 2016, 193–272.
[zitiert: Balzer/ Nugel, NJW 2016]

Bayerisches Landesamt für Datenschutzaufsicht (Hrsg.), Synopse der ePrivacy-VO folgender Fassungen: Vorschlag der Europäischen Kommission vom 10. Januar 2017, (COM(2017) final 2017/0003 (COD)und Entwurf einer legislativen Entschließung des Europäischen Parlaments vom 23.10.2017, A8-0324/2017,

29.01.2018, abrufbar: https://www.lda.bayern.de/media/eprivacy_synopse.pdf (letzter Abruf: 03.12.2018).
[zitiert: BayLDA, Synopse ePrivacy-VO]

Benedikt, Kristin, Die geplante ePrivacy-Verordnung und ihr Verhältnis zur DSGVO und zum Telemediengesetz, in: Datenschutz-Berater (DB) 2018, 80-82.
[zitiert: Benedikt, DB 2018, 80]

Berndt, Stephan, Das Automobil im Visier der Strafverfolgungsbehörden – Das Auslesen von Daten der „Black-Box" automatisierter Fahrzeuge zur Strafverfolgung, Neue Zeitschrift für Verkehrsrecht (NZV) 2018, 249–257.
[zitiert: Berndt, NZV 2018, 249]

Bieker, Felix/ Hansen, Marit/ Friedewald, Michael, die grundrechtskonforme Ausgestaltung der Datenschutz–Folgenabschätzung nach der europäischen Datenschutz–Grundverordnung, in: Recht der Datenverarbeitung (RDV) 2016, 188–197.
[zitiert: Bieker/ Hansen/ Friedewald, RDV 2016, 188]

Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.), Strategie automatisiertes und vernetztes Fahren – Leitanbieter bleiben, Leitmarkt werden, Regelbetrieb einleiten, 2015, abrufbar: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/broschuere-strategie-automatisiertes-vernetztes-fahren.pdf?__blob=publicationFile (letzter Abruf: 15.11.2018).
[zitiert: BMVI, Strategie automatisiertes und vernetztes Fahren]

Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.), IVS–Aktionsplan „Straße", 2012, abrufbar: https://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/ivs-aktionsplan-strasse-broschuere.pdf?__blob=publicationFile (letzer Abruf: 14.11.2018).
[zitiert: IVS–Aktionsplan „Straße"]

Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.), Maßnahmenplan der Bundesregierung zum Bericht der Ethik-Kommission Automatisiertes und Vernetztes Fahren (Ethik-Regeln für Fahrcomputer), 25.08.2017, BT-Drucks. 18/13500.
[zitiert: BMVI, Maßnahmenplan Ethik-Kommission]

Brink, Stefan/ Wolff, Heinrich Amadeus (Hrsg.), BeckOK Datenschutzrecht, DSGVO, 26. Edition, Stand 01.05.2018.
[zitiert: Brink/ Wolff–*Bearbeiter*, DSGVO]

Britz, Gabriele, Grundrechtsschutz durch das Bundesverfassungsgericht und den Europäischen Gerichtshof, Referat auf Einladung des Arbeitskreises Europäisches Verfassungsrecht der Vereinigung der Deutschen Staatsrechtslehrer, Stand

06.10.2014, abrufbar: http://www.uni-giessen.de/fbz/fb01/professuren/britz/forschung/publikationen/publikationen#arbeitspapiere (letzter Abruf: 05.10.2018).
[zitiert: Britz, 2014]

Deutscher Anwaltverein (Hrsg.), Ausschuss Informationsrecht, Stellungnahme Nr.: 4/2018, zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union COM (2017) 495 final, Januar 2018, abrufbar: https://anwaltverein.de/de/newsroom/vo-vorschlag-zu-free-flow-of-data?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2018/ (letzter Abruf: 09.11.2018).
[zitiert: DAV, Stellungnahme 4/2018]

Deutscher Anwaltsverein (Hrsg.), Ausschuss Informationsrecht, Stellungnahme Nr. 24/2017, datenschutz- und persönlichkeitsrechtliche Aspekte von § 63a StVG-E und § 32 Abs. 1 Nr. 8 StVG-E im Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes („Entwurf zum hoch- oder vollautomatisierten Fahren"), abrufbar: https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo (letzter Abruf: 20.11.2018).
[zitiert: DAV, Stellungnahme 24/2017]

Dewri, Rinku/ Annadata, Prasad/ Eltarjaman, Wisam/ Thurimella, Ramakrishna, Inferring Trip Destinations From Driving Habits Data, in: WPES '13 Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society, 2013, ACM, 267–272, abrufbar: https://cs.du.edu/~rdewri/data/MyPapers/Conferences/2013WPES-Extended.pdf (letzter Abruf: 20.11.2018).
[zitiert: Dewri et al., 2013]

Enev, Mirov/ Takakuwa, Alex/ Koscher, Karl/ Kohno, Tadayoshi, Automobile Driver Fingerprinting, in: Proceedings on Privacy Enhancing Technologies, 2016 (1), 34-51.
[zitiert: Enev et al 2016]

Ernsthaler, Jürgen, SIM–TD Deliverable D5.5, Bewertung Rechtliche Rahmenbedingungen, 12.09.2013, abrufbar: https://www.eict.de/fileadmin/redakteure/Projekte/simTD/Deliverables/simTD-TP5-Abschlussbericht_Teil_B-5_Rechtliche_Rahmenbedingungen_V10.pdf (letzter Abruf: 20.11.2018)
[zitiert: Ernsthaler, SIM-TD]

Ethik–Kommission Automatisiertes und Vernetztes Fahren (Leitung: Di Fabio, Udo; Herausgeber: BMVI), Bericht vom 20.06.2017, abrufbar: Bundesministerium für Verkehr und Digitale Infrastruktur,

https://www.bundesregierung.de/Content/Infomaterial/BMVBS/bericht-der-ethik-kommission_348344.html (letzter Abruf: 14.12.2018). [zitiert: Ethik–Kommission]

Europäischer Datenschutzausschuss (EDSA), Erklärung zur Überarbeitung der ePrivacy–Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre von Personen im Hinblick auf die Geheimhaltung und die Vertraulichkeit ihrer Kommunikation, 25.05.2018, online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_de.pdf (letzter Abruf: 20.10.2018). [zitiert: EDSA, Erklärung zur ePrivacy–VO]

Europäischer Datenschutzausschuss (EDSA), Endorsement 1/2018 of GDPR Article 29 Working Party documents, abrufbar: https://edpb.europa.eu/node/89 (letzter Abruf: 14.11.2018). [zitiert: EDSA, Endorsement 1/2018]

Europäischer Datenschutzbeauftragter (EDSB), Zusammenfassung der Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-VO), 2017/C 234/03, 20.07.2017, abrufbar: https://edps.europa.eu/sites/edp/files/publication/17-07-20_eprivacyreg_ex_summ_de.pdf (letzter Abruf: 04.12.2018). [EDSB, Stellungnahme ePrivacy–VO]

Europäischer Datenschutzbeauftragter (EDSB), Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, 11.04.2017, abrufbar: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf (letzter Abruf: 20.11.2018). [zitiert: EDSB, Toolkit Erforderlichkeit]

Europäische Kommission, C (2018) 5356 final, Antwort an das nationale Parlament, 03.08.2018, abrufbar: http://ec.europa.eu/transparency/regdoc/rep/3/2018/DE/C-2018-5356-F1-DE-MAIN-PART-1.PDF (letzter Abruf: 09.11.2018). [zitiert: Europäische Kommission, C (2018) 5356 final]

Europäische Kommission, Access to in-vehicle data and resources, Final Report 2017, abrufbar: https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf (letzter Abruf: 03.12.2018). [zitiert: Europäische Kommission, Access to in-vehicle data]

Europäische Kommission, COM (2017) 9 final, Aufbau einer europäischen Datenwirtschaft, abrufbar: https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-9-F1-DE-

MAIN-PART-1.PDF (letzer Abruf: 14.12.2018).
[zitiert: Europäische Kommission, COM (2017) 9 final]

Europäische Kommission, COM(2016) 766 final, Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme - ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität, abrufbar: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0766&from=DE (letzer Abruf: 14.12.2018).
[zitiert: Europäische Kommission, COM (2016) 766 final]

Forum Privatheit, (Hrsg.: Friedewald, Michael/ Ammicht Quinn, Regina/ Hansen, Marit/ Heesen, Jessica/ Hess, Thomas/ Lamla, Jörn/ Matt, Christian/ Roßnagel, Alexander/ Trepte, Sabine/ Waidner, Michael), White Paper Datenschutz-Folgenabschätzung, 3. Auflage, Karlsruhe, November 2017, abrufbar: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (letzter Abruf: 10.12.2018).
[zitiert: Forum Privatheit, DSFA].

Gao, Xianyi/ Firner, Bernhard/ Sugrim, Shridatt/ Kaiser-Pendergrast, Victor/ Yang, Yulong/ Lindqvist, Janne, Elastic Pathing: Your Speed is Enough to Track you, in: UbiComp '14 Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014, ACM, 975-986, abrufbar: http://www.winlab.rutgers.edu/~janne/elasticpathing-ubicomp14.pdf (letzter Abruf: 20.11.2018).
[zitiert: Gao et al., 2014]

Goldhammer, Michael, Zur Neudefinition des Geschäftsgeheimnisses als Chance für das öffentliche Recht, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2017, 1809–1814.
[zitiert: Goldhammer, NVwZ 2017, 1809]

Grünwald, Andreas/Nüßing, Christoph, Machine To Machine (M2M)–Kommunikation – Regulatorische Fragen bei der Kommunikation im Internet der Dinge, Multimedia und Recht (MMR) 2015, 378–383.
[Grünwald/Nüßing, MMR 2015, 378]

Hansen, Marit, Das Netz im Auto und das Auto im Netz – Herausforderungen für eine datenschutzgerechte Gestaltung vernetzter Fahrzeuge, in: Datenschutz und Datensicherheit (DuD) 2015, 367–371.
[zitiert: Hansen, DuD 2015]

Hansen, Marit/ Bieker, Felix/ Deibler, Daniel/ Obersteller, Hannah/ Schlehahn, Eva/ Zwingelberg, Harald, Legal Data Protection Considerations, in: Rannenberg/ Carmenisch/ Sabouri (Hrsg.), Attribute–based Credentials for Trust, Frankfurt/

Zürich Oktober 2014, 143–160.
[zitiert: Hansen et al, in: ABC4Trust, 143]

Hansen, Marit/ Hansen, Markus/ Häuser, Marita/ Janneck, Kai/ Krasemann, Henry/ Meints, Martin/ Meissner, Sebastian/ Raguse, Maren/ Rost Martin/ Schallaböck, Jan/ Clauß, Sebastian/ Steinbrecher, Sandra/ Pfitzmann, Andreas, Verkettung digitaler Identitäten, Untersuchung im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel 2007, abrufbar: https://www.datenschutzzentrum.de/uploads/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf1.pdf (letzter Abruf: 13.11.2018).
[Hansen et al., Verkettung digitaler Identitäten]

Hoeren, Thomas, Ein Treuhandmodell für Autodaten? - § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierten Fahrfunktionen, in: Neue Zeitschrift für Verkehrsrecht (NZV) 2018, 153 - 155.

Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation (International Working Group on Data Protection in Telecommunications, IWGDPT), Working Paper Vernetzte Fahrzeuge, Budapest (Ungarn) 2018, abrufbar: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/ (letzter Abruf: 24.10.2018).
[zitiert: IWGDPT, vernetzte Fahrzeuge]

Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation (International Working Group on Data Protection in Telecommunications, IWGDPT), Arbeitspapier zur Verfolgung des Aufenthaltsortes auf der Basis von Meldungen von Mobilfunkgeräten, Berlin 2015. abrufbar: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/ (letzter Abruf: 10.10.2018).
[zitiert: IWGDP, Verfolgung von Aufenthaltsorten]

Jandt, Silke, Spezifischer Datenschutz für Telemedien und die DSGVO zwischen Rechtssetzung und Rechtsanwendung, in: Zeitschrift für Datenschutz (ZD) 2018, 405–408.
[zitiert: Jandt, ZD 2018, 405]

Jourdan, Frank/ Matschi, Helmut, Automatisiertes Fahren – Wie weit kann die Technik den Fahrer ersetzen? Entwickler oder Gesetzgeber, wer gibt die Richtung vor?, in: Neue Zeitschrift für Verkehrsrecht (NZV) 2015, 26 – 29.
[zitiert: Jourdan/ Matschi, NZV 2015, 26]

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), AK Technik (Hrsg.), Das Standard–Datenschutzmodell (SDM), eine Methode zur Datenschutzberatung und –Prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 – Erprobungsfassung, von der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 25./26. April

2018 in Düsseldorf einstimmig beschlossen, abrufbar: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf (letzter Abruf: 10.12.2018).
[zitiert: DSK, SDM, V.1.1]

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Düsseldorf 26. April 2018, abrufbar: https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf (letzter Abruf: 25.10.2018).
[zitiert: DSK, Positionsbestimmung TMG].

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier (KP) Nr. 16, Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO abrufbar: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_16_Gemeinsame-Verantwortliche.pdf (letzter Abruf: 25.10.2018).
[zitiert: DSK, KP Nr. 16]

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, abrufbar: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf (letzter Abruf: 30.10.2018).
[zitiert: DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten]

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Marktortprinzip: Regelungen für außereuropäische Unternehmen, Kurzpapier Nr. 7, abrufbar: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_7.pdf (letzter Abruf: 20.11.2018).
[zitiert: DSK, KP Nr. 7]

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK),Kurzpapier Nr. 5, abrufbar: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_5_Datenschutz-Folgenabschaetzung.pdf (letzter Abruf: 27.12.2017)
[zitiert: DSK, KP Nr. 5].

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK), Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik), Orientierungshilfe – Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft, V.1.01 (Stand: 26.10.2012).
[zitiert: DSK, AK Technik 2012]

Klink-Straub, Judith/ Straub, Tobias, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, in: Neue Juristische Wochenschrift (NJW) 2018, 3201–3206.
[zitiert: Klink-Straub/ Straub, NJW 2018, 3201]

Klink-Straub, Judith/ Straub, Tobias, Vernetzte Fahrzeuge – portable Daten. Das Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO, in: Zeitschrift für Datenschutz (ZD) 2018,459–463.
[zitiert: Klink-Straub/ Straub, ZD 2018, 459]

Kühling, Jürgen/ Buchner, Benedikt (Hrsg.), Datenschutz–Grundverordnung (DSGVO), Kommentar, 1. Auflage, München 2017.
[zitiert: Kühling/ Buchner – *Bearbeiter*, DSGVO]

Kühling, Jürgen/ Drechsler, Stefan, Alles „acte clair"? – Die Vorlage an den EuGH als Chance, in: Neue Juristische Wochenschrift (NJW) 2017, 2950–2955.
[zitiert: Kühling/Drechsler, NJW 2017, 2950]

Kühling, Jürgen/ Martini, Mario/ Heberlein, Johanna/ Kühl, Benjamin/ Nink, David/ Weinzierl, Quirin/ Wenzel, Michael, Die Datenschutz–Grundverordnung und das nationale Recht, erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016.
[zitiert: Kühling/Martini et al, 2016]

Kühling, Jürgen/ Sackmann, Florian, Datenschutzordnung 2018 – nach der Reform ist vor der Reform?!, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2018, 681–686.
[zitiert: Kühling/Sackmann, NVwZ 2018, 681]

König, Carsten, Die gesetzlichen Neuregelungen zum automatisierten Fahren, in: Neue Zeitschrift für Verkehrsrecht (NVZ) 2017, 123 127.
[zitiert: König, NVZ 2017]

Lüdemann, Volker/ Sengstacken, Christin, Lebensretter eCall: Türöffner für neue Telematik-Dienstleistungen, in: Recht der Datenverarbeitung (RDV) 2014, 177–182.
[zitiert: Lüdemann/ Sengstacken, RDV 2014, 177]

Lüdemann, Volker/Ortmann, Manuel Christian/Pokrant,Patrick, Datenschutz beim Smart Metering – Das geplante Messstellenbetriebsgesetz (MbSG) auf dem Prüfstand, in: Recht der Datenverarbeitung (RDV) 2016, 125-133.
[zitiert: Lüdemann/Ortmann/Pokrant, RDV 2016]

Lüttringhaus, Jan D., Vertragsfreiheit und Materialisierung im Europäischen Binnenmarkt – Die Verbürgerung und Materialisierung unionaler Vertragsfreiheit im Zusammenspiel von EU-Privatrecht, BGB und ZPO (Beiträge zum ausländischen und internationalen Privatrecht 120), Tübingen 2018, Habilitationsschrift,

Universität Hamburg 2017.
[zitiert: Lüttringhaus, 2018]

Maunz, Theodor/ Dürig, Günther (Hrsg.), Grundgesetz-Kommentar, 84. Ergänzungslieferung August 2018.
[Maunz/Dürig–*Bearbeiter*, GG]

Bundesregierung, Maßnahmenplan der Bundesregierung zum Bericht der Ethik-Kommission, 25.08.2017, BT-Drucks. 18/13500.
[zitiert: BReg, Maßnahmenplan zum Bericht der Ethik-Kommission]

Michalevsky, Yan/ Nakibly, Gabi/ Schulman, Aaron/ Arumugam, Gunaa/ Veerapandian, Dan Boneh, PowerSpy: Location Tracking using Mobile Device Power Analysis, in: Proceedings of the 24th USENIX Security Symposium, Washington D.C 2015, abrufbar: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-michalevsky.pdf (letzter Abruf: 23.11.2018),
[zitiert: Michaelsky et. al. 2015]

Montjoye, Y.-A. de/ Hidalgo, C.A./ Verleysen, M./ Blondel, V.D., Unique in the Crowd: The privacy bounds of human mobility, in: Sci. Rep.3, 1376; DOI:10.1038/srep01376 (2013), online: https://www.nature.com/articles/srep01376.pdf (letzter Abruf: 01.11.2018).
[zitiert: Montjoye et. al., 2013]

Nürnberger, Stefan, Datenverarbeitung im (vernetzten) Fahrzeug, in: Datenschutz und Datensicherheit (DuD) 2018, 79–82.
[zitiert: Nürnberger, DuD 2018]

Paal, Boris/ Pauly, Daniel (Hrsg.), Beck'sche Kompakt–Kommentare Datenschutzgrundverordnung Bundesdatenschutzgesetz, 2. Aufl., München 2018.
[zitiert: Paal/Pauly-*Bearbeiter*, DSGVO]

Pfitzmann, Andreas/ Hansen, Marit, A Terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, Version v0.34, August 2010, abrufbar: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (letzter Abruf: 10.12.2018).
[zitiert: Pfitzmann/ Hansen, Anon Terminology v.034]

Robrahn, Rasmus/Bremert, Benjamin, Interessenskonflikte im Datenschutzrecht, in: Zeitschrift für Datenschutz (ZD) 2018, 291–297.
[zitiert: Robrahn/Bremert, ZD 2018]

Roßnagel, Alexander, Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? Bedeutung der Grundsätze für die datenschutzrechtliche

Praxis, in: Zeitschrift für Datenschutz (ZD) 2018, 339 - 344.
[zitiert: Roßnagel, ZD 2018, 339]

Roßnagel, Alexander, Pseudonymisierung personenbezogener Daten – Ein zentrales Instrument im Datenschutz nach der DS-GVO, in: Zeitschrift für Datenschutz (ZD) 2018, 243–247.
[zitiert: Roßnagel, ZD 2018, 243]

Roßnagel, Alexander, Kontinuität oder Innovation? Der deutsche Spielraum in der Anpassung des bereichsspezifischen Datenschutzrechts, in: Datenschutz und Datensicherheit (DuD) 2018, 477–481.
[zitiert: Roßnagel, DuD 2018, 447]

Schmid, Alexander/ Wessels, Ferdinand, Event Data Recordning für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG, in: Neue Zeitschrift für Verkehrsrecht (NVZ) 2017, 357 – 373.
[zitiert: Schmid/ Wessels, NVZ 2017, 357]

Strauß, Stefan, Identifizierbarkeit in soziotechnischen Systemen – Eine Typologie von Identitätsinformation für systematisches Privacy Impact Assessment, in: Datenschutz und Datensicherheit (DuD) 2018, 497–501.
[zitiert: Strauß, DuD 2018, 497]

Stender-Vorwachs, Jutta/ Steege, Hans, Kleine SIM-Karte –große Konsequenz: Automobilhersteller als TK-Anbieter?, in: Multimedia und Recht (MMR) 2018, 212.
[zitiert: Stender-Vorwachs/Steege, MMR 2018, 212]

Spindler, Gerald/ Lönner, Andreas/ Nink, Judith, Verantwortlichkeiten von IT–Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, Göttingen 2007, abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=3 (letzter Abruf: 13.12.2018).
[Spindler 2007]

Tinnefeld, Marie–Theres/Conrad, Isabell, Die selbstbestimmte Einwilligung im europäischen Recht, Voraussetzungen und Probleme, in: Zeitschrift für Datenschutz (ZD) 2018.
[zitiert: Tinnefeld/ Conrad, ZD 2018]

Troncoso, Carmela/Costa-Montenegro, Enrique/Diaz, Claudia/Schiffner, Stefan, On the difficulty of achieving anonymity for Vehicle-2-X-communication, in: Computer Networks Nr. 55 (14), 2011, S. 3199–3210, abstract abrufbar: https://doi.org/10.1016/j.comnet.2011.05.004 (letzter Abruf: 20.11.2018).
[zitiert: Troncoso et al., 2011]

Verband der Automobilindustrie (Hrsg.), Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, gemeinsame Erklärung

mit der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) Berlin/Schwerin, 26.01.2016, abrufbar: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2016/ErklaerungDSK_VDA_VernetzteKfz.html;jsessionid=D4406830416A2FC3FB57B89D48042C47.2_cid344?nn=5217320 (letzter Abruf: 19.11.2018).
[zitiert: VDA und DSK, Gemeinsame Erklärung]

Verband der Automobilindustrie e. V. (Hrsg.), Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten: Das Konzept „NEVADA-Share & Secure“, 24.10.2017, abrufbar: https://www.vda.de/de/themen/innovation-und-technik/datensicherheit/fahrzeug-schuetzen.html (letzter Abruf: 24.10.2018).
[zitiert: VDA, Konzept NEVADA]

Verband der Automobilindustrie e.V. (Hrsg.), Position: Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten, 19.09.2016, abrufbar: https://www.vda.de/de/themen/innovation-und-technik/vernetzung/Zugang-zum-Fahrzeug-und-zu-im-Fahrzeug-generierten-Daten.html (letzter Abruf: 20.11.2018).
[zitiert: VDA, Position Zugang]

Verband der Automobilindustrie (Hrsg.), Datenschutzprinzipien für vernetzte Fahrzeuge, 03.11.2014, abrufbar: https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html (letzter Abruf: 20.11.2018).
[zitiert: VDA, Datenschutzprinzipien]

Wagner, Bernd, Disruption der Verantwortlichkeit – Private Nutzer als datenschutzrechtliche Verantwortliche im Internet of Things, in: Zeitschrift für Datenschutz (ZD) 2018, 307 – 312.
[zitiert: Wagner, ZD 2018]

Watanabe, Takuya; Akiyama, Mitsuaki; Mori, Tatsuya, Tracking the Human Mobility Using Mobile Device Sensors, IEICE TRANS. INF. & SYST., VOL.E100–D, NO.8 AUGUST 2017, 1680, online: https://www.jstage.jst.go.jp/article/transinf/E100.D/8/E100.D_2016ICP0022/_pdf (letzter Abruf: 01.11.2018).
[zitiert: Watanabe et. al. 2017]

Weichert, Thilo, Der Personenbezug von Kfz–Daten, in: Neue Zeitschrift für Verkehrsrecht (NZV) 2017, 507–513.
[zitiert: Weichert, NZV 2017, 507]

Weichert, Thilo, Car-to-Car-Communikation zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung, in: Straßenverkehrsrecht (SVR) 2016, 361 –367.
[zitiert: Weichert, SVR 2016]

Weichert, Thilo, Datenschutz im Auto – Teil 1, das Kfz als großes Smartphone mit Rädern, in: Straßenverkehrsrecht (SVR) 2014, 201-207.
[zitiert: Weichert, SVR 2014, 201]

Weichert, Thilo, Datenschutz im Auto – Teil 2, das Kfz als großes Smartphone mit Rädern, in: Straßenverkehrsrecht (SVR) 2014, 241-247.
[zitiert: Weichert, SVR 2014, 241]

Wissenschaftliche Dienste des Bundestages (Hrsg.), Zulässigkeit der Verwendung von Daten aus dem Maut-System zur Strafverfolgung (15.12.2005), abrufbar: https://www.bundestag.de/blob/424352/f9b2073dabf278848d70c4ee079eaa75/wf-iii-358-05-pdf-data.pdf (letzter Abruf: 15.09.2018).
[zitiert: WD BT, Mautdaten]

Wissenschaftliche Dienste des Deutschen Bundestages (Hrsg.), Autonomes und automatisiertes Fahren auf der Straße – rechtlicher Rahmen, Ausarbeitung v. 22.05.2018, WD 7 – 3000 – 111/18, abrufbar: https://www.bundestag.de/blob/562790/c12af1873384bcd1f8604334f97ee4b9/wd-7-111-18-pdf-data.pdf (letzter Abruf: 20.11.2018).
[zitiert: WD BT, autonomes und automatisiertes Fahren]

Zang, Hui/ Bolot, Jean, Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study, MobiCom '11 Proceedings of the 17th annual international conference on Mobile computing and networking, 2011, ACM, 145-156, abrufbar: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.651.44&rep=rep1&type=pdf (letzter Abruf: 23.11.2018).
[zitiert: Zang/ Bolot, 2011]