iKoPA Integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge

Deliverable 3.1

Datenschutz bei vernetzten Fahrzeugen

Version number	1.0
Dissemination level	Public
Project Coordination	htw saar
Due date	2017-05-31
Date of preparation	2017-05-29

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:

Rasmus Robrahn – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Revision and History chart

Version	Date	Description
0.1	2016-06-08	Document creation, first version
0.2	2017-04-07	First review version
0.3	2017-04-26	Second review version
0.4	2017-05-24	Review comments included
1.0	2017-05-29	Final version 1.0

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 EINLEITUNG UND ZUSAMMENFASSUNG

Vernetzte und automatisierte Fahrzeuge werfen eine Vielzahl rechtlicher Fragestellungen auf. Viel diskutiert werden Haftungsfragen, also wer für Schäden haftet, die durch automatisierte Fahrzeuge verursacht werden. In der Literatur werden die datenschutzrechtlichen Aspekte der Vernetzung weniger intensiv diskutiert. Dies ist verwunderlich, da die Auswirkungen auf das Schutzgut des Datenschutzrechts, die informationelle Selbstbestimmung ganz erheblich sein können. Deshalb verwundert es, dass die Diskussion vielfach unter dem Stichwort „Wem gehören die Fahrzeugdaten?“[1] geführt wird, handelt es sich dabei doch um eine Frage, die weder in Rechtsprechung noch in der bisherigen datenschutzrechtlichen Literatur mit einer dogmatischen Grundlage unterfüttert wurden. Dieses Deliverable möchte einen Beitrag dazu leisten, diese Lücke im Diskurs zu schließen, indem es eine umfassende datenschutzrechtliche Analyse vor dem Hintergrund der informationellen Selbstbestimmung leistet.

Das vernetzte und automatisierte Fahrzeug fügt sich in einen Trend zur zunehmenden Digitalisierung von Alltagsgegenständen ein, die häufig als „smart“ bezeichnet bzw. dem „Internet of Things“ zugerechnet werden. Mit der Digitalisierung dieser Alltagsgegenstände geht auch eine immer umfassendere digitale Erfassung unseres Alltags einher. Die Daten erreichen Qualitäten und Quantitäten in neuen Dimensionen. Häufig geschieht dies sogar ohne ausreichende Transparenz für die Nutzer. Die Gefahren, die sich daraus für die informationelle Selbstbestimmung ergeben sind enorm.[2] Der Datenschutz hat in diesen Spannungsverhältnissen die Aufgabe, die informationelle Selbstbestimmung derer zu schützen, deren personenbezogene Daten verarbeitet werden. Erst kürzlich hat das VG Hamburg in einem Verfahren zur Zulässigkeit der Weitergabe von Nutzerdaten von WhatsApp an Facebook deutliche Worte zur gesellschaftlichen Bedeutung des Datenschutzes gefunden:

„Denn die geplante Datenerhebung ist von gesellschaftlicher Relevanz. Insgesamt sind ca. 35 Millionen Nutzer betroffen. Angesichts dieser erheblichen Anzahl an Personen, die von der Datenerhebung betroffen sein wird, besteht die Gefahr, dass die vorläufige Erhebung zu einer Gesellschaftsordnung beiträgt, in der Bürger nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß. Dies ist mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren (vgl. BVerfG, Urt. v. 15.12.1983, a.a.O., Rn. 148).“[3]

---

[1] Vgl. Leupold/Wiebe, CW 2016; Störing, c’t 2016, 128 ff.; Hoeren, MMR 2013, 486 ff; Schwartmann/Hentsch, RDV 2015, 221 ff.

[2] Karaboga et al., Das versteckte Internet, S. 33 ff.; Auch in den USA gibt es Bestrebungen, den Datenschutz bei vernetzten Fahrzeugen strenger zu regeln, vgl. Keppeler, RDV 2015, 299 ff.

[3] VG Hamburg, Beschl. v. 24.04.2017, Az. 13 E 5912/16 S. 38.

In diese Entwicklung fügt sich auch das vernetzte und datenverarbeitende Fahrzeug ein. Innovative Konzepte zur Erhöhung der Verkehrssicherheit, des Komforts im Straßenverkehr, einem verbesserten Umweltschutz, die Reduzierung von Staus und zur Reduzierung von Parkplatzproblemen in den Innenstädten sind natürlich ausdrücklich zu begrüßen. Es sind aber intelligente Lösungen zu finden, die diese Ziele erreichen und gleichzeitig ein hohes Datenschutzniveau sichern, also die noch vorzustellenden Gewährleistungsziele des Standard-Datenschutzmodells erfüllen. Man darf zuversichtlich sein, dass es so gelingt, die gesellschaftlichen Vorteile des vernetzten und automatisierten Fahrens nicht mit großen Abstrichen beim Datenschutz zu erkaufen.

Erst dann, wenn diese Ziele der Datenverarbeitung rund um das vernetzte Fahrzeug und der Datenschutz wirklich in einen Konflikt kommen, ist im konkreten Fall eine Abwägung vorzunehmen.

Nachfolgend werden daher zunächst die datenschutzrechtlichen Vorgaben dargestellt und anschließend die Methodik erläutert, aus der die Datenschutzanforderungen des iKoPA Deliverables D1v1 entwickelt wurden. Im rechtlichen Teil wird dargestellt, welchen verfassungsrechtlichen Hintergrund das Datenschutzrecht hat, welche Gesetze unter welchen Bedingungen zur Anwendung kommen und welche Vorgaben diese Gesetze machen. Im technisch-organisatorischen Teil wird dargestellt, wird das Standard-Datenschutzmodell dargestellt, mit dem die Datenschutzanforderungen in iKoPA Deliverable D1v1 erstellt wurden.

2 NATIONALES DATENSCHUTZRECHT

2.1 Verfassungsrechtlicher Hintergrund

Das vernetzte und automatisierte Fahrzeug wirft eine Reihe grundrechtlich relevanter Fragestellungen auf. Am prominentesten ist die Diskussion um die Reaktion automatisierter Fahrzeuge auf unmittelbar bevorstehende Unfälle.[4] Darüber hinaus wird aber eine Vielzahl von miteinander kollidierenden Grundrechten von vernetzten und automatisierten Fahrzeugen berührt. Diese sind miteinander in einen Ausgleich zu bringen.[5] Im Folgenden wird dargestellt, welche dieser Grundrechte aus Sicht des Datenschutzes eine besondere Rolle spielen und was durch diese Grundrechte geschützt wird.

Kenntnisse der Grundrechte sind für die korrekte Anwendung des Datenschutzrechts unabdingbar. Nach Art. 1 Abs. 3 GG binden die Grundrechte Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht. Die unmittelbare Bindung staatlicher Gewalt an die Grundrechte ist unabdingbar für einen effektiven Schutz der Grundrechte[6] und ist lückenlos.[7] Die unmittelbare Bindung der Exekutive an die Verfassung ist auch in Art. 20 Abs. 3 GG vorgesehen. Sie kommt insbesondere dann zur Geltung, wenn Behörden Ermessen eingeräumt wird oder wenn Behörden und Gerichte auslegungsbedürftige Rechtsbegriffe vorfinden.[8] Wie noch zu zeigen sein wird, ist das Datenschutzrecht zugunsten technikneutraler Regelungen stark von solchen auslegungsbedürftigen Rechtsbegriffen durchzogen. Obwohl betont werden muss, dass die Verfassung insbesondere dem Gesetzgeber[9] aber auch der Verwaltung[10] Spielräume eröffnet, ist bei so hochgradig abstraktem Recht wie dem Datenschutzrecht ebenfalls zu betonen, dass die Verfassung diese Spielräume der Behörden und Gerichte bei der Auslegung des Datenschutzrechts begrenzt.

---

[4] Das BMVI hat zu dieser Frage eine Ethikkommission unter der Leitung des ehemaligen Bundesverfassungsrichters Prof. Dr. Dr. Udo Di Fabio eingesetzt. Vgl. https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2016/157-dobrindt-ethikkommission.html

[5] Vgl. Roßnagel, DuD 2015, 353, 353 ff.

[6] Maunz/Dürig/Herdegen, GG, Art. 1 Abs. 3 Rn. 3.

[7] Maunz/Dürig/Herdegen, GG, Art. 1 Abs. 3 Rn. 11.

[8] Maunz/Dürig/Grzeszick, GG, Art. 20 Rn. 21.

[9] Maunz/Dürig/Grzeszick, GG, Art. 20 Rn. 19.

[10] BVerfGE 46, 160, 164.

2.1.1 Das Grundrecht auf informationelle Selbstbestimmung

Das deutsche Datenschutzrecht und seine Auslegung werden wesentlich durch das Grundrecht auf informationelle Selbstbestimmung geprägt. Dieses Grundrecht wird aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs.1 GG hergeleitet und stellt eine Fallgruppe des allgemeinen Persönlichkeitsrechts dar. Durch seine Nähe zur Menschenwürde (Art. 1 Abs. 1 GG) verfügt es schon bei einer abstrakten Sichtweise über ein erhöhtes Gewicht.[11] Dieses allgemeine Persönlichkeitsrecht greift dort, wo ein Schutz durch spezielle Grundrechte fehlt, aber durch die Bedeutung für die freie Entfaltung der Persönlichkeit ein besonderer Schutzbedarf besteht.[12] Mit dem Volkszählungsurteil hat das Bundesverfassungsgericht schon 1983 die informationelle Selbstbestimmung als einen solchen Bereich anerkannt.[13]

„Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[14]

[11] Maunz/Dürig/Di Fabio, GG, Art. 2 Rn. 130.

[12] Maunz/Dürig/Di Fabio, GG, Art. 2 Rn. 127.

[13] BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83.

[14] BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83, Rn. 172.

Das Bundesverfassungsgericht führt weiter aus, die freie Entfaltung der Persönlichkeit setze „unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“[15]

Das Grundrecht gewährt dem Bürger gegenüber dem Staat einerseits einen Abwehranspruch gegen Eingriffe in den Schutzbereich des Grundrechts, andererseits ermöglicht es ihm auch, vom Staat den Schutz seiner informationellen Selbstbestimmung zu verlangen. Einer solchen Schutzpflicht kann der Staat insbesondere nachkommen, indem er einfachrechtliche Normen zum Schutz personenbezogener Daten schafft.[16]

Das Grundrecht auf informationelle Selbstbestimmung stellt somit das Fundament des deutschen Datenschutzrechts dar. Folgerichtig erklärt § 1 Abs. 1 BDSG es zum Zweck des Bundesdatenschutzgesetzes, den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts zu schützen. Aufgabe des Datenschutzes beim vernetzten und automatisierten Fahrzeug muss es daher sein, das Recht auf informationelle Selbstbestimmung in diesem Bereich umzusetzen.

2.1.2 Grundrecht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme

Daneben kann auch das Recht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme betroffen sein, welches ebenfalls eine Fallgruppe des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG darstellt.

„Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.“[17]

Das BVerfG hat die Notwendigkeit für den persönlichkeitsrechtlichen Schutz von informationstechnischen Systemen mit deren Bedeutung für die

[15] BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83, Rn.173.

[16] Zum Spielraum bei Schutzpflichten: BVerfGE 46, 160.

[17] BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07, Rn. 204.

Persönlichkeitsentfaltung begründet[18] und darüber hinaus bereits 2008 erkannt, dass in Hinblick auf die zunehmende Vernetzung von Alltagsgegenständen von dem Begriff der informationstechnischen Systeme nicht nur Personalcomputer erfasst sind:

„Die Relevanz der Informationstechnik für die Lebensgestaltung des Einzelnen erschöpft sich nicht in der größeren Verbreitung und Leistungsfähigkeit von Personalcomputern. Daneben enthalten zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten. So liegt es beispielsweise zunehmend bei Telekommunikationsgeräten oder elektronischen Geräten, die in Wohnungen oder Kraftfahrzeugen enthalten sind.“[19]

Die eigenständige Bedeutung des Grundrechts auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme in Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung wird vom BVerfG damit begründet, dass das Grundrecht auf informationelle Selbstbestimmung dort keinen ausreichenden Schutz gewährt, wo ein Nutzer einem System allein durch die Nutzung Daten anvertraut. Schon das Verschaffen des Zugriffs auf diese Systeme stellt einen Eingriff in das allgemeine Persönlichkeitsrecht dar, ohne dass es einer Erhebung von personenbezogenen Daten bedarf.[20] Das gilt für alle Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.“[21]

Wie auch das Grundrecht auf informationelle Selbstbestimmung verfügt das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme als Ausprägung des allgemeinen Persönlichkeitsrechts über eine schutzrechtliche Dimension. Dem Staat obliegt die Pflicht, die Grundrechtsträger vor Beeinträchtigungen ihres allgemeinen Persönlichkeitsrechts auch durch private Dritte zu schützen. [22] Obwohl der Staat bei dem „wie“ des Schutzes über weite Spielräume verfügt,[23] könnte man fragen, ob der Staat seiner Schutzpflicht für das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme in Hinblick auf vernetzte Fahrzeuge bislang ausreichend

[18] BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07, Rn. 170 ff.

[19] BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07, Rn. 173.

[20] BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07, Rn. 201.

[21] BVerfG, Urt. v. 27.02.2008, Az. 1 BvR 370/07, Rn. 203.

[22] Roßnagel/Schnabel, NJW 2008, 3534, 3535; Maunz/Dürig/Di Fabio, GG, Art. 2 Rn. 135.

[23] BVerfG, NJW 1977, 2255, 2255.

nachkommt, [24] zumal dieses Grundrecht durch die zunehmende Verarbeitung persönlichkeitsrechtlich relevanter Daten im Fahrzeug an Gewicht gewinnt.[25]

2.1.3 Fernmeldegeheimnis

Das Fernmeldegeheimnis ist nach Art. 10 GG geschützt. Es schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mittels Telekommunikationsverkehrs und erfasst nicht nur die Inhalte der Kommunikation sondern auch die Umstände der Kommunikation, also auch wann und wie oft zwischen bestimmten Personen Telekommunikation stattgefunden hat.[26] Es schützt darüber hinaus aber auch „den Informations- und Datenverarbeitungsprozeß, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt, und den Gebrauch, der von den erlangten Kenntnissen gemacht wird“.[27]

Das Grundrecht schützt daher im Rahmen des vernetzten Fahrzeugs insbesondere die Kommunikationsvorgänge zwischen den Fahrzeugen und Backendservern, der Schutz endet aber grundsätzlich mit Abschluss des Kommunikationsvorgangs.

2.1.4 Weitere Grundrechte

Beim vernetzten Fahrzeug spielen aber nicht nur diese für Datenverarbeitungen typischen Grundrechte eine Rolle. Es geht daneben um das Grundrecht auf Fortbewegungsfreiheit, das Grundrecht auf körperliche Unversehrtheit, die Sicherheit des Eigentums, die Berufsausübung, die unternehmerische Freiheit und die Forschungsfreiheit,[28] die hier nicht weiter vertieft werden sollen.

2.2 Europarechtlicher Hintergrund

Neben den deutschen verfassungsrechtlichen Bestimmungen spielt auch der europarechtliche Hintergrund des Datenschutzrechts eine große Rolle.

Die Charta der Grundrechte der Europäischen Union verlangt in Art. 8 den Schutz personenbezogener Daten. Also ist auch im europäischen Primärrecht der grundrechtliche Schutz personenbezogener Daten gewährleistet. Adressaten des

[24] Einen Überblick über Regelungen zur IT-Sicherheit im Automobilbereich findet sich bei Bartelt et al., DuD 2017, 211, 214 ff.

[25] Roßnagel, SVR 2014, 281, 283.

[26] BVerfG, Urt. v. 02.03.2010, Az. 1 BvR 256/08, Rn. 189 m.w.N.

[27] BVerfGE 130, 313, 359.

[28] Roßnagel, DuD 2015, 353, 354.

Grundrechts sind primär die Union und ihre Stellen. Bei der Durchführung von Unionsrecht sind auch die Mitgliedsstaaten an Art. 8 GrCh gebunden.[29]

Mit der 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 hat der europäische Gesetzgeber den Mitgliedsstaaten einen Handlungsrahmen vorgegeben, innerhalb dessen sie den Datenschutz zu regeln haben. Deutschland hatte zu diesem Zeitpunkt bereits ein Bundesdatenschutzgesetz, musste dies aber an die europäischen Vorgaben anpassen. [30]

2.3 Anwendbares einfachgesetzliches Recht

Es kommen mehrere Gesetze mit datenschutzrechtlichen Normen für die Anwendung auf das vernetzte Fahrzeug in Betracht. Dabei handelt es sich um das Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze. Deshalb wird nun in einem ersten Schritt aufgezeigt, welches Recht unter welchen Bedingungen und für welche Teilbereiche des vernetzten Verkehrs anwendbar ist.

2.3.1 IVSG

Zunächst kommt das Gesetz über intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG) als anwendbares Recht in Betracht. Titel und Geltungsbereich sind identisch, das Gesetz gilt für intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern, § 1 IVSG. Bei intelligenten Verkehrssystemen handelt es sich nach der Legaldefinition des § 2 Nr. 1 IVSG um „Systeme bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an Schnittstellen zu anderen Verkehrsträgern eingesetzt werden“. Daher hat das IVSG einen sehr weiten Anwendungsbereich, der alle modernen datenverarbeitenden Technologien im Kraftfahrzeug erfasst. In § 3 S. 2 IVSG wird hinsichtlich datenschutzrechtlicher Erlaubnisnormen aber lediglich auf bundesgesetzliche Regelungen verwiesen, die Norm selbst ist kein eigener Erlaubnistatbestand. [31] Daher hat dieses Gesetz für die nachfolgenden datenschutzrechtlichen Betrachtungen keine weitere Relevanz.

[29] Jarass, GrCh, Art. 8 Rn. 3.

[30] Vgl. Simitis, in: Simitis, BDSG, Einl. Rn. 89 ff.

[31] Kremer, RDV 2014, 240, 246.

2.3.2 TKG

Als weiteres anwendbares Recht kommen insbesondere das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) in Betracht.

Das Fernmeldegeheimnis und der Datenschutz sind in den §§ 88 ff. TKG geregelt. Das Fernmeldegeheimnis richtet sich nach § 88 Abs. 2 TKG an jeden Diensteanbieter im Sinne von § 3 Nr. 6 TKG. Die Vorschriften zum Datenschutz im TKG in den §§ 91 ff. TKG sind nach § 91 Abs. 1 S. 1 TKG dann anwendbar, wenn eine Erhebung oder Verwendung von personenbezogenen Daten „durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken“ stattfindet.

Diensteanbieter im telekommunikationsrechtlichen Sinne sind nach § 3 Nr. 6 TKG diejenigen, die ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung dieser Dienste mitwirken. Für die Geschäftsmäßigkeit ist keine Gewinnerzielungsabsicht erforderlich. Es ist nach § 3 Nr. 10 TKG ausreichend, dass ein Angebot auf Dauer ausgerichtet ist und eine gewisse Häufigkeit aufweist.[32] Telekommunikationsdienste sind wiederum in § 3 Nr. 24 TKG definiert. Es handelt sich demnach um „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen.“ Ein Telekommunikationsdienst besteht also im Schwerpunkt im technischen Transport, nicht in einer inhaltlichen Leistung.[33] In der iKoPA-Architektur finden sich die Telekommunikationsdienste auf der Ebene der Communication Network plane.[34] Das CellularNetwork und das IRS Network sind Telekommunikationsdienste. Bei dem CellularNetwork handelt es sich um das Mobilfunknetz, über das Signale transportiert werden. Bei dem IRSNetwork handelt es sich um ein Netzwerk aus Stationen, die sich an den Straßen befinden und Informationen mittels des WLAN-Standards IEEE 802.11p (ITS G5), der für Anwendungen in intelligenten Verkehrssystemen entwickelt wurde, verbreiten. Dieses Netzwerk dient damit lediglich der Übertragung von Signalen.

Nach § 91 Abs. 1 S. 2 TKG sind auch juristische Personen von den datenschutzrechtlichen Vorschriften geschützt, sofern deren Daten dem Fernmeldegeheimnis unterliegen. Dies

[32] Geppert/Schütz/Schütz, BeckTKG-Komm, § 3 Rn. 33.

[33] Geppert/Schütz/Schütz, BeckTKG-Komm, § 3 Rn. 79.

[34] Vgl. Fünfrocken et al, iKoPA D1v1, S. 241 ff.

stellt eine Besonderheit des TKG dar, da sonst durch datenschutzrechtliche Vorschriften nur natürliche Personen geschützt werden.[35]

2.3.3 TMG

Das TMG ist nach § 1 TMG für alle elektronischen Informations- und Telekommunikationsdienste anwendbar, die nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind. Damit wird neben der Anwendbarkeit des TMGs zugleich der Begriff der Telemedien legaldefiniert. Das TMG gilt auch für öffentliche Stellen. Nicht maßgeblich ist, ob ein Entgelt erhoben wird. Für die Bestimmung, ob etwas ein Telemedium ist, werden daher ein positives und drei Negativkriterien formuliert. Das positive Kriterium ist, dass es sich um einen Informations- und Kommunikationsdienst handelt. Die Negativkriterien sind, dass es sich nicht um Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk handelt. Der Unterschied zu anderen Diensten besteht damit zum einen in der nichtlinearen Übertragung und zum anderen darin, dass sie sich nicht im Erbringen von Signalen über Telekommunikationsnetze erschöpfen.[36] Die Abgrenzung zum Rundfunk erfolgt über die Linearität. Diese liegt vor, wenn Angebote entlang eines Sendeplans verbreitet und zeitgleich Empfangen werden sollen. Telemedien werden demgegenüber zum individuellen Abruf durch die Nutzer bereitgestellt.[37] Die Verbreitung von Informationen mittels DAB+ stellt daher Rundfunk dar, da die darüber verbreiteten Informationen nicht zum individuellen Abruf bereitgestellt werden, sondern zeitgleich durch die Nutzer empfangen werden sollen. Allerdings verweist § 47 Abs. 1 Rundfunkstaatsvertrag für den Datenschutz im Wesentlichen auf das Telemediengesetz, weshalb hier keine gesonderte Analyse des Rundfunkstaatsvertrags erforderlich ist.

2.3.4 BDSG

Das BDSG ist nach § 1 Abs. 3 BDSG nur dann anwendbar, wenn andere Rechtsvorschriften des Bundes auf personenbezogene Daten nicht anwendbar sind. Sofern andere Vorschriften auf die personenbezogenen Daten anwendbar sind, gehen sie den Regelungen des BDSG vor.

Bei dem BDSG handelt es sich daher um ein subsidiäres Auffanggesetz. Es ist auch insoweit anwendbar, wie spezialgesetzliche Regelungen keine Vollregelungen darstellen, also der

[35] Vgl. Kapitel 2.1.1.

[36] Gersdorf/Paal/Martini, BeckOK InfoMedienR, TMG, § 1 Rn. 4.

[37] Gersdorf/Paal/Martini, BeckOK InfoMedienR, TMG, § 1 Rn. 15.

bereichsspezifische Schutz personenbezogener Daten nicht vollumfassend ist. Das BDSG sichert damit die Vermeidung datenschutzrechtsfreier Räume.[38]

Adressaten des BDSG sind öffentliche Stellen des Bundes, öffentliche Stellen der Länder, soweit das Landesrecht den Datenschutz nicht regelt und nichtöffentliche Stellen.

2.3.5 Landesdatenschutzrecht

Die Datenschutzgesetze der Länder gelten für die öffentlichen Stellen der Länder, vgl. z.B. § 3 LDSG SH. Sie sind also für den Umgang mit personenbezogenen Daten aus vernetzten Fahrzeugen durch öffentliche Stellen der Länder zu beachten. Da die Datenschutzgesetze der Länder sich stark mit den Vorschriften des BDSG überschneiden, ist es hier nicht angezeigt, das Datenschutzrecht jedes einzelnen Landes zu analysieren.

2.3.6 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung gilt ab dem 25. Mai 2018. Sie genießt Anwendungsvorrang vor dem nationalen Datenschutzrecht der Mitgliedsstaaten. Eine Analyse der Datenschutz-Grundverordnung in Hinblick auf vernetzte und automatisierte Fahrzeuge erfolgt in der zweiten Version dieses Dokumentes, die zum Ende des Projekts veröffentlicht wird. Das bietet den Vorteil, dass dadurch eine vertiefte Analyse vor dem Hintergrund der im Erscheinen befindlichen rechtswissenschaftlichen Literatur durchgeführt werden kann.

2.3.7 e-Privacy-Verordnung

Die e-Privacy-Verordnung soll den Schutz der Persönlichkeit im Bereich der elektronischen Kommunikation regeln. Sie soll ebenfalls ab dem 25. Mai 2018 gelten. Bekannt ist bislang allerdings nur der Entwurf der Europäischen Kommission,[39] sodass noch nicht absehbar ist, wie sich der Entwurf im weiteren Gesetzgebungsprozess noch verändern wird. Auch dieses Regelwerk soll in der zweiten Version dieses Dokuments vertieft werden.

2.4 Vorschriften des BDSG

In diesem Kapitel werden die Regelungen des Bundesdatenschutzgesetzes dargestellt und erst danach werden die spezialgesetzlichen Vorgaben untersucht. Grund dafür ist, dass das BDSG grundlegende Begriffe des Datenschutzrechts enthält, die für das weitere Verständnis der spezialgesetzlichen Regelungen hilfreich sind und für deren Erörterung

[38] Wolff/Brink/Gusy, BeckOK DatenSR, BDSG, § 1 Rn. 81.

[39] 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 Kommunikation), abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017PC0010.

der Fokus dann auf die Besonderheiten der jeweiligen Regelungsmaterie gelegt werden kann.

2.4.1 Personenbezug

Das BDSG ist nur dann anwendbar, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, § 1 Abs. 2 BDSG. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Zunächst ist festzuhalten, dass das Datenschutzrecht nur natürliche Personen schützt. Juristische Personen, wie z.B. AGs und GmbHs, werden vom Datenschutzrecht grundsätzlich nicht geschützt.[40] Datenschutzrecht bezweckt den Schutz des allgemeinen Persönlichkeitsrechts. Träger dieses Persönlichkeitsrechts können aber nur natürliche Personen sein. Eine Mietwagenfirma könnte also grundsätzlich nicht datenschutzrechtliche Ansprüche gegen einen Automobilhersteller geltend machen.

Bei Einzelangaben handelt es sich um Informationen über eine bestimmte oder bestimmbare natürliche Person.[41]Aus diesen Informationen müssen sich Aussagen über persönliche oder sachliche Verhältnisse der betroffenen natürlichen Person tätigen lassen. Dies ist z.B. bei der Adresse, dem Familienstand, einer Versicherungsnummer und Telefonnummern unproblematisch der Fall.

Aus dem Wortlaut der Norm, nach dem auch Einzelangaben über bestimmbare natürliche Personen personenbezogen sind, ergibt sich, dass der Personenbezug nicht unmittelbar vorliegen muss. Es ist vielmehr ausreichend, dass er herstellbar ist.

Eine Identifizierung von Personen erfolgt zwar häufig anhand des Namens, es ist aber bereits ausreichend, dass eine Person anhand von individualisierenden Kennzeichen identifiziert werden kann. [42]

Grundsätzlich sind auch pseudonymisierte Daten personenbezogen. Bei einer Pseudonymisierung werden der Name und andere Identifikationsmerkmale durch ein Kennzeichen ersetzt, wodurch die Bestimmung des Betroffenen ausgeschlossen oder wesentlich erschwert werden soll, § 3 Abs. 6a BDSG. Eine Pseudonymisierung lässt den Personenbezug daher nur dann entfallen, wenn die Bestimmung des Betroffenen ausgeschlossen wird, also wenn die Bestimmung der Person nach der Lebenserfahrung oder dem Stand der Wissenschaft ausscheidet.[43] Grundsätzlich bleibt der Personenbezug

[40] Wolff/Brink/Schild, BeckOK DatenSR, BDSG, § 3 Rn. 2.

[41] Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 3 Rn. 3.

[42] Art. 29-Datenschutzgruppe, WP 136, S. 16.

[43] Scholz, in: Simitis, BDSG, § 3 Rn. 219.

aber durch die Zuordnungsregel erhalten, weshalb für die Belastbarkeit einer Pseudonymisierung Maßnahmen zu treffen sind, durch die die Zuordnungsregel geschützt wird.[44]

In der juristischen Literatur und Rechtsprechung wurde insbesondere anhand der IP-Adresse diskutiert, wie weit der Begriff des Personenbezugs auszulegen ist. 2011 hatte der Europäische Gerichtshof entschieden, dass IP-Adressen personenbezogene Daten sind, sich aber noch nicht dazu geäußert, ob dies nur für Internetprovider gilt oder auch für andere Stellen, die IP-Adressen speichern.[45] Diese Frage gelang durch einen Vorlagebeschluss des Bundesgerichtshofs zum Europäischen Gerichtshof. Der BGH legte dar, dass nach dem relativen Ansatz der Personenbezug von dynamischen IP-Adressen für Webseitenbetreiber zu verneinen sei, wenn der Betroffene seine Personalien nicht angibt. Zudem dürfe der Internetprovider den Webseitenbetreibern keine Auskünfte über die Identität der Betroffenen erteilen. Nicht ausreichend sei es, dass eine Staatsanwaltschaft diese Informationen beschaffen könne.[46] Der EuGH entschied, „dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.“[47] Er scheint sich damit für eine vermittelnde Position entschieden zu haben. Zwar ist bei der Beurteilung des Personenbezugs auch Zusatzwissen Dritter zu berücksichtigen, jedoch nur dann, wenn der Verantwortliche über rechtliche Zugriffsmöglichkeiten auf diese Zusatzinformationen verfügt.

Nunmehr sind diese allgemeinen Grundsätze auf das vernetzte Fahrzeug zu übertragen. In einer gemeinsamen Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie konnte man sich zum Personenbezug dahingehend einigen, dass Fahrzeugdaten zumindest dann personenbezogen sind, „wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.“[48] Darüber hinaus kommen aber eine Vielzahl

[44] Scholz, in: Simitis, BDSG, § 3 Rn. 217a.

[45] EuGH, Urteil v. 24.11.2011, Az.: C-70/10, Rn. 51.

[46] BGH, Beschluss v. 28.10.2014, Az.: VI ZR 135/13, Rn. 31, 32.

[47] EuGH, Urteil v. 19.10.2016, Az.: C582/14, Rn. 49.

[48] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, 2016, S. 1, abrufbar unter

weiterer Daten in Betracht, aus denen sich die für den Personenbezug notwendige Bestimmbarkeit einer natürlichen Person ergeben kann.

Die durch das vernetzte Fahrzeug erzeugten Daten sind vielfältig. Es fallen Daten über das Fahrzeug, über die Insassen und über die Umgebung an. Daten über das Fahrzeug beinhalten die Fahrzeug-Identifizierungsnummer, eindeutige mobile Gerätekennungen, SIM-Karten-Nummern, MAC-Adressen, RFID-Kennungen, Standortdaten, Bewegungsrichtungen und Geschwindigkeiten und Daten zum Betriebszustand. Daten über die Personen im Fahrzeug umfassen beispielsweise Registrierungsdaten, also Namen und Adressen, Kontodaten, Nutzerkonten, Voreinstellungen, biometrische Merkmale, Daten über die Fahrtauglichkeit des Fahrers und Identifikatoren für mobile Geräte, die jemand mit dem Fahrzeug verbindet. Umgebungsdaten umfassen z.B. Bild-, Video und Tonaufnahmen.[49] Mit dieser Systematisierung ist freilich noch keine Aussage über den Personenbezug der jeweiligen Daten getroffen. Für alle drei Kategorien gilt nämlich, dass es sich grundsätzlich um personenbezogene Daten handelt, denn sie erlauben Aussagen über den Fahrer, Halter oder Eigentümer eines Fahrzeugs. Daten aus Innenraumsensoren können auch Informationen über Mitfahrer enthalten. Außenweltsensoren erfassen Informationen über andere Verkehrsteilnehmer.[50] Es geht also grade nicht um die Frage ob personenbezogene oder fahrzeugbezogene Daten vorliegen, weil Daten, die sich auf das Fahrzeug beziehen auch Informationen über die eben genannten Personen enthalten.[51] So können auch des Personenbezugs zunächst relativ „unverdächtige“ Daten zu einem sog. Automobile Driver Fingerprinting genutzt werden. Dabei können Sensordaten, wie z.B. der Bremssensor, dazu genutzt werden das Verhalten eines Fahrers zu individualisieren und damit von anderen Fahrern abzugrenzen.[52] Andere Sensoren nutzen für die fahrzeuginterne aber auch außerhalb des Fahrzeugs abfangbare Kommunikation eindeutige Identifikatoren, die sich über die Lebensdauer der Sensoren nicht ändern. [53] Dies spricht dafür, dass nahezu alle Fahrzeugdaten zunächst personenbeziehbar sind. [54]

---

https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html.

[49] Hansen, DuD 2015, 367, 367 ff.

[50] Lüdemann, ZD 2015, 247, 250; Kremer, RDV 2014, 240, 244; Weichert, SVR 2014, 201, 204; Hornung, DuD 2015, 359, 361.

[51] Buchner, DuD 2015, 372, 373.

[52] Enev et al., PoPETs 2016, 34 ff.

[53] Rouf et al., S. 9.

[54] Im Ergebnis so auch Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 25. Tätigkeitsbericht vom 17.06.2015, S. 208; Vgl, Hornung, DuD 2015, 359, 364.

Dort, wo nicht sicher gesagt werden kann, ob es sich um anonyme Daten oder personenbeziehbare Daten handelt, etwa weil das zur Verfügung stehende Zusatzwissen mit dem die Daten verkettet werden können nicht abschließend beurteilt werden kann oder weil nicht absehbar ist, welche Deanonymisierungstechniken einem Angreifer zur Verfügung stehen, darf die verantwortliche Stelle das Risiko einer Personenbestimmung nicht einfach in Kauf nehmen. Das Datenschutzrecht als Ordnungsrecht setzt für die Ergreifung von Maßnahmen durch eine Aufsichtsbehörde nicht voraus, dass die verantwortliche Stelle vorsätzlich oder fahrlässig eine Fehlbeurteilung hinsichtlich des Personenbezugs trifft.[55] Deshalb kann den verantwortlichen Stellen nur zu raten sein, den Begriff des Personenbezugs präventiv auch auf solche Daten anzuwenden, bei denen ein Personenbezug nicht ausgeschlossen werden kann.

2.4.2 Persönliche und familiäre Tätigkeiten

Das BDSG ist nur dann anwendbar, wenn es sich bei dem Umgang mit personenbezogenen Daten nicht um eine persönliche oder familiäre Tätigkeit handelt. Dies folgt aus § 1 Abs. 2 Nr. 3 BDSG wonach das BDSG auf nicht-öffentliche Stellen anwendbar ist, außer die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Die Ausnahme schützt den Bereich persönlicher Lebensführung, den der Gesetzgeber für ebenso schutzwürdig betrachtet hat, wie die Betroffenen. Voraussetzung ist, dass die Datenverarbeitung in einem privaten Aktionskreis stattfindet. Ist dies der Fall, spielt es keine Rolle, wie intensiv in die Rechte der Betroffenen eingegriffen wird, allerdings bleiben zivilrechtliche Ansprüche der Betroffenen unberührt.[56] Im Rahmen dieser Anwendungsausnahme können nicht nur Daten über den Freundes- und Familienkreis verarbeitet werden. Allerdings stellt dies ein starkes Indiz für eine persönliche oder familiäre Tätigkeit dar. Es fällt aber darüber hinaus auch z.B. die Sammlung von Daten über Sportler oder Künstler im Rahmen von privaten Hobbies unter diese Ausnahme.[57] Nicht unter die Ausnahme fällt aber die Verbreitung von personenbezogenen Daten durch eine Veröffentlichung im Internet, wodurch diese einer unbegrenzten Zahl von Personen zugänglich gemacht werden.[58] Unproblematisch fällt daher beispielsweise die lokale Speicherung von privaten Kontaktdaten in einem Fahrzeug unter die Ausnahme, nicht aber die beruflichen Kontaktdaten, die z.B. ein Anwalt oder ein Arzt in sein Fahrzeug einspeichert. Schwieriger ist die Beurteilung, ob Sensoren, die auf die Außenwelt des

[55] Vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 38; Art. 29-Datenschutzgruppe, WP 136, S. 19.

[56] Damman, in: Simitis, BDSG, § 1 Rn. 149.

[57] Wolff/Brink/Gusy, BeckOK DatenSR, BDSG, § 1 Rn. 75.

[58] EuGH, Urt. v. 6.11.2003, Az. C-101/01, Rn. 47

Fahrzeugs gerichtet sind und dabei personenbeziehbare Daten erzeugen, unter die Ausnahme fallen können. Der EuGH hat in einem Verfahren, in dem es um die Rechtmäßigkeit einer Videobeobachtung des öffentlichen Straßenraums durch eine Privatperson ging, entschieden, dass eine solche Videoüberwachung, die auf einen Bereich außerhalb der privaten Sphäre gerichtet ist, keine persönliche oder familiäre Tätigkeit darstellt.[59] Unter Zugrundelegung dieses Maßstabes unterfällt die Generierung personenbezogener Daten durch Sensoren, die auf die Außenwelt gerichtet sind, nicht der Anwendungsausnahme für persönliche oder familiäre Tätigkeiten.

2.4.3 Verantwortliche Stelle und Auftragsdatenverarbeitung

Primärer Adressat des Datenschutzrechts ist die verantwortliche Stelle. Die Bestimmung der verantwortlichen Stelle ist daher elementar für die Umsetzung des Datenschutzrechts. Wo Verantwortlichkeiten unklar sind, besteht die Gefahr, dass den datenschutzrechtlichen Pflichten nicht nachgekommen wird.[60] Die Bestimmung der verantwortlichen Stelle wird insbesondere dann schwierig, wenn mehrere Stellen an der Datenverarbeitung beteiligt sind, da dann Verantwortlichkeit und Auftragsdatenverarbeitung voneinander abzugrenzen sind.

2.4.3.1 Verantwortliche Stelle

Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle, wer „personenbezogene Daten für sich selbst erhebt, speichert oder verarbeitet oder dies durch andere im Auftrag vornehmen lässt." Die Legaldefinition des § 3 Abs. 7 BDSG weicht damit im Wortlaut von Art. 2 d) der Richtlinie 95/46/EG (Datenschutzrichtlinie) ab. Danach ist der Verantwortliche nämlich derjenige, der allein oder gemeinsam mit anderen über Mittel und Zwecke der Datenverarbeitung entscheidet.

Der Verband der Automobilindustrie (VDA) und die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder haben sich in einer gemeinsamen Erklärung darauf geeinigt, dass zwischen Offline- und Online-Autos zu differenzieren sei. In beiden Fällen komme es darauf an, wer personenbezogene Daten aus dem Fahrzeug erhalte und somit erhebe. Bei Offline-Autos seien daher in der Regel Werkstätten verantwortliche Stellen. Bei Online-Autos seien dagegen diejenigen, die personenbezogene Daten erhielten verantwortliche Stellen, was in der Regel die Hersteller oder gegebenenfalls dritte Diensteanbieter seien.[61] Eine Begründung dieses Ergebnisses enthält die gemeinsame Erklärung nicht.

---

[59] EuGH, Urt. v. 11.12.2014, Az. C-212/13, Rn. 33.

[60] Vgl. Art. 29-Datenschutzgruppe, WP 169, S. 9.

[61] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), S. 2, abrufbar unter

Die Artikel-29-Datenschutzgruppe hat sich in ihrer Stellungnahme 169 intensiv mit der Definition des für die Verarbeitung Verantwortlichen im Sinne der Richtlinie auseinandergesetzt. Die Definition besteht aus drei Elementen. Der für die Verarbeitung Verantwortliche muss, erstens, eine natürliche oder juristische Person, Behörde, Einrichtung oder eine andere Stelle sein. Er muss, zweitens, über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Und er muss, drittens, diese Entscheidung entweder allein oder gemeinsam mit anderen treffen. Die Frage, wer die Entscheidung über eine Datenverarbeitung trifft, soll nicht durch die Analyse von formalen Gesichtspunkten sondern durch die Analyse der faktischen Umstände eines Einzelfalles beantwortet werden. [62] Sind mehrere Stellen an einer Datenverarbeitung beteiligt, kommt es zur Abgrenzung von Verantwortlichkeit und Auftragsdatenverarbeitung also nicht maßgeblich auf vertragliche Zuweisungen von Verantwortlichkeit, sondern auf die tatsächlichen Verhältnisse zwischen den Vertragsparteien an. Ansonsten könnten die Vertragsparteien die datenschutzrechtliche Verantwortlichkeit frei zuweisen.[63]

Vor dem Hintergrund der Stellungnahme der Artikel-29-Datenschutzgruppe und dem Wortlaut von Art. 2 d) der Richtlinie 95/46/EG, in dessen Lichte der § 3 Abs. 7 BDSG auszulegen ist,[64] ist die Hervorhebung die Heranziehung des Erhebungstatbestandes zur Bestimmung der verantwortlichen Stelle in der gemeinsamen Erklärung kritisch zu sehen. Zum einen macht es einen Unterschied, ob man für die Verantwortlichkeit ein Bestimmen über die Mittel und Zwecke der Datenverarbeitung oder den Erhebungstatbestand prüft – der Erhebungstatbestand dient der Abgrenzung von Fällen, in denen eine Person personenbezogene Daten ohne ein ihr zurechenbares Verhalten erhält zu solchen Fällen, in denen sie personenbezogene Daten willentlich erhält[65] - zum anderen wird durch die gemeinsame Erklärung eine Schutzlücke hinsichtlich der innerhalb eines Fahrzeugs verarbeiteten Daten geschaffen, deren Erforderlichkeit nicht ersichtlich ist. Diese Schutzlücke entsteht dadurch, dass eine Erhebung immer nur dann vorliegen soll, wenn Daten aus dem Fahrzeug ausgelesen werden (Offline-Autos) oder eine Kommunikation mit einer anderen Stelle stattfindet (Online-Autos).[66]

---

https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html

[62] Art. 29-Datenschutzgruppe, WP 169, S. 11.

[63] Art. 29-Datenschutzgruppe, WP 169, S. 14.

[64] Vgl. zum Grundsatz der richtlinienkonformen Auslegung Calliess/Ruffert/Ruffert, AEUV, Art. 288, Rn. 77 ff.

[65] Simitis, in: Simitis, BDSG, § 3 Rn. 104.

[66] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), S. 1.

Diese Anknüpfung an das Auslesen von Daten für die Bestimmung der Verantwortlichkeit kann schon dann nicht überzeugen, wenn man sich vor Augen führt, dass ein Fahrzeug z.B. auch durch einen Anwalt oder Arzt beruflich genutzt werden kann und es möglich ist, dass in den Fahrzeugspeichern Daten über die Mandanten oder Patienten eingebracht werden. Z.B. durch Synchronisierung mit dem Smartphone oder im eingebauten Navigationsgerät. Dann wäre das Fahrzeug nicht anders zu behandeln, also sonstige IT eines Anwalts oder Arztes. Schon damit ist gezeigt, dass das Fahrzeug selbst kein datenschutzrechtliches Vakuum sein kann.

Darüber hinaus muss derjenige, der die Daten erhält nicht notwendig auch der Verantwortliche sein. Wenn eine andere Stelle über die Mittel und Zwecke der Verarbeitung entscheidet ist die Stelle, welche die personenbezogenen Daten erhält als Auftragsdatenverarbeiter einzustufen.

Ebenso überzeugt es nicht, für die Verantwortlichkeit lediglich eine Verfügungsmacht über Daten zur Voraussetzung von Verantwortlichkeit zu machen.[67] Maßgeblich ist nach dem Wortlaut der Richtlinie vielmehr, ob über Mittel und Zwecke der Datenverarbeitung allein oder gemeinsam entschieden wird.

Die gemeinsame Erklärung erkennt aber ganz richtig, dass der Hersteller nicht schon deshalb verantwortliche Stelle ist, weil er das Fahrzeug zusammenbaut oder verkauft. Anderenfalls wäre z.B. die Unterscheidung zwischen der ausgebenden Stelle in § 6c BDSG und der verantwortlichen Stelle überflüssig. Verantwortliche Stelle ist grundsätzlich derjenige, der die Zwecke bestimmt. Datenverarbeitungsanlagen lassen sich regelmäßig für eine Vielzahl von unterschiedlichen Zwecken einsetzen. Für all diese Zwecke dem Hersteller der Verarbeitungsanlage zur verantwortlichen Stelle zu machen, wäre ein für den Hersteller unüberschaubares Risiko, da seine Verarbeitungslagen in einer Vielzahl ganz unterschiedlicher Lebenssachverhalte zum Einsatz kommen könnten.

Die Unterschiede dieser Ansichten sind aber überschaubar. Nach der hier vertretenen Auffassung fällt die Datenverarbeitung im Fahrzeug nicht von vornherein aus dem Anwendungsbereich des Datenschutzrechts heraus, sondern es wird Platz für die angemessene Bewertung von Einzelfällen gelassen.

Als erster Ansatzpunkt dafür, wer über die Mittel und Zwecke der Verarbeitung innerhalb eines Fahrzeugs entscheidet, kann betrachtet werden, wem das Fahrzeug sachenrechtliche zugeordnet ist und wer Halter des Fahrzeugs ist. Die sachenrechtliche Zuordnung spielt deshalb eine Rolle, weil sie durch gesetzliche Ansprüche abgesichert ist, die Zugriffsmöglichkeiten auf die Datenverarbeitung ermöglichen. Es lassen sich also zumindest Aussagen über die Mittelbestimmung treffen. Im Folgenden werden daher

[67] A.A. Weichert, SVR 2016, 361.363.

mögliche Verantwortlichkeiten des Eigentümers, des Halters und des Besitzers untersucht.

Als erstes ist der Eigentümer zu betrachten. Er hat zivilrechtlich grundsätzlich die stärkste Stellung aber dennoch ist die Stellung als Eigentümer bei Fahrzeugen in vielen Fällen für die Bestimmung über die Mittel kein gutes Indiz. Das liegt daran, dass es besonders bei Fahrzeugen häufig vorkommt, dass die Stellung des Eigentümers besonders schwach ist. Fahrzeuge werden häufig unter Eigentumsvorbehalt verkauft. Das bedeutet zweierlei, nämlich dass die derjenige, der das Verarbeitungsmittel in seinem unmittelbaren Zugriff hat, häufig nicht der Eigentümer ist und die Eigentümerstellung wegen dem Anwartschaftsrecht des Käufers[68] nicht so stark ist, wie dies sonst der Fall ist.

Weiterhin kann sich eine datenschutzrechtliche Verantwortlichkeit für die im Fahrzeug stattfindende Verarbeitung aus der Stellung als Halter ergeben. Halter ist derjenige, der die Verfügungsmacht über das Fahrzeug besitzt und auf dessen Kosten es betrieben wird.[69] Es kommt nicht darauf an, wer als Halter in die Zulassungsbescheinigung Teil I eingetragen ist, aus der Eintragung ergibt sich lediglich ein Anscheinsbeweis.[70] Der Halter ist im Regelfall derjenige, der die Entscheidung darüber getroffen hat, welches Fahrzeug verwendet wird. Dies sind z.B. Arbeitgeber und Mietwagenfirmen, die grundsätzlich entscheiden, welche Fahrzeuge sie anschaffen. Auch wenn der Halter nicht Eigentümer ist, wird er aber Inhaber des Anwartschaftsrechts sein. Wenn die Datenverarbeitung innerhalb des Fahrzeugs zu einer persönlichen oder familiären Tätigkeit durchgeführt wird, unterfällt es nicht dem Datenschutzrecht unterfällt. Anders ist es z.B. wenn Verarbeitungen im Fahrzeug für nichtpersönliche oder nichtfamiliäre Zwecke eingesetzt werden, also z.B. durch die bereits genannten Arbeitgeber, Mietwagenfirmen, Ärzte und Anwälte.

Es muss betont werden, dass dies nur einer der ersten Schritte einer datenschutzrechtlichen Prüfung ist. Allein aus der Feststellung der datenschutzrechtlichen Verantwortlichkeit lassen sich z.B. noch keine Aussagen über die datenschutzrechtliche Zulässigkeit oder Unzulässigkeit treffen.

Für die Übertragung von Daten in ein Backend ist es richtig, dass grundsätzlich derjenige, der die Daten erhält – dies wird regelmäßig der Diensteanbieter, bei iKoPA der „Service Provider“ sein - auch verantwortliche Stelle wird. Aber auch von diesem Grundsatz gibt es Ausnahmen. So ist es denkbar, dass die Stelle, welche die Daten erhält, ihre Tätigkeit für

[68] Bamberger/Roth/Kindl, BeckOK BGB, § 929, Rn. 73 ff.

[69] BVerwGE 29, 136, 136 ff.

[70] Vgl. OVG Lüneburg, Beschl. v. 30.01.2014, Az. 12 ME 243/13, Rn. 7.

eine andere Stelle ausübt und somit eine Auftragsdatenverarbeitung vorliegt. Dies hängt also in der iKoPA-Architektur von dem Verhältnis der Service Provider zueinander ab.

2.4.3.2 Auftragsdatenverarbeitung

Liegt eine Auftragsdatenverarbeitung vor, ist § 11 BDSG zu beachten. Auftragsverarbeitung liegt dann vor, wenn der Auftraggeber sich zur Durchführung von Verarbeitungsvorgängen einer anderen Stelle bedient.

Die verantwortliche Stelle muss den Auftragnehmer sorgfältig auswählen. Ein besonderer Gesichtspunkt müssen dabei die vom Auftragnehmer eingesetzten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten sein. Dies betrifft in der iKoPA-Architektur vor allem die Service-Provider, die untereinander kommunizieren können.[71] Liegt ein Fall der Auftragsverarbeitung vor, ist zwischen den Service Providern ein schriftlicher Vertrag zu schließen, der den Anforderungen des § 11 Abs. 2 BDSG genügen muss. Dieser muss unter anderem Gegenstand und Dauer des Auftrags, die Art der Daten, die Zwecke, die zu treffenden technischen und organisatorischen Maßnahmen, Kontrollrechte des Auftraggebers und den Umfang der Weisungsbefugnisse des Auftraggebers gegenüber dem Auftragnehmer festlegen. Bevor die Datenverarbeitung beginnt, muss der Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen beim Auftragnehmer überprüfen und dies sodann regelmäßig wiederholen.

Solche Auftragsverhältnisse können z.B. dann vorliegen, wenn die Service Provider sich zur Erhebung von personenbezogenen Daten eines Servers des Fahrzeugherstellers bedienen müssen, wie es das Konzept des „Extended Vehicle“ vorsieht.[72]

2.4.4 Rechtsgrundlagen

Jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten bedarf einer Rechtsgrundlage oder einer Einwilligung durch den Betroffenen. Dieser fundamentale datenschutzrechtliche Grundsatz wird als Verbot mit Erlaubnisvorbehalt[73] bezeichnet und ergibt sich aus der Formulierung des § 4 Abs. 1 BDSG. Gemäß § 4 Abs. 1 BDSG ist die „Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat“ und findet seine Grundlage in Art. 7 RL 95/46/EG, kann durch

[71] Fünfrocken et al., iKoPA D1v1, S. 237.

[72] Vgl. ACEA Position Paper, Access to vehicle data for third-party services, Dezember 2016, abrufbar unter https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf.

[73] Scholz/Sokol, in: Simitis, BDSG, § 4 Rn. 3.

den nationalen Gesetzgeber also nicht abgeschafft werden. Dieser Grundsatz gilt selbstverständlich auch für Datenverarbeitungen im Zusammenhang mit Fahrzeugen.

Eine Herausforderung bei der Auswahl der richtigen Erlaubnisnorm stellt die Vielzahl der von der Fahrzeugdatenverarbeitung möglicherweise Betroffenen dar. Von der Datenverarbeitung betroffen können insbesondere Halter, Eigentümer, Vorbesitzer, Fahrer, Beifahrer und sonstige Verkehrsbeteiligte, also z.B. auch Fußgänger sein.[74] Werden personenbezogene Daten dieser Personen erhoben, verarbeitet oder genutzt, so muss auch hierfür eine Rechtsgrundlage vorliegen. Die in Frage kommenden Erlaubnistatbestände finden sich in § 28 BDSG.

2.4.4.1 Verarbeitung zur Begründung, Durchführung oder Beendigung eines Vertrages

Nach § 28 Abs. 1 S. 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern, Übermitteln und Nutzen personenbezogener Daten für eigene Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Sie ist bei nicht-öffentlichen Stellen die zentrale Erlaubnisnorm für Datenverarbeitungen.[75] Die Vorschrift findet damit insbesondere auf Datenverarbeitungen für die Erfüllung von Verträgen zwischen Betroffenen und verantwortlichen Stellen Anwendung,[76] kann aber u.a. auch auf die Anbahnung von Vertragsverhältnissen angewandt werden.[77]

Zentraler Prüfungspunkt ist die Erforderlichkeit der Datenverarbeitung. Die Erforderlichkeit ist gegeben, wenn die Durchführung des Vertrages ohne die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten nicht möglich ist.[78] Die Erforderlichkeit lässt sich als Erfüllung einer Minimalitäts-Eigenschaft verstehen. „Es geht hierbei um die Frage, welche Menge ein minimales Set an Attributen (Eigenschaften) bildet, um die in einem Vertrag vereinbarten Funktionen erfüllen zu können. D.h., diese minimale Menge erlaubt keine Streichung eines Attributes, wenn die geforderten Funktionen geleistet werden sollen, enthält andererseits auch kein überflüssiges Attribut, das fehlen könnte, ohne die Erfüllung der geforderten Funktion zu gefährden.“[79]

---

[74] Weichert, SVR 2014, 201, 204.

[75] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 1.

[76] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 23.

[77] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 24.

[78] DKWW/Wedde, BDSG, § 28 Rn. 15, a.A. Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 33, Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 28 Rn. 15, die lediglich fordern, dass der Verzicht auf die Datenverarbeitung nicht sinnvoll oder unzumutbar sein muss.

[79] Taeger/Gabel/Taeger, BDSG, § 28 Rn. 51.

Liegt die Erforderlichkeit vor, ist eine darüber hinausgehende Interessenabwägung nicht erforderlich. [80] Werden also nur die für die Erfüllung eines bestimmten Vertrags erforderlichen Daten verarbeitet, können grundsätzlich auch Datenverarbeitungen im Zusammenhang mit vernetzten Fahrzeugen über diese Norm gerechtfertigt werden.

Eine Einschränkung ergibt sich aber aus der Vielzahl der von der Datenverarbeitung betroffenen Personen. Die Berechtigung aus § 28 Abs. 1 S. 1 Nr. 1 BDSG kann sich nämlich nur auf den Partner des Schuldverhältnisses erstrecken. Daten anderer Personen, also Dritter, können nur dann von dieser Rechtsgrundlage erfasst sein, wenn der Partner des Schuldverhältnisses hinsichtlich dieser Daten verfügungsbefugt ist. Eine solche Verfügungsbefugnis kann sich unter anderem aus einer Einwilligung ergeben.[81]

Mit dem Halter oder Fahrer wird der Verantwortliche zwar im Regelfall ein Vertragsverhältnis haben, hinsichtlich anderer möglicher Betroffener ist dies aber anders. Schon mit allen in Betracht kommenden Mitfahrern wird in der Regel kein Vertragsverhältnis vorliegen. Dies gilt erst recht nicht für andere Verkehrsteilnehmer.

Für die Verarbeitung der erforderlichen Daten des Vertragspartners des Diensteanbieters handelt es sich daher vor allem deshalb um eine sehr praktikable Norm, weil neben dem Vertragsschluss keine zusätzlichen Formvorschriften einzuhalten sind. Der Nachteil für den Diensteanbieter besteht darin, dass die Reichweite der datenschutzrechtlichen Erlaubnis auf den Vertragspartner begrenzt ist.

Diese Norm ist aber für das in iKoPA vorgesehene Reservierungssystem einschlägig, weil darauf geachtet wurde, ein besonders sparsames Reservierungssystem zu entwickeln. Bei einem Echteinsatz könnte daher die Datenverarbeitung durch den zwischen dem Nutzer und dem Reservierungsservice bestehenden Vertrag gerechtfertigt werden.

2.4.4.2 Verarbeitung zur Wahrung berechtigter Interessen der verantwortlichen Stelle

Nach § 28 Abs. 1 S. 1 Nr. 2 kann das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten dadurch gerechtfertigt werden, dass es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen die berechtigten Interessen der verantwortlichen Stelle überwiegen.

Die Vorschrift erlaubt die Datenverarbeitung unter drei Voraussetzungen. Es muss, erstens, ein berechtigtes Interesse der verantwortlichen Stelle vorliegen. Zweitens muss

[80] DKWW/Wedde, BDSG, § 28 Rn. 15.

[81] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 32; a.A. Simitis in: Simitis, BDSG, § 28 Rn. 62.

die Verarbeitung erforderlich zur Wahrung dieses Interesses sein und die Betroffeneninteressen dürfen, drittens, nicht überwiegen.

Berechtigte Interessen sind alle von der Rechtsordnung anerkannten Interessen, [82] weshalb dieses Tatbestandsmerkmal kaum eine eingrenzende Funktion erfüllen kann. Allerdings muss es sich um ein eigenes Interesse der verantwortlichen Stelle handeln.[83]

Hinsichtlich der Erforderlichkeit gelten die gleichen Voraussetzungen, wie unter 2.4.4.1.

Die dritte Tatbestandsvoraussetzung ist die Abwägung, deren Ergebnis sein muss, dass die schutzwürdigen Interessen der Betroffenen nicht das berechtigte Interesse des Verantwortlichen überwiegen. Es sind also zunächst die Interessen der verantwortlichen Stelle zu gewichten. Dann sind die Interessen der Betroffenen zu gewichten und anschließend sind die beiden Ergebnisse miteinander zu vergleichen.[84] Auf Seiten der Betroffenen ist die Eingriffsintensität in die Grundrechte zu prüfen. Dabei ist z.B. zu berücksichtigen, ob leicht verknüpfbare Daten verarbeitet werden sollen oder ob es sich um Daten handelt, die Informationen über den besonders geschützten inneren Lebensbereich des Betroffenen beinhalten.[85]

Dadurch lassen sich insbesondere Datenverarbeitungen rechtfertigen, die die Rechte der Betroffenen nur in geringem Umfang berühren. Wenn z.B. Außenweltsensoren wie LiDAR auch personenbeziehbare Daten erfassen, dient dies dem berechtigten Interesse am Betrieb eines automatisierten Fahrzeugs und der Unfallvermeidung. Sofern die Daten möglichst schnell gelöscht werden, können diese gewichtigen Interessen die Betroffeneninteressen überwiegen. [86] Ebenso besteht ein berechtigtes Interesse an der Erhöhung der Verkehrssicherheit durch CAM[87]- und DENM[88]-Nachrichten. Diese sollen Dienste, wie die Warnung vor langsamen oder stehenden Fahrzeugen, Warnungen vor Straßenarbeiten, Warnungen vor sich nähernden Einsatzfahrzeugen und die Anzeige von

[82] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 59; Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 28 Rn. 24.

[83] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 60; Simitis, in: Simitis, BDSG, § 28 Rn. 105.

[84] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 28 Rn. 66.

[85] SDM, V.1.0, S. 37 f.

[86] Vgl. Roßnagel et al., Datenschutzrecht 2016, S. 62.

[87] European Telecommunication Standards Institute, Intelligtent Transport Systems (ITS), Vehicular Communications, Basic Set of Applications, Part 2: Specification of Cooperative Awareness Basic Service, ETSI EN 302 637-2 V1.3.1 (2014-09).

[88] European Telecommunication Standards Institute, Intelligtent Transport Systems (ITS), Vehicular Communications, Basic Set of Applications, Part 2: Specification of Decentralized Environmental Notification Basic Service, ETSI EN 302 637-3 V1.2.1 (2014-09).

Verkehrszeichen im Fahrzeug ermöglichen.[89] Es handelt sich also um gewichtige Zwecke, für die eine Datenverarbeitung, die ansonsten den datenschutzrechtlichen Vorgaben entspricht, grundsätzlich gerechtfertigt ist, sofern CAMs nur im erforderlichen Umfang aufgezeichnet werden, der Nutzer eine Deaktivierungsmöglichkeit hat, die Verarbeitung dem Transparenzgrundsatz entspricht und durch Kontrollen eine flächendeckende Aufzeichnung von CAMs unterbunden wird.[90]

2.4.4.3 Verarbeitung allgemein zugänglicher Daten

§ 28 Abs. 1 S. 1 Nr. 2 BDSG enthält eine Rechtsgrundlage zur Verarbeitung allgemein zugänglicher Daten. Die Regelung soll die Informationsfreiheit aus Art. 5 Abs. 1 S. 1 GG schützen. Allgemein zugängliche Daten sind eine der wichtigsten Möglichkeiten, sich frei zu informieren.[91] Zu den allgemein zugänglichen Daten gehören Informationen aus Zeitungen, Rundfunk, Fernsehen und Registern, bei denen der Zugang nicht beschränkt ist. Es muss sich um solche Daten handeln, die dazu bestimmt sind, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[92] Nicht erforderlich ist, dass der Personenkreis tatsächlich bestimmt wurde, sondern lediglich, dass er bestimmbar ist.

Ein Raum für die Anwendung dieser Norm beim vernetzten Fahren ist nicht ersichtlich. Dies wäre nur dann der Fall, wenn personenbeziehbare Daten z.B. über DAB+[93] verteilt werden würden und damit allgemein verfügbar wären. Ein solches Bereitstellen von personenbeziehbaren Daten über Rundfunk wäre aber aufgrund der Sensibilität von personenbeziehbaren Fahrzeugdaten kritisch zu sehen und ist im Rahmen des iKoPA-Projektes auch nicht vorgesehen. Ansonsten ist die Bereitstellung von nicht personenbezogenen Daten über Rundfunk positiv zu bewerten, da hierbei keine Kommunikation vom Fahrzeug ausgehen muss.

Auch die CAM und DENM-Nachrichten, mit denen Fahrzeuge Informationen im Nahbereich verteilen können, sind keine allgemein zugänglichen Daten im Sinne der Norm, da es sich um Informationen handelt, die mit einer Reichweite von ca. 800 Metern ausgesandt werden.[94] Dadurch ist der Empfängerkreis individuell bestimmbar.

[89] Strubbe/Thenée/Wieschebrink, DuD 2017, 223, 224.

[90] Vgl. Kiometzis/Ullmann, DuD 2017, 227, 231.

[91] Simitis, in: Simitis, BDSG, § 28 Rn. 146 f.

[92] Simitis, in: Simitis, BDSG, § 28 Rn. 151.

[93] Vgl. Fünfrocken et al., iKoPA D1v1, S. 115.

[94] Vgl. Strubbe/Thenée/Wieschebrink, DuD 2017, 223, 223.

2.4.4.4 Einwilligung

Neben einer Rechtsgrundlage kann nach § 4 Abs. 1 BDSG auch eine Einwilligung des Betroffenen den Umgang mit personenbezogenen Daten rechtfertigen. Die Einwilligung des Betroffenen gilt als Ausdruck der informationellen Selbstbestimmung[95], wird aber aufgrund der mangelnden tatsächlichen Einflussmöglichkeiten der Betroffenen als Fiktion kritisiert.[96]

Die Voraussetzungen für eine wirksame Einwilligung sind in § 4a BDSG geregelt. Danach muss die Einwilligung in informierter Weise und freiwillig erfolgen. Zudem ist für Einwilligungen nach dem BDSG grundsätzlich die Schriftform erforderlich und die Einwilligung ist vor Beginn der Datenverarbeitung einzuholen.

2.4.4.4.1 *Informiertheit*

Notwendige Bedingung dafür, dass der Betroffene die Reichweite seiner Einwilligung abschätzen kann und damit gleichzeitig Voraussetzung einer selbstbestimmten Entscheidung ist die Informiertheit der Einwilligung. Die verantwortliche Stelle unterliegt einer umfassenden Informationspflicht. Zu den bereitzustellenden Informationen gehören die Verarbeitungszwecke, die Identität der verantwortlichen Stelle, potentielle Datenempfänger, Speicherdauer, die betroffenen personenbezogenen Daten und ggf. die Folgen einer Verweigerung der Einwilligung. Zeitlich hat die Erfüllung der Informationspflicht in unmittelbarem Zusammenhang mit der Einholung der Einwilligung zu stehen.[97]

Kommt die verantwortliche Stelle ihrer Informationspflicht nicht ausreichend nach, ist die Einwilligung insoweit unwirksam, wie der Betroffene nicht informiert ist. Die Einwilligung kann nämlich in dem Ausmaß, in dem der Betroffene nicht informiert ist, nicht ihre Legitimationswirkung entfalten.[98]

Die Betroffenen ausreichend zu informieren ist daher eine anspruchsvolle Aufgabe, von der gleichzeitig die Rechtmäßigkeit der Datenverarbeitung abhängt. Soweit Fahrzeuge über ein Human Machine Interface verfügen, bietet es sich an, darüber auch die Informationen bereitzustellen, weil damit ein enger zeitlicher Zusammenhang zur Datenverarbeitung hergestellt wird. Allerdings ist der Platz für Darstellungen hier meist

[95] Simitis, in: Simitis, BDSG, § 4a Rn. 2.

[96] Simitis, in: Simitis, BDSG, § 4a Rn. 3.

[97] Wolff/Brink/Kühling, BeckOK DatenSR, BDSG, § 4a Rn. 43.

[98] Wolff/Brink/Kühling, BeckOK DatenSR, BDSG, § 4a Rn. 43; a.A. wohl Simitis, in: Simitis, BDSG, § 4a Rn. 76, der ohne Abgrenzung die Datenverarbeitung bei mangelnder Information als unzulässig bezeichnet.

noch sehr begrenzt. Deshalb kann es sinnvoll sein, tiefergehende Informationen schriftlich in der Borddokumentation oder auf Webseiten vorzuhalten.

2.4.4.4.2 *Freiwilligkeit*

Nach § 4a Abs. 1 S. 1 BDSG ist es Voraussetzung einer wirksamen Einwilligung, dass diese auf der freien Entscheidung des Betroffenen beruht. Das Tatbestandsmerkmal der Freiwilligkeit soll den Betroffenen vor dem häufig vorhandenen Ungleichgewicht zwischen der verantwortlichen Stelle und dem Betroffenen schützen. Ein solches Ungleichgewicht kann zur Folge haben, dass der Betroffene nur formal eine Wahlmöglichkeit hat, aufgrund einer Zwangslage aber dennoch einwilligen muss.[99] Eine in dieser Hinsicht besonders problematische Konstellation ist das Arbeitsverhältnis, weil es die Existenzgrundlage des Betroffenen berührt. Gleichwohl wird die Freiwilligkeit der Einwilligung auch in Arbeitsverhältnissen in Literatur und Rechtsprechung nicht generell ausgeschlossen.[100] Aufgrund des wirtschaftlichen und sozialen Ungleichgewichts wird vertreten, dass eine Vermutung dafür spricht, dass eine gegenüber dem Arbeitgeber abgegebene Einwilligung unfreiwillig ist, was dann durch den Arbeitgeber zu widerlegen wäre.[101] Demgegenüber hat das BAG gefordert, dass der Arbeitnehmer Sachverhalte vorträgt, die gegen die Freiwilligkeit der Einwilligung sprechen.[102]

Schwierig zu beurteilen ist die Freiwilligkeit daher insbesondere in solchen Fällen, in denen es sich bei vernetzten oder sonst datenverarbeitenden Fahrzeugen um Dienst- oder Firmenwagen handelt und diese somit im Rahmen von Dienst- oder Arbeitsverhältnissen eingesetzt werden.

2.4.4.4.3 *Form*

Die Einwilligung soll grundsätzlich schriftlich erfolgen. Deshalb sind Email oder Fax regelmäßig nicht ausreichend. Es bedarf einer Unterschrift oder der elektronischen Form nach § 126a BGB.[103] Nur ausnahmsweise braucht diese Form nach § 4a Abs. 1 S. 3 BDSG nicht eingehalten werden. Dafür müssen besondere Umstände vorliegen, die den Verzicht auf die Schriftform angemessen erscheinen lassen. Der Verzicht auf die Schriftform muss die Ausnahme bleiben, wie sich aus der eindeutigen Formulierung der Norm ergibt.[104] Gegen eine weite Anwendung der Ausnahme spricht darüber hinaus, dass dadurch die

---

[99] Wolff/Brink/Kühling, BeckOK DatenSR, BDSG, § 4a Rn. 35.

[100] BAG, Urt. v. 11.12.2014, Az. 8 AZR 1010/13, Rn. 32; Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 4a Rn. 22b.

[101] DKWW/Däubler, BDSG, § 4a Rn. 23.

[102] BAG, Urt. v. 11.12.2014, Az. 8 AZR 1010/13, Rn. 33.

[103] Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 4a Rn. 29.

[104] Simitis, in: Simitis, BDSG, § 4a Rn. 44.

Funktionen von Formvorschriften unterlaufen würden. Formvorschriften sollen u.a. durch ihre Warnfunktion vor übereilten Erklärungen schützen sowie eine Klarstellungs- und Beweisfunktion hinsichtlich des Erklärungsinhalts erfüllen.[105]

2.4.4.4.4 *Zwischenergebnis zur Einwilligung*

Ist die Einwilligung zur Rechtfertigung von Datenverarbeitungen im Zusammenhang mit vernetzten Fahrzeugen noch ein praktikables Mittel, wenn man als Betroffenen nur den Fahrer hat, stellt sich dies schon anders dar, wenn man auch die anderen möglichen Betroffenen betrachtet. Hinsichtlich des Fahrers kann eine Einwilligung z.B. über das Infotainmentsystem erfolgen. Schon wenn man aber auch für die Mitfahrer jeweils eine Einwilligung einholen will, kann dies sehr unhandlich werden, z.B. wenn alle Mitfahrer erst längere Einwilligungstexte lesen und verstehen sollen. Unmöglich ist wiederum die Einholung der Einwilligung von allen sonstigen Verkehrsteilnehmern wie z.B. Fußgängern.

2.4.4.5 Zwischenergebnis zu den Rechtsgrundlagen

Als Zwischenergebnis zu den Rechtsgrundlagen lässt sich festhalten, dass die sog. Drittbetroffenen die größte Herausforderung darstellen. Soweit sich die Datenverarbeitung im Rahmen des zur Erbringung eines Vertrages zwischen Diensteanbieter und Betroffenem Erforderlichen bewegt, ist die Datenverarbeitung durch § 28 Abs. 1 Nr. 1 BDSG gerechtfertigt. Hier setzt iKoPA an, indem z.B. zum Nachweis von Berechtigungen nicht die Offenlegung einer Identität gefordert wird, sondern lediglich die Existenz einer Berechtigung mittels eines kryptographischen Verfahrens nachgewiesen werden muss. Sollen darüber hinaus personenbezogene Daten erhoben, verarbeitet oder genutzt werden, muss eine Einwilligung eingeholt werden. Die Verarbeitung der personenbezogenen Daten Drittbetroffener lässt sich praktikabel nur über eine Interessenabwägung rechtfertigen. Die sich daraus ergebende Rechtsunsicherheit lässt sich nur dann auf ein erträgliches Maß reduzieren, wenn nachweislich datenschutzfreundliche Technologie zum Einsatz kommt, deren Eingriffstiefe in die Rechte der Betroffenen Personen auf ein Minimum reduziert ist. Im Kapitel zum technischen Datenschutz wird gezeigt, mit welcher Methodik auch in anderen Bereichen des vernetzten Fahrzeugs sich Lösungen entwickeln lassen, die diese Hürde nehmen können. Den an der Entwicklung des vernetzten Fahrzeugs beteiligten Unternehmen ist es daher dringend zu raten, sich mit den Anforderungen eines anspruchsvollen technischen Datenschutzes im vernetzten Fahrzeug auseinanderzusetzen und sich so auch Vorteile im Wettbewerb zu sichern. In Zukunft werden z.B. Mietwagenfirmen und staatliche Institutionen verstärkt darauf achten müssen, Fahrzeuge mit datenschutzfördernder Technologie anzuschaffen. Soweit es sich um staatliche Akteure

[105] Vgl. Bamberger/Roth/Wendtland, BeckOK BGB, § 125, Rn. 1.

handelt, sind diese in ihrem Handeln unmittelbar an das Grundrecht der informationellen Selbstbestimmung gebunden. Durch die insoweit deutlicheren Vorschriften der Datenschutz-Grundverordnung, auf die in der zweiten Version dieses Dokuments eingegangen wird, wird diese Ansicht gestärkt.

2.4.5 Zweckbindung

Nach § 28 Abs. 1 S. 2 BDSG sind bei der Erhebung von Daten die Zwecke der Verarbeitung konkret festzulegen. § 28 Abs. 2 BDSG normiert die Möglichkeiten der Zweckentfremdung. [106] Sie ist nur zulässig, wenn die Voraussetzungen von § 28 Abs. 1 S. 1 Nr. 2 oder 3 BDSG vorliegen oder es zur Wahrung von berechtigten Interessen eines Dritten oder zur Gefahrenabwehr oder Strafverfolgung erforderlich ist und die Betroffeneninteressen nicht überwiegen. Darüber hinaus wird wissenschaftliche Forschung privilegiert. Solche Zweckentfremdungen können z.B. bei der Verwendung von Fahrzeugdaten für die Beweisführung in Gerichtsprozessen zulässig sein.[107]

2.4.6 Betroffenenrechte

Die §§ 33 ff. BDSG enthalten Rechte des Betroffenen gegen die verantwortliche Stelle, mit denen der Betroffene Einfluss auf die Datenverarbeitung nehmen kann.

2.4.6.1 Benachrichtigung

Die Benachrichtigung des Betroffenen ist in § 33 BDSG geregelt. Werden personenbezogene Daten ohne Kenntnis des Betroffenen gespeichert, muss dieser über die Speicherung, die Art der Daten, die Zweckbestimmung und die Identität der verantwortlichen Stelle benachrichtigt werden.

Abs. 2 enthält umfangreiche Ausnahmen von der Benachrichtigungspflicht. Betroffene müssen unter anderem dann nicht benachrichtigt werden, wenn sie von einer Speicherung oder Übermittlung bereits Kenntnis haben, wenn Daten geheim zu halten sind oder wenn die Speicherung und Übermittlung durch ein Gesetz vorgesehen ist. Der letzte Punkt kann beispielsweise beim ab 2018 verpflichtend in Neuwagen einzubauenden eCall-System vorliegen.

2.4.6.2 Auskunft

§°34°BDSG normiert einen Auskunftsanspruch des Betroffenen gegen die verantwortliche Stelle. Der Betroffene kann von der verantwortlichen Stelle verlangen, dass diese ihm Auskunft erteilt über die zu seiner Person gespeicherten Daten, den Zweck, die Herkunft

[106] Vgl. BeckOK DatenSR, BDSG, § 28 Rn. 90.

[107] Roßnagel et al, Datenschutzrecht 2016, S. 62.

der Daten und die Empfänger oder die Kategorien von Empfängern, an die die Daten weitergegeben werden.

2.4.6.3 Berichtigung

Nach § 35 Abs. 1 BDSG sind personenbezogene Daten zu berichtigen, wenn diese unrichtig sind. Daten sind unrichtig, wenn sie nicht mit der Tatsachenlage übereinstimmen.[108] Solche Berichtigungsansprüche können z.B. entstehen, wenn die Service Provider in der iKoPA-Architektur unrichtige Daten speichern.

2.4.6.4 Löschung

Der Anspruch auf Löschung findet sich in § 35 Abs. 2 BDSG. Personenbezogene Daten müssen gelöscht werden, wenn ihre Speicherung unzulässig ist, es sich um besondere Kategorien personenbezogener Daten handelt und die Richtigkeit der Daten von der verantwortlichen Stelle nicht bewiesen werden kann, wenn die Verarbeitung für eigene Zwecke erfolgt und die weitere Speicherung der Daten nicht mehr erforderlich ist. Werden Daten geschäftsmäßig zum Zweck der Übermittlung verarbeitet, muss regelmäßig überprüft werden, ob eine weitere Speicherung noch erforderlich ist. Ist dies nicht der Fall und widerspricht der Betroffene der Löschung nicht, sind die Daten zu löschen, wenn die Erforderlichkeit nicht mehr gegeben ist.

Der Begriff des Löschens ist in § 3 Abs. 4 S. 2 Nr. 5 BDSG definiert. Es handelt sich demnach um das Unkenntlichmachen von personenbezogenen Daten. Dies kann beispielsweise durch Vernichtung des Datenträgers oder durch Überschreiben erfolgen.[109]

2.4.6.5 Sperrung

Der Anspruch auf Sperrung ist in § 35 Abs. 3, 4 und 4a BDSG geregelt. Die Sperrung tritt an die Stelle einer Löschung, wenn einer Löschung Aufbewahrungsfristen entgegenstehen, angenommen werden muss, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden oder eine Löschung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Daten sind nach § 3 Abs. 4 Nr. 4 BDSG gesperrt, wenn sie so gekennzeichnet werden, dass ihre weitere Verarbeitung oder Nutzung eingeschränkt ist.[110]

[108] Vgl. Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 35 Rn. 8; Dix, in: Simitis, BDSG, § 35 Rn. 9.

[109] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 35 Rn. 26.

[110] Wolff/Brink/Wolff, BeckOK DatenSR, BDSG, § 35 Rn. 46.

2.4.7 Internationaler Datenverkehr

Es kommt für die Rechtmäßigkeit eines Verfahrens auch darauf an, in welchen Staat personenbezogene Daten übermittelt werden. Dabei gilt, dass grenzüberschreitender Datenverkehr innerhalb der Union den allgemeinen Vorschriften unterliegt, also eine Rechtsgrundlage einschlägig oder eine Einwilligung eingeholt werden muss. Zusätzliche Anforderungen nach § 4b Abs. 2 BDSG sind zu erfüllen, wenn Übermittlungen in Drittländer vorgenommen werden. Die Übermittlung hat zu unterbleiben, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ob ein solches schutzwürdige Interesse vorliegt hängt im Wesentlichen davon ab, ob bei der Übermittlung in ein Drittland ein angemessenes Datenschutzniveau gewährleistet werden kann. Ein solches angemessenes Datenschutzniveau kann sich z.B. aus genehmigten Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben.[111] Es ergeben sich aus einer Verarbeitung in einem Drittland aber Unwägbarkeiten, die sich vermeiden lassen. Der EuGH entschied zum Safe-Harbor-Abkommen, das vorsah, dass sich US-Unternehmen einer Selbstzertifizierung unterziehen, um ein angemessenes Datenschutzniveau nachzuweisen, dass dieses ungültig war. Er begründete dies unter anderem mit den Befugnissen, über die die US-Geheimdienste verfügen. „Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens“.[112] Solche Umstände sind von den verantwortlichen Stellen regelmäßig nicht unmittelbar beeinflussbar, weshalb zu raten ist, eine Übermittlung in Drittstaaten möglichst nicht vorzunehmen.

2.4.8 Automatisierte Einzelfallentscheidungen

Nach § 6a BDSG sind automatisierte Einzelfallentscheidungen grundsätzlich verboten. Voraussetzung ist, dass es sich um Entscheidungen handelt, die für den Betroffenen eine rechtliche Folge haben können oder ihn sonst erheblich beeinträchtigen können und dass diese Entscheidung auf einer automatisierten Verarbeitung personenbezogener Daten beruht, die der Bewertung von einzelnen Persönlichkeitsmerkmalen dient.

Zweck der Vorschrift ist der Schutz vor den Risiken von Profilbildungen und darauf beruhenden wertenden Entscheidungen. Das Individuum soll als solches beurteilt werden und nicht einer für es nicht durchschaubaren Datenverarbeitung ausgeliefert sein. Dem Betroffenen sollen Transparenz und Fairness bei der Entscheidungsfindung ermöglicht

[111] Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 4b Rn. 6.

[112] EuGH, Urt. v. 06.10.2015, Az. C-362/14, Rn. 94; Zu den Auswirkungen vgl. Ambrock, NZA 2015, 1493 ff.; zur Wesensgehaltsgarantie vgl. Bock/Engeler, DVBl 2016, 593 ff.

werden[113] und so die „ungeprüfte Unterwerfung des Individuums unter die Entscheidung der Maschine verhindert werden“.[114]

Die Norm ist nicht allgemein auf das automatisierte Fahren übertragbar. Denkbar wäre dies z.B. bei der Entscheidung, einen Fahrspurwechsel durchzuführen, eine Vollbremsung vorzunehmen, über eine Kreuzung zu fahren oder einen Parkplatz mit Ladesäule zu reservieren.

Im Regelfall wird eine ausschließlich automatisierte Entscheidung vorliegen. Diese entfällt nur dann, wenn durch einen Menschen eine einer Richtigkeits- und Plausibilitätskontrolle durchgeführt wird.[115] Fällt ein automatisiertes Fahrzeug die Entscheidung, einen Fahrspurwechsel durchzuführen, eine Vollbremsung vorzunehmen oder über eine Kreuzung zu fahren, wird zumindest bei ab Stufe 3 des automatisierten Fahrens nicht mehr bei jeder Entscheidung eine menschliche Kontrolle vorgenommen.[116] Ab dieser Stufe muss der Fahrer das Fahrzeug nämlich nicht mehr dauerhaft überwachen.

Diese Entscheidungen müssen ein gestaltender Akt mit einer abschließenden Wirkung sein. Die Entscheidung muss aber auch auf der Bewertung einzelner Persönlichkeitsmerkmale beruhen, also auf der elektronischen Auswertung von Persönlichkeitsprofilen.[117] Solche Auswertungen von Persönlichkeitsprofilen durch das automatisierte Auto selbst sind nicht zu erwarten und es ist auch nicht ersichtlich anhand welcher Persönlichkeitsmerkmale Modifikationen an Fahrbefehlen entschieden werden.[118] Möglich wäre dies allerdings durch Backendsysteme, mit denen das Fahrzeug kommuniziert. Denkbar wäre es z.B., dass die Zuweisung von Parkplätzen automatisiert so vorgenommen wird, dass bestimmte Personengruppen näher an für sie interessanten Geschäften parken müssen, was eine Profilbildung voraussetzen würde. Allerdings ist eine solche Funktion in iKoPA nicht geplant.

2.4.9 Optisch-elektronische Überwachung

§ 6b BDSG regelt die Zulässigkeit der Beobachtung öffentlich-zugänglicher Räume mittels optisch-elektronischer Einrichtungen.

---

[113] Scholz, in: Simitis, BDSG, § 6a Rn. 3.

[114] Wolff/Brink/von Lewinski, BeckOK DatenSR, BDSG, § 6a Rn. 1.

[115] Wolff/Brink/von Lewinski, BeckOK DatenSR, BDSG, § 6a Rn. 15.

[116] Vgl. Verband der Automobilindustrie, Automatisierung, S. 14 f., abrufbar unter https://www.vda.de/de/themen/innovation-und-technik/automatisiertes-fahren/automatisiertes-fahren.html

[117] Scholz, in: Simitis, BDSG, § 6a Rn. 21.

[118] So aber wohl Weichert, SVR 2014, 241, 241.

Sie ist nur zulässig, wenn sie zur Aufgabenerfüllung öffentlicher Stellen erforderlich ist, zur Wahrnehmung des Hausrechts erforderlich ist oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Daneben dürfen keine Anhaltspunkte für ein Überwiegen der schutzwürdigen Interessen der Betroffenen bestehen. Nach Abs. 2 sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen kenntlich zu machen.

Problematisch ist, ob die Norm auch auf in automatisierten Fahrzeugen verbaute Kameras und sonstige Sensoren anwendbar ist. Fraglich könnte sein, ob eine Beobachtung stattfindet, weil damit ja keine Überwachung bezweckt sei. Das VG Schwerin hat zu dieser Frage richtigerweise ausgeführt:

„Die Anwendbarkeit des § 6b BDSG kann demgegenüber nicht davon abhängen, ob das Beobachten eines öffentlich zugänglichen Raums mit optisch-elektronischen Einrichtungen auf die Überwachung der Betroffenen ausgerichtet ist (so aber anscheinend Wrede, DuD 2010, 225, 228). Werden in dem beschriebenen Maße personenbezogene oder zumindest personenbeziehbare Daten erhoben, bleibt es auch dann bei der Einordnung als Videoüberwachung, wenn die Beobachtung eine lediglich (unvermeidliche) Nebenfolge des eigentlich Gewollten und die ungewollte Erfassung von Personen sogar unerwünscht ist (vgl. auch Onstein in Auernhammer, BDSG, 4. Aufl., § 6b Rn. 22; Wedde in Däubler/Klebe/Wedde/Weichert, a.a.O., § 6b Rn. 14).“[119]

Es kommt daher nicht darauf an, dass in das Fahrzeug eingebaute Kameras nicht dazu gedacht sind, eine Überwachung des Straßenverkehrs durchzuführen, sondern vorrangig der Erkennung von Hindernissen und damit der sicheren Navigation dienen, weil dafür eine Beobachtung erforderlich ist.

Die Norm ist anwendbar, wenn Kameras in Parkhäusern eingesetzt werden, um eine genaue Positionsbestimmung von automatisierten Fahrzeugen zu gewährleisten. Auch dabei kommt es nicht darauf an, dass die Beobachtung lediglich eine Nebenfolge des eigentlichen Zwecks, nämlich der Positionsbestimmung ist. Der Einsatz dieser Kameras ist aber nach § 6b Abs. 1 Nr. 3 BDSG gerechtfertigt, weil er zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Soweit die dabei anfallenden Daten nur in dem Rahmen verarbeitet werden, der zur Positionsbestimmung erforderlich ist, muss nicht von einem Überwiegen der Betroffeneninteressen ausgegangen werden.

Bei LiDAR-Systemen handelt es sich nicht um optisch elektronische Einrichtungen im Sinne der Norm. Optisch-elektronische Einrichtungen liegen dann vor, wenn Licht in elektrische Signale umgewandelt wird. Nicht von der Vorschrift erfasst werden sollen dagegen andere

[119] VG Schwerin, Beschl. v. 18.06.2015, Az. 6 B 1637/15 SN.

Bereiche des elektromagnetischen Spektrums, wie z.B: Radar. [120] LiDAR basiert darauf, dass das zurückgestrahlte Licht eines Laserimpulses detektiert wird. Allerdings liegt der Laserimpuls außerhalb des sichtbaren Spektrums. Deshalb fällt LiDAR nicht unter die Norm, weil es keine optische Einrichtung ist. Der Gesetzgeber wollte mit der Norm die Videoüberwachung regeln. Deshalb ist die Norm so zu verstehen, dass nur der sichtbare Teil des elektromagnetischen Spektrums von der Norm erfasst wird.

2.4.10 Mobile personenbezogene Speicher- und Verarbeitungsmedien

Wenn mobile personenbezogene Speicher- und Verarbeitungsmedien ausgegeben werden, unterliegt die ausgebende Stelle den Transparenzpflichten des § 6c BDSG. Die Besonderheit dieser Norm liegt darin, dass sie sich an die ausgebende Stelle und nicht an die verantwortliche Stelle richtet. Es muss daher keine Mittel- oder Zweckbestimmung durch den Verpflichteten erfolgen, sondern es reicht aus, dass dieser das Speicher- oder Verarbeitungsmedium an den Betroffenen übergibt, aushändigt oder versendet und damit zur ausgebenden Stelle wird.[121]

Bei datenverarbeitenden Fahrzeugen handelt es sich um mobile personenbezogene Speicher- und Verarbeitungsmedien. Der Begriff ist in § 3 Abs. 10 BDSG legaldefiniert. Es handelt sich um Datenträger, die an den Betroffenen ausgegeben werden, auf denen eine Verarbeitung über die reine Speicherung hinaus stattfindet und bei denen die Verarbeitung nur durch den Gebrauch des Mediums beeinflusst werden kann.

Datenverarbeitende Fahrzeuge werden an die Betroffenen übergeben und somit ausgegeben.

Mobile personenbezogene Speicher- und Verarbeitungsmedien sind von reinen Datenträgern insbesondere dadurch abgrenzbar, dass sie über die Speicherung hinaus eine Verarbeitung von Daten auf dem Medium ermöglichen. Voraussetzung ist dafür die Ausstattung mit einem eigenen Prozessor.[122] Beispiele dafür sind SIM-Karten, RFID-Chips und Smart Cards.[123] Der Begriff ist allerdings ausdrücklich technikoffen formuliert. Es kommt daher nicht auf die Erscheinungsform des Mediums an.[124] Deshalb macht es grundsätzlich keinen Unterschied, ob das Medium in ein Fahrzeug eingebaut oder in eine Plastikkarte integriert ist.

[120] Scholz, in: Simitis, BDSG, § 6a Rn. 38 f.

[121] Scholz, in: Simitis, BDSG, § 6c Rn. 24.

[122] Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 6c Rn. 2; Scholz, in: Simitis, BDSG, § 6c Rn. 5.

[123] Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 6c Rn. 3.

[124] Scholz, in: Simitis, BDSG, § 3 Rn. 267.

Datenverarbeitende Fahrzeuge sind keine reinen Speichermedien, sondern verarbeiten personenbezogene Daten.

Soweit die Verarbeitung nur durch den Gebrauch des Fahrzeugs beeinflusst werden kann, unterfallen datenverarbeitende Fahrzeuge daher dem § 6c BDSG. Diese dritte Voraussetzung ist nur dann nicht gegeben, wenn der Betroffene durch die Eingabe von Befehlen die Datenverarbeitung beeinflussen kann. Daher ist die Norm auf Notebooks, Smartphones und Tablets nur eingeschränkt anwendbar. Soweit die Datenverarbeitung durch den Betroffenen gesteuert werden kann, ist die Norm nicht anwendbar. Soweit Bereiche aber nicht der Kontrolle des Betroffenen unterliegen und dort personenbezogene Daten verarbeitet werden, liegt die Voraussetzung vor. Für eine Steuerung der Datenverarbeitung ist nicht ausreichend, dass lediglich zwischen wenigen, vorgegebenen Alternativen ausgewählt werden kann.[125] Das gleiche gilt für Fahrzeuge. Nur soweit der Betroffene die Verarbeitung innerhalb des Fahrzeugs steuern kann, ist die Voraussetzung, dass die Verarbeitung lediglich durch den Gebrauch beeinflusst werden kann, nicht gegeben. Anderenfalls sind die Transparenzpflichten des § 6c BDSG zu erfüllen.

2.5 Vorschriften des TMG

Das TMG ist unter den Voraussetzungen, die in Kapitel 2.3.3 genannt werden, anwendbar. Die datenschutzrechtlichen Normen sind nach § 11 Abs. 1 TMG nicht anwendbar, wenn Telemediendienste in Dienst- oder Arbeitsverhältnissen zu ausschließlich beruflichen oder dienstlichen Zwecken oder ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen eingesetzt werden. Dann kommen grundsätzlich die Vorschriften des BDSG zur Anwendung.[126]

2.5.1 Grundsätze

Auch im TMG gilt das sogenannte Verbot mit Erlaubnisvorbehalt. Normiert ist es in § 12 Abs. 1 TMG. Danach dürfen Diensteanbieter personenbezogene Daten nur soweit erheben und verwenden, wie dies durch eine Rechtsgrundlage oder eine Einwilligung gerechtfertigt ist. Abs. 2 regelt, dass auch bei Telemedien der Zweckbindungsgrundsatz gilt, also eine Verarbeitung von personenbezogenen Daten für andere Zwecke ebenfalls einer Rechtsgrundlage oder einer Einwilligung bedarf.

[125] Scholz, in: Simitis, BDSG, § 6c Rn. 277.

[126] Vgl. Spindler/Schuster/Spindler/Nink, TMG, § 11 Rn. 24.

2.5.2 Unterrichtungspflicht

§ Abs. 1 TMG regelt eine Unterrichtungspflicht des Diensteanbieters gegenüber dem Nutzer. Zu Beginn des Nutzungsvorgangs muss „über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogenen Daten sowie über die“ Verarbeitung von personenbezogenen Daten in einem Staat außerhalb des Anwendungsbereichs der Datenschutzrichtlinie in allgemeinverständlicher Form unterrichtet werden.

Zweck der Regelung ist die für den Nutzer transparente Nutzung des Telemediendienstes.[127] Sie muss „zu Beginn des Nutzungsvorgangs“ erfolgen, also nicht schon vor dem Nutzungsvorgang.[128]

2.5.3 Elektronische Einwilligung

Für die Einwilligung im Rahmen eines Telemediendienstes regelt § 13 Abs. 2 TMG, dass die Einwilligung unter bestimmten Voraussetzungen auch elektronisch erklärt werden kann. Dazu muss sichergestellt sein, dass die Einwilligung bewusst und eindeutig erteilt wurde, die Einwilligung protokolliert wird, der Inhalt der Einwilligung durch den Nutzer jederzeit abgerufen werden kann und er die Einwilligung jederzeit widerrufen kann.

Es sind nicht die Voraussetzungen der §§ 126 Abs. 3, 126a BGB zu erfüllen. Das würde bedeuten, dass das Einwilligungsdokument mit einer qualifizierten elektronischen Signatur zu versehen wäre. Für eine elektronische Einwilligung gelten aber die erleichterten Voraussetzungen des § 13 Abs. 2 TMG.[129] Ein Häkchen in eine Checkbox zu setzen kann daher ausreichend sein.[130] Nicht ausreichend ist es, wenn dieses Kästchen bereits vorangekreuzt ist, da dann eine bewusste und eindeutige Handlung nicht vorliegt.[131] Schließlich könnte die Checkbox auch einfach übersehen worden sein. Somit muss ein Opt-in statt einem Opt-out stattfinden.

2.5.4 Bestandsdaten

Die Verarbeitung von Bestandsdaten richtet sich nach § 14 TMG. Bestandsdaten sind diejenigen, die für die „Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind“. Typischerweise handelt es sich um Name, Anschrift, Email-Adresse, Zahlungsart und Zahlungsdaten.[132] Was erforderlich ist, kommt auf den

[127] Spindler/Schuster/Spindler/Nink, TMG, § 13 Rn. 2.

[128] Müller-Broich, TMG, § 13 Rn. 1.

[129] Spindler/Schuster/Spindler/Nink, TMG, § 13 Rn. 13.

[130] OLG Brandenburg, Urt. v. 11.01.2006, Az. 7 U 52/05.

[131] Spindler/Schuster/Spindler/Nink, TMG, § 13 Rn. 13.

[132] Spindler/Schuster/Spindler/Nink, TMG, § 14 Rn. 3.

konkreten Nutzungsvertrag an. Wird kein Entgelt vereinbart, ist die Erhebung der Kontoverbindung beispielsweise nicht erforderlich.

2.5.5 Nutzungsdaten

Nutzungsdaten, also insbesondere Daten zur Identifikation des Nutzers, Angaben über Beginn und Ende der Nutzung und Angaben über die in Anspruch genommenen Telemedien dürfen nur erhoben und verwendet werden, soweit dies zur Nutzung oder zur Abrechnung erforderlich ist. Sie sind in § 15 TMG geregelt. Von ihnen abzugrenzen sind die Inhaltsdaten, also solche Daten, die mittels eines Telemediendienstes übermittelt werden. Bei einem Online-Formular z.B. handelt es sich bei denjenigen Daten, die in das Formular eingetragen werden, um Inhaltsdaten. Die unterfallen dem BDSG, da das TMG insoweit keine Reglung trifft.[133] Nutzungsdaten sind dagegen Daten, die allein schon durch die Nutzung des Dienstes entstehen.[134]

2.5.6 Nutzungsprofile

Für sich genommen sind einzelne Nutzungsdaten nicht sehr aussagekräftig. So ist z.B. die IP-Adresse für sich alleine für den Diensteanbieter nicht sehr interessant. Verbindet man solche Daten in Nutzungsprofilen werden dagegen Aussagen über Hobbys, Kaufverhalten oder sonstige Vorlieben und Abneigungen ermöglicht.[135] Für Werbung, Marktforschung und bedarfsgerechte Gestaltung der Telemedien dürfen nach § 15 Abs. 3 TMG pseudonyme Nutzungsprofile angelegt werden, sofern der Nutzer dem nicht widerspricht. In der Datenschutzerklärung ist auf das Widerspruchsrecht hinzuweisen.

So könnten z.B. für die bedarfsgerechte Gestaltung einer App zur Reservierung von Parkplätzen entsprechende pseudonyme Nutzungsprofile angelegt werden. Allerdings gilt für dieses dann ein strenges Zweckbindungsgebot. Nur die in § 15 Abs. 3 TMG genannten Zwecke sind zulässig.

2.5.7 Recht auf anonyme oder pseudonyme Nutzung

Die Nutzung eines Dienstes muss anonym oder pseudonym möglich sein, sofern das technisch möglich und zumutbar ist und der Nutzer muss über diese Möglichkeit informiert werden, § 13 Abs. 6 TMG. Es handelt sich um eine Konkretisierung des Gebots der Datensparsamkeit in § 3a BDSG.[136] Fraglich ist die Reichweite des Schutzes. Es wird sowohl vertreten, dass der Schutz nur gegenüber den anderen Nutzern besteht als auch, dass der Schutz auch gegenüber dem Diensteanbieter besteht. Richtigerweise besteht der

[133] Spindler/Schuster/Spindler/Nink, TMG, § 15 Rn. 3.

[134] Engel-Flechsig, DuD 1997, 8, 14.

[135] Spindler/Schuster/Spindler/Nink, TMG, § 15 Rn. 9.

[136] Spindler/Schuster/Spindler/Nink, TMG, § 13 Rn. 21.

Schutz auch gegenüber dem Diensteanbieter, da dieser eine namentliche Registrierung nur dann verlangen kann, wenn dies für das Vertragsverhältnis erforderlich ist, § 14 Abs. 1 TMG. Außerdem soll das Gebot der Datensparsamkeit auch insbesondere vor dem Diensteanbieter schützen.[137]

2.5.8 TOM nach § 13 Abs. 4 TMG

Nach § 13 Abs. 4 TMG ist durch technische und organisatorische Maßnahmen sicherzustellen, dass die Nutzung des Dienstes jederzeit beendet werden kann, dass Nutzungsdaten unmittelbar nach Beendigung der Nutzung gelöscht oder gesperrt werden, dass Dritte keine Kenntnis von der Telemediennutzung nehmen können, dass eine Verkettung von personenbezogenen Daten über mehrere Dienste hinweg nicht möglich ist, dass Nutzungsdaten nur für Abrechnungszwecke zusammengeführt werden können und Nutzungsprofile nicht mit Angaben zur Identifikation des Nutzers zusammengeführt werden können. In Kapitel 3 wird beschrieben, wie dies umgesetzt werden kann.

2.6 Vorschriften des TKG

Das TKG ist unter den in Kapitel 2.3.2 genannten Voraussetzungen bei vernetzten Fahrzeugen anwendbar.

2.6.1 Fernmeldegeheimnis

Das Fernmeldegeheimnis ist in § 88 TKG normiert. Es handelt sich um die einfachgesetzliche Ausprägung des oben dargestellten Fernmeldegeheimnisses aus Art. 10 GG. Während Art. 10 GG allerdings nur den Staat adressiert, richtet sich das TKG an Diensteanbieter, [138] also diejenigen, die Telekommunikationsdienstleistungen erbringen oder daran mitwirken. Der Staat kommt damit seiner Pflicht zum Schutz des grundrechtlichen Fernmeldegeheimnisses nach.[139]

2.6.1.1 Kenntnisnahmeverbot

Nach § 88 Abs. 3 TKG ist es den Diensteanbietern verboten, sich über das erforderliche Maß zur Erbringung des Dienstes oder zum Schutz der technischen Systeme Kenntnis vom Inhalt oder den Umständen der Kommunikation zu verschaffen. Die näheren Umstände erfassen zumindest alle Verkehrsdaten, also beispielsweise die in § 96 TKG genannten Anschlussnummern, Standortdaten, Beginn und Ende der Verbindung. Zu den Inhalten

[137] Schnabel/Freund, CR 2010, 718, 719.

[138] In diesem Kapitel bezeichnet „Diensteanbieter“ Diensteanbieter im Sinne des TKG.

[139] Geppert/Schütz/Bock, BeckTKG-Komm, § 88, Rn. 1; Spindler/Schuster/Eckhardt, TKG, § 88 Rn. 1.

der Kommunikation im Sinne dieser Norm zählt alles, was durch den Telekommunikationsvorgang ausgesandt, übermittelt oder empfangen wird.[140]

2.6.1.2 Zweckbindung

Alle Tatsachen, die unter das Fernmeldegeheimnis fallen, dürfen nur für Zwecke der Erbringung des Dienstes oder den Schutz der technischen Systeme verwendet werden. Also selbst wenn es erforderlich ist, dass ein Diensteanbieter von Inhalten oder Umständen der Telekommunikation Kenntnis nimmt, darf er diese nicht zweckentfremden.[141]

2.6.2 Bestandsdaten

Die Rechtsgrundlage für die Erhebung von Bestandsdaten findet sich in §§ 95, Abs. 3 Nr. 3 TKG. Ein Diensteanbieter darf Bestandsdaten erheben und verwenden, soweit dies zur Begründung, inhaltlichen Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erforderlich ist, wobei Bestandsdaten solche Daten sind, die für diesen Zweck erhoben werden.

Dabei handelt es sich um Daten, welche zur Identifikation des Teilnehmers und für Abrechnungszwecke genutzt werden. Typischerweise also Name und Vorname, Geburtsdatum und –ort, Adresse und Bankverbindung.[142] Nach Abs. 2 dürfen diese Daten für die Beratung von Teilnehmern, für Werbung für eigene Angebote, für Marktforschung verwenden, sofern der Teilnehmer eingewilligt hat und die Verwendung für diese Zwecke erforderlich ist. Sollten die an der Vernetzung von Fahrzeugen beteiligten Diensteanbieter solche Maßnahmen durchführen wollen, müssen sie hierfür die Einwilligung der Betroffenen einholen.

Nach Abs. 3 sind die Bestandsdaten nach Vertragsende mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen.

2.6.3 Verkehrsdaten

Verkehrsdaten sind nach § 3 Nr. 30 TKG solche Daten, die bei der Erbringung von Telekommunikationsdiensten erhoben, verarbeitet oder genutzt werden. Davon umfasst sind z.B. Kennnummern von Anschlüssen oder Endeinrichtungen, Standortkennungen von Absendern und Empfängern, Zeitpunkte und Dauer von Verbindungen und übermittelte Datenmengen, das verwendete Protokoll sowie das Format der Nachricht. [143] Die

[140] Spindler/Schuster/Eckhardt, TKG, § 88 Rn. 10.

[141] Spindler/Schuster/Eckhardt, TKG, § 88 Rn. 35.

[142] Graf/Graf, BeckOK StPO, TKG, § 95 Rn. 3.

[143] Spindler/Schuster/Ricke, TKG, § 3 Rn. 49.

Erhebung von Verkehrsdaten ist in § 96 Abs. 1 TKG geregelt. Die Erforderlichkeit der Erhebung von Verkehrsdaten bestimmt sich nach der Ausgestaltung des Telekommunikationsdienstes.[144]

Zum Zwecke der Entgeltermittlung und Entgeltabrechnung dürfen Verkehrsdaten verwendet werden, soweit sie dafür benötigt werden, § 97 Abs. 1 TKG.

Darüber hinaus können Verkehrsdaten mit Einwilligung des Betroffenen auch zu Zwecken der Vermarktung der Dienste, zur bedarfsgerechten Gestaltung der Dienste und zur Bereitstellung von Diensten mit Zusatznutzen verwendet werden, § 96 Abs. 3 TKG. Die Verkehrsdaten sind allerdings unverzüglich zu anonymisieren, also der Personenbezug zu entfernen, was vor dem Hintergrund des Erforderlichkeitsmaßstabs eine Selbstverständlichkeit sein sollte.

Die Verkehrsdaten sind unverzüglich zu löschen, § 96 Abs. 1 S. 3 TKG. Maßgeblicher Zeitpunkt ist die Beendigung der Verbindung. Von diesem Zeitpunkt an sind die Daten ohne schuldhaftes Zögern zu löschen, sofern die weitere Speicherung der Daten nicht für einen nach § 96 Abs. 1 TKG anerkannten Zweck weiterhin erforderlich ist.[145]

2.6.4 Standortdaten

§ 98 TKG regelt die Verarbeitung von Standortdaten. Sie dürfen verarbeitet werden, wenn dies für einen Dienst mit Zusatznutzen erforderlich ist und die Daten entweder anonymisiert wurden oder eine Einwilligung des Teilnehmers vorliegt.

Standortdaten sind Daten, die sich auf den Standort des Endgerätes beziehen. Sie können sich aus geographischer Länge, Breite und Höhe, den Grad der Genauigkeit, die Identifikation des Netzpunktes und den Zeitpunkt zusammensetzen.[146] Standortdaten sind besonders sensibel, weil sich aus ihnen Bewegungsprofile erstellen lassen, die Aussagen über Gewohnheiten, soziale Beziehungen und zukünftiges Verhalten ermöglichen.[147] So können Besuche in einem Krankenhaus, an religiösen Orten oder politischen Veranstaltungen nachvollziehbar werden.[148] Dies gilt auch für vernetzte Fahrzeuge. Die Benutzung von Fahrzeugen ist eng mit dem Alltag einer Vielzahl von Bürgern verknüpft. Solche Daten können auch in Gerichtsprozessen eine große Rolle

[144] Spindler/Schuster/Eckhardt, TKG, § 96 Rn. 3.

[145] Spindler/Schuster/Eckhardt, TKG, § 96 Rn. 4.

[146] Geppert/Schütz/Bock, BeckTKG-Komm, § 98, Rn. 1.

[147] Geppert/Schütz/Bock, BeckTKG-Komm, § 98, Rn. 1; Art. 29-Datenschutzgruppe, WP 185, S. 7.

[148] Art. 29-Datenschutzgruppe, WP 185, S. 8.

spielen, insbesondere wenn sich aus ihnen Wegstrecken und Geschwindigkeiten ermitteln lassen und so z.B. der Schuldnachweis bei Unfällen geführt werden kann.[149]

Allerdings ist § 98 TKG nur dann anwendbar, wenn ein Dienst im Zusammenhang mit der Erbringung eines Telekommunikationsdienstes und durch den Telekommunikationsdienstebetreiber erfolgt. Auf gesondert erhobene Standortdaten wie z.B. GPS und deren Nutzung durch Telemediendienste ist § 98 TKG nicht anwendbar, weshalb der Anwendungsbereich der Norm nicht besonders groß sein dürfte.[150]

Auch wenn der jeweilige Teilnehmer eine Einwilligung gegeben hat, muss ihm nach § 98 Abs. 2 TKG die Möglichkeit gegeben werden, die Verarbeitung auf einfache Weise unentgeltlich zeitweise zu untersagen.

2.6.5 Informationspflichten

Die an der Vernetzung von Fahrzeugen und Infrastruktur beteiligten Diensteanbieter müssen die Teilnehmer bei Vertragsschluss nach § 93 TKG über Art Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten unterrichten. Dies muss in einer allgemeinverständlichen Form geschehen und die Teilnehmer sind auf Wahl und Gestaltungsmöglichkeiten hinzuweisen. Die Informationspflichten dienen dem Transparenzgrundsatz.

Es muss nicht über alle technischen Einzelheiten des Telekommunikationsnetzes aufgeklärt werden aber es genügt auch nicht nur Informationen über wenige Datenverarbeitungstatbestände bereit zu stellen. Die Information soll so erfolgen, dass der Betroffene sein Recht auf informationelle Selbstbestimmung ausüben kann.[151] Um dies zu erreichen sollten die Datenarten genannt und erklärt werden, erläutert werden, dass ggf. Verbindungsdaten für die Rechnungserstellung benötigt werden oder die Nutzung von Daten zur Erkennung und Beseitigung von Störungen und zur Unterbindung von Leistungserschleichungen erfolgt.[152]

[149] Vgl. LG Köln, Urt. v. 23.05.2016, Az. 113 KLs 34/15.

[150] Weichert, SVR 2014, 201, 206; Vgl. auch Steidle, MMR 2009, 167, 168 f.

[151] Geppert/Schütz/Bock, BeckTKG-Komm, § 93, Rn. 25.

[152] Geppert/Schütz/Bock, BeckTKG-Komm, § 93, Rn. 26 ff.

3 TECHNISCHER DATENSCHUTZ

Nach § 9 BDSG sind technische und organisatorische Maßnahmen zu treffen um die Anforderungen des BDSG und der Anlage zu § 9 BDSG zu erfüllen. Durch die Maßnahmen soll ein angemessenes Schutzniveau hergestellt werden. In der Anlage zu § 9 S. 1 BDSG werden zu treffende Maßnahmen genannt. Dabei handelt es sich um Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und die Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden. Allerdings sind diese Maßnahmen nach dem Wortlaut nur „insbesondere“ zu treffen, weshalb die Aufzählung nicht abschließend ist.

Es bedarf daher einer systematischen Herangehensweise um technische und organisatorische Maßnahmen zu entwickeln. Der technische Datenschutz lässt sich mit dem Standard-Datenschutzmodel (SDM)[153] entwickeln. Das Modell wurde von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 einstimmig zustimmend zur Kenntnis genommen. Es dient dazu, abstrakte datenschutzrechtliche Anforderungen in konkrete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu überführen.

Zugunsten von technikoffenen Regelungen sind datenschutzrechtliche Normen hochgradig abstrakt. Dies ist zwar aus Sicht des Gesetzgebers sinnvoll, – würde er sehr genaue und technikspezifische Vorschriften erlassen, wäre er nur noch damit beschäftigt, auf technische Änderungen zu reagieren – führt aber zu Rechtsunsicherheit.[154] Das SDM ist eine Methode, mit der Risiken für das Recht auf informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten durch technische und organisatorische Maßnahmen reduziert werden können.[155]

Dazu haben die Aufsichtsbehörden im SDM sieben Gewährleistungsziele definiert, Verfahren in Daten, IT-Systeme und Prozesse gegliedert, drei unterschiedliche Schutzbedarfe definiert und werden in einem Anhang einen Katalog von standardisierten Schutzmaßnahmen veröffentlichen. [156] So soll der Weg von abstrakten datenschutzrechtlichen Anforderungen zu konkreten Maßnahmen zum Schutz der Betroffenen gegangen werden.

[153] SDM, V.1.0.

[154] Vgl. zur DSGVO Roßnagel/Nebel/Richter, ZD 2015, 455, 460.

[155] SDM, V.1.0, S. 6.

[156] SDM, V.1.0, S. 10.

3.1 Gewährleistungsziele

Gewährleistungsziele nach dem SDM beschreiben Eigenschaften eines Verfahrens, die vorliegen und durch technische und organisatorische Maßnahmen gewährleistet werden müssen. Dadurch wird eine normgerechte Verarbeitung ermöglicht.[157] Die Aufstellung der Datenschutzmaßnahmen lässt sich anhand dieser Gewährleistungsziele systematisieren. Es handelt sich um das grundlegende Gewährleistungsziel Datenminimierung, die drei aus der IT-Sicherheit bekannten Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit sowie die Datenschutz-Gewährleistungsziele Nichtverkettung, Transparenz und Intervenierbarkeit.

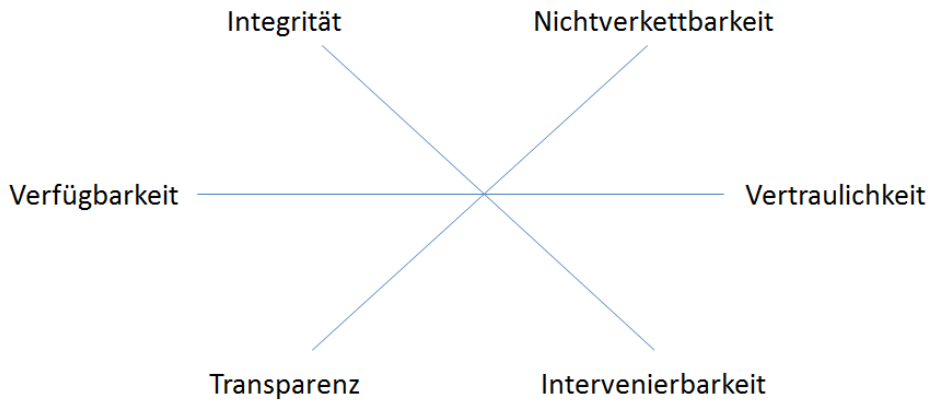

Abbildung 1: Typische Darstellung der Gewährleistungsziele

Das Verhältnis zwischen den Gewährleistungszielen ist nicht konfliktfrei. Bei den Gewährleistungszielen Vertraulichkeit und Verfügbarkeit leuchtet dies sofort ein. Maßnahmen, welche die Vertraulichkeit erhöhen, schränken die Verfügbarkeit zumindest für bestimmte Personen ein. Allerdings entstehen nicht nur auf den oben dargestellten Achsen Wechselwirkungen zwischen den Schutzzielen. Um z.B. sinnvoll intervenieren zu können, muss man ein System verstehen, was Transparenz voraussetzt. Transparenz wiederum kann sich negativ auf die Vertraulichkeit auswirken, wenn dadurch Geheimnisse offenbar werden, welche für die IT-Sicherheit wichtig sind. Die Gewährleistungsziele haben den Vorteil, diese Konflikte bei der Entwicklung von Systemen zu offenbaren und schaffen damit die Möglichkeit, dass diese Konflikte in einem Entwicklungsprozess einer Lösung zugeführt werden.[158]

[157] SDM, V.1.0, S. 10.

[158] Hansen, Jensen, Rost, IWPE, 159, 160 f.

3.1.1 Datenminimierung

Das Gewährleistungsziel Datenminimierung wird im SDM als grundlegend bezeichnet und damit besonders herausgehoben. Durch dieses Ziel wird der datenschutzrechtliche Grundsatz der Erforderlichkeit operationalisiert. Bei keinem Verarbeitungsschritt sollen mehr Daten erhoben, verarbeitet, gespeichert oder genutzt werden, als für das Erreichen eines Zweckes erforderlich ist.[159]

3.1.2 Verfügbarkeit

Das Gewährleistungsziel Verfügbarkeit zielt darauf ab, dass personenbezogene Daten zur Verfügung stehen und ordnungsgemäß verwendet werden können. Berechtigte sollen Zugriff auf die personenbezogenen Daten haben und personenbezogene Daten auffinden können.[160]

3.1.3 Integrität

Integrität als Gewährleistungsziel fordert die Einhaltung der für Prozesse und Systeme vorgesehenen Spezifikationen und den Schutz von personenbezogenen Daten vor unbeabsichtigter Zerstörung, Verfälschung. Personenbezogene Daten sollen aktuell, vollständig und richtig sein. Es müssen Möglichkeiten bestehen, Daten zu korrigieren und zu aktualisieren. [161]

3.1.4 Vertraulichkeit

Vertraulichkeit ist dann gegeben, wenn Unbefugte personenbezogene Daten nicht zur Kenntnis nehmen können. Aus Sicht des Datenschutzes können Unbefugte nicht nur Personen außerhalb der verantwortlichen Stelle sein, sondern auch Personen innerhalb der verantwortlichen Stelle, deren Kenntnisnahme der personenbezogenen Daten nicht erforderlich ist.[162]

3.1.5 Nichtverkettung

Das Gewährleistungsziel Nichtverkettung fordert, dass der Grundsatz der Zweckbindung eingehalten wird. Daten dürfen grundsätzlich nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Ein Unterlaufen der Zweckbindung soll technisch und organisatorisch ausgeschlossen werden. Besondere Risiken für die Nichtverkettung

[159] SDM, V.1.0, S. 11 ff.

[160] SDM, V.1.0, S. 13.

[161] SDM, V.1.0, S. 13.

[162] SDM, V.1.0, S. 13 f.

entstehen aus einer hohen Aussagekräftigkeit und der besonderen Größe von Beständen personenbezogener Daten.[163]

3.1.6 Transparenz

Transparenz fordert, dass Betroffene, verantwortliche Stellen und Aufsichtsbehörden personenbezogene Verfahren in einem jeweils angemessenen Maße verstehen können. Besonders wichtig ist dabei die Information, welche Daten für welche Zwecke erhoben und verarbeitet werden, welche Systeme und Prozesse dabei zum Einsatz kommen und zwischen welchen Entitäten welche Daten übertragen werden. Bei mehreren involvierten Entitäten muss erkennbar sein, wer wofür verantwortlich ist. Transparenz ist eine Voraussetzung für die Erkennung von Mängeln.[164]

3.1.7 Intervenierbarkeit

Das Gewährleistungsziel Intervenierbarkeit zielt auf die technische und organisatorische Umsetzung der Betroffenenrechte (Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung) ab. Dies setzt voraus, dass die verantwortliche Stelle in den Verarbeitungsprozess eingreifen kann. [165] Voraussetzung dafür ist, dass die verantwortliche Stelle ihre Systeme beherrscht.[166]

3.1.8 Zwischenfazit

Diese systematische und umfassende Herangehensweise an den Datenschutz über die Gewährleistungsziele macht vor allem eines sehr deutlich: Momentan geht die Diskussion um Datenschutz durch Privacy by Design beim vernetzten Fahrzeug in die falsche Richtung. Die Ziele des Datenschutzes werden unzulässig verkürzt, wenn man ihn auf die Herstellung von Transparenz und die Gewährleistung von Wahlmöglichkeiten reduziert. [167] Damit werden nur zwei der oben genannten Schutzziele angesprochen, nämlich Transparenz und Intervenierbarkeit, wobei auch die Intervenierbarkeit nur auf Wahlmöglichkeiten verkürzt wird. Die aus Sicht des Datenschutzes besonders relevanten Schutzziele der Nicht-Verkettbarkeit und Datensparsamkeit werden allerdings vollständig missachtet. Das Projekt iKoPA leistet hier einen wertvollen Beitrag, indem es datensparsame, nicht-verkettbare Lösungsmöglichkeiten aufzeigt.

---

[163] SDM, V.1.0, S. 14 f.

[164] SDM, V.1.0, S. 15.

[165] SDM, V1.0, S. 15.

[166] Bock/Rost, DuD 2011, 30, 32.

[167] Verband der Automobilindustrie, Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten, Positionspapier vom 19.09.2016.

3.2 Der Verfahrensbegriff

Das BDSG soll nach § 1 Abs. 1 den Einzelnen vor Beeinträchtigungen beim Umgang mit seinen Daten schützen. Der Umgang mit Daten erstfasst das Erheben, die Verarbeitung und die Nutzung von Daten.[168] Im Kontext des technischen und organisatorischen Datenschutzes ist ein angemessener Verfahrensbegriff notwendig, um den Untersuchungsgegenstand bestimmen zu können. Das SDM definiert daher ein Verfahren als aus drei Komponenten bestehend, nämlich den personenbezogenen Daten, den beteiligten technischen Systemen und die Prozesse innerhalb derer die Daten verarbeitet werden.[169] So sollen für alle Komponenten eines Verfahrens angemessene Schutzmaßnahmen gefunden werden können.[170]

3.3 Schutzbedarf

Nach § 9 S. 2 BDSG muss der Aufwand für die Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Damit wird dem Grundsatz der Verhältnismäßigkeit Genüge getan, indem hinsichtlich der zu treffenden technischen und organisatorischen Maßnahmen eine Einzelfallbetrachtung ermöglicht wird.[171] Das Standard-Datenschutzmodell ermöglicht diese Einzelfallbetrachtung über die Feststellung des Schutzbedarfs. Dazu wird festgestellt, ob ein normaler, ein hoher oder ein sehr hoher Schutzbedarf vorliegt.[172] Im Unterschied zur IT-Sicherheit ist für die Feststellung des datenschutzrechtlichen Schutzbedarfs die Betroffenenperspektive maßgeblich.[173]

Ein normaler Schutzbedarf liegt bei jeder Verarbeitung personenbezogener Daten vor. Der Grund dafür ist, dass jede Verarbeitung personenbezogener Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Nach dem Bundesverfassungsgericht gibt es „unter den Bedingungen der automatischen Datenverarbeitung“ kein belangloses Datum.[174]

Ein hoher oder sehr hoher Schutzbedarf ist dann festzustellen, wenn der Eingriff in das Grundrecht auf informationelle Selbstbestimmung eine erhöhte Intensität aufweist. Dies

[168] Vgl. Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 1 Rn. 22.

[169] SDM, V.1.0, S. 34 f.

[170] Rost, DuD 2012, 433, 435.

[171] Gola/Schomerus/Gola/Klug/Körffer, BDSG, § 9 Rn. 7 ff.

[172] SDM, V.1.0, S. 37.

[173] SDM, V.1.0, S. 36.

[174] BVerfGE 65, 1, 43.

ist durch eine Betrachtung des Einzelfalls zu bestimmen, es können allerdings Kriterien genannt werden, die für eine erhöhte Eingriffsintensität sprechen.

Dies kann der Fall bei biometrischen Daten oder anderen Daten, die lebenslang als Anker für eine Verkettung von Daten dienen können, sein. Anderen Daten wie KFZ-Kennzeichen oder Fahrzeugidentifikationsnummern bleiben über einen langen Zeitraum einer Person zugeordnet und können über diesen Zeitraum Anker für die Verkettung von Daten sein. Ein Verfahren kann auch deshalb besonders eingriffsintensiv sein, weil es möglicherweise Auswirkungen auf die finanzielle Situation, das Ansehen oder die körperliche Unversehrtheit des Betroffenen haben kann. Ein Verfahren kann auch die Gefahr bergen, dass es das Verhalten einer Vielzahl von Betroffenen beeinflusst, z.B. bei einer flächendeckenden Videoüberwachung.[175] Eine erhöhte Eingriffsintensität kann sich auch aus der Vielzahl der betroffenen Personen[176] oder einer Vielzahl von Daten über eine einzelne Person ergeben, die dann ein vollständigeres Bild über eine Persönlichkeit abgeben können.[177]

Der Schutzbedarf von Daten, die im Zusammenhang mit vernetzten Fahrzeugen entstehen lässt sich anhand dieser Kriterien gut bestimmen. Ein hoher Schutzbedarf ist immer dann anzunehmen, wenn Positionsdaten verarbeitet werden. Diese erlauben umfassende Einblicke in den Alltag, es lassen sich z.B. Rückschlüsse auf Hobbies, besuchte Ärzte oder Teilnahmen an Demonstrationen ziehen. Werden viele verschiedene Dienste für das das vernetzte Fahrzeug über den gleichen Service Provider angeboten, kann dieser Service Provider einen umfassenderen Einblick in die Fahrzeugnutzung der Betroffenen gewinnen. Aber auch ein Service Provider, der einen Dienst für eine sehr große Anzahl Betroffener bereitstellt, hat einen erhöhten Schutzbedarf zu erfüllen. Vor diesem Hintergrund sind die im Bereich des vernetzten Fahrzeugs zu beobachtenden Zentralisierungstendenzen[178] kritisch zu sehen. Sie führen dazu, dass an den zentralen Kommunikationsknoten ein sehr hoher Schutzbedarf entsteht. Aber auch andere Tendenzen, wie die Erhebung von Gesundheitsdaten, z.B. durch Alkoholmessgeräte oder biometrischen Daten (Fingerabdrucksensoren) durch die Fahrzeug-IT treiben den Schutzbedarf nach oben.

[175] Vgl. SDM, V.1.0, S. 37 f.

[176] Vgl. BVerfG, Urt. v. 02.03.2010, Az.: 1 BvR 256/08, Rn. 210.

[177] BVerfGE 65, 1, 42.

[178] Vgl. VDA, Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten, abrufbar unter https://www.vda.de/de/themen/innovation-und-technik/vernetzung/Zugang-zum-Fahrzeug-und-zu-im-Fahrzeug-generierten-Daten.html

Ein erhöhter Schutzbedarf hat zur Folge, dass die verantwortliche Stelle einen erhöhten Aufwand bei den Maßnahmen treiben muss und mehr Ressourcen (z.B. Zeit, Geld) für die Entwicklung, Implementierung und Überwachung der Maßnahmen bereitzustellen hat.

3.4 Maßnahmen

Der Maßnahmenkatalog findet sich in iKoPA Deliverable D1v1 und ist anhand der hier dargelegten Methodik entstanden.

4 LITERATURVERZEICHNIS

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.), Das Standard-Datenschutzmodell, V.1.0 2016, zitiert als: SDM, V.1.0.

Ambrock, Jens, Nach Safe Harbor: Schiffbruch des transatlantischen Datenverkehrs?, Neue Zeitschrift für Arbeitsrecht (NZA) 2015, S. 1493-1497, zitiert als: Ambrock, NZA 2015.

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20.06.2007, WP 136, zitiert als: Art.-29-Datenschutzgruppe, WP 136.

Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, 16.02.2010, WP 169, zitiert als: Art.-29-Datenschutzgruppe, WP 169.

Artikel-29-Datenschutzgruppe, Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, 16.05.2011, WP 185, zitiert als: Art-29-Datenschutzgruppe, WP 185.

Bamberger, Georg/Roth, Herbert (Hrsg.), Beck’scher Online-Kommentar BGB, 41. Edition Stand 01.11.2016, zitiert als: Bamberger/Roth/Bearbeiter, BeckOK BGB

Bartelt, Andreas/Eisenmann, Susanne/Ihle, Markus, Langzeitabsicherung von Automobilen, Datenschutz und Datensicherheit (DuD) 2017, S. 211-216, zitiert als: Bartelt et al., DuD 2017, 211.

Bock, Kirsten/Engeler, Malte, Die verfassungsrechtliche Wesensgehaltsgarantie als absolute Schranke im Datenschutzrecht, Deutsches Verwaltungsblatt (DVBl) 2016, S. 593-599, zitiert als: Bock/Engeler, DVBl 2015.

Buchner, Benedikt, Datenschutz im vernetzten Automobil, Datenschutz und Datensicherheit (DuD) 2015, S. 372-377, zitiert als: Buchner, DuD 2015.

Calliess, Christian/Ruffert, Matthias (Hrsg.), Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 5. Aufl., München 2016, zitiert als: Calliess/Ruffert/Bearbeiter, AEUV.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Bundesdatenschutzgesetz, 4. Aufl., Frankfurt am Main 2014, zitiert als: DKWW/Bearbeiter, BDSG.

Enev, Miro/Takakuwa, Alex/Koscher, Karl/Kohno, Tadayoshi, Automobile Driver Fingerprinting, Proceedings on Privacy Enhancing Technologies (PoPETs) 2016, S. 34-51, zitiert als: Enev et al., PoPETs 2016.

Engel-Flechsig, Stefan, „Teledienstedatenschutz”, Datenschutz und Datensicherheit (DuD) 1997, S. 8-16, zitiert als: Engel-Flechsig, DuD 1997.

Fünfrocken, Manuel/Gashimov, Dimitrij/Küfner, Mathias/Petri, Richard/Rachinski, Delian/Robrahn, Rasmus/Schmid, Andreas/Schmidt, Matthias/Schünemann, Björn/Sturm, Mats/Vogt, Jonas/Walters, Eckhard/Wolniak, Niclas/Zwingelberg, Harald, iKoPA Deliverable D1v1 – Requirements Analysis and System Architecture, 2017, zitiert als: Fünfrocken et al., iKoPA D1v1.

Geppert, Martin/Schütz, Raimund, Beck'scher TKG-Kommentar, 4. Aufl. München 2013, zitiert als: Geppert/Schütz/Bearbeiter, BeckTKG-Komm.

Gersdorf, Hubertus/Paal, Boris (Hrsg.), Beck'scher Online-Kommentar Informations und –Medienrecht, 15. Edition, Stand 01.02.2017, München, zitiert als: Gersdorf/Paal/Bearbeiter, BeckOK InfoMedienR.

Gola, Peter/Schomerus, Rudolf (Hrsg.), BDSG, 12. Aufl., München 2015, zitiert als: Gola/Schomerus/Bearbeiter, BDSG.

Graf, Jürgen-Peter (Hrsg.), Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 27. Edition, Stand 01.01.2017 München, zitiert als: Graf/Bearbeiter, BeckOK StPO.

Hansen, Marit/Jensen, Meiko/Rost, Martin, Protection Goals for Privacy Engineering, 2015 International Workshop on Privacy Engineering (IWPE), Security and Privacy Workshops (SPW), 2015 IEEE, S. 159-166, zitiert als: Hansen, Jensen, Rost, IWPE 2015, 159.

Hansen, Marit, Das Netz im Auto & das Auto im Netz, Datenschutz und Datensicherheit (DuD), 2015, S. 367-371, zitiert als: Hansen, DuD 2015.

Hoeren, Thomas, Dateneigentum, Multimedia und Recht (MMR) 2013, S. 486-491, zitiert als: Hoeren, MMR 2013

Hornung, Gerrit, Verfügungsrechte an fahrzeugbezogenen Daten, Datenschutz und Datensicherheit (DuD), 2015, S. 359-366, zitiert als: Hornung, DuD 2015.

Jarass, Hans D., Charta der Grundrechte der europäischen Union, 3. Aufl. 2016, zitiert als: Jarass, GrCh.

Karaboga, Murat/Matzner, Tobias/Morlok, Tina/Pittroff, Fabian/Nebel, Maxi/Ochs, Carsten/von Pape, Thilo/Pörschke, Julia Victoria/Schütz, Philip/Fhom, Hervais Simo, Das Versteckte Internet, Juli 2015, zitiert als: Karaboga et al., Das versteckte Internet.

Keppeler, Lutz M., Der US-amerikanische Entwurf des „Security and Privacy in your Car Act", Recht der Datenverarbeitung (RDV) 2015, S. 299-306, zitiert als Keppeler, RDV 2015.

Kiometzis, Michael/Ullmann, Markus, Fahrdaten für alle?, Datenschutz und Datensicherheit (DuD) 2017, S. 227-232, zitiert als: Kiometzis/Ullmann, DuD 2017.

Kremer, Sascha, Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz?, Recht der Datenverarbeitung (RDV), 2014, S. 240-252. zitiert als: Kremer, RDV 2014.

Leupold, Andreas/Wiebe, Andreas, Wem gehören die Daten im Internet of Things?, Computerwoche 07.12.2016, abrufbar unter https://www.computerwoche.de/a/wem-gehoeren-die-daten-im-internet-of-things,3328337, zitiert als: Leupold/Wiebe, CW 2016.

Lüdemann, Volker, Connected Cars, Zeitschrift für Datenschutz (ZD) 2015, S. 247-254, zitiert als: Lüdemann, ZD.

Maunz, Theodor/Dürig, Günter (Hrsg.), Grundgesetz, 76. Ergänzungslieferung, München 2015, zitiert als: Maunz/Dürig/Bearbeiter, GG.

Müller-Broich, Jan D., Telemediengesetz, 1. Aufl., Baden-Baden 2012, zitiert als: Müller-Broich, TMG.

Rost, Martin, Standardisierte Datenschutzmodellierung, Datenschutz und Datensicherheit (DuD) 2012, S. 433-438, zitiert als: Rost, DuD 2012, 433.

Rost, Martin/Bock, Kirsten Privacy By Design und die Neuen Schutzziele, Datenschutz und Datensicherheit (DuD) 2011, S. 30-35, zitiert als: Bock/Rost, DuD 2011.

Roßnagel, Alexander/Schnabel, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, Neue Juristische Wochenschrift 2008, S. 3534-3538, zitiert als: Roßnagel/Schnabel, NJW 2008.

Roßnagel, Alexander, Fahrzeugdaten – wer darf über sie entscheiden?, Straßenverkehrsrecht (SVR) 2014, S. 281-287, zitiert als: Roßnagel, SVR 2014.

Roßnagel, Alexander, Grundrechtsausgleich beim vernetzten Automobil, Datenschutz und Datensicherheit (DuD) 2015, S. 353 – 358, zitiert als: Roßnagel, DuD 2015, 353.

Roßnagel, Alexander/Nebel, Maxi/Richter, Philipp, Was bleibt vom Europäischen Datenschutzrecht?, Zeitschrift für Datenschutz (ZD) 2015, S. 455 – 460, zitiert als: Roßnagel/Nebel/Richter, ZD 2015, 455.

Roßnagel, Alexander/Geminn, Christian/Jandt, Silke/Richter, Philipp, Datenschutzrecht 2016 „Smart“ genug für die Zukunft?, Kassel 2016, zitiert als: Roßenagel et al., Datenschutzrecht 2016.

Rouf, Ishtiaq/Miller, Rob/Mustafa, Hossen/Taylor, Travis/Oh, Sangho/Xu, Wenyuan/Gruteser, Marco/Trappe, Wade/Seskar, Ivan, Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, http://www.winlab.rutgers.edu/~gruteser/papers/xu_tpms10.pdf, zitiert als: Rouf et al.

Schnabel, Christoph/Freund, Bernhard, „Ach wie gut, dass niemand weiß …“ – Selbstdatenschutz bei der Nutzung von Telemedienangeboten, Computer und Recht (CR) 2010, S. 718-721, zitiert als: Schnabel/Freund, CR 2010.

Schwartmann, Rolf/Hentsch, Christian-Henner, Eigentum an Daten – Das Urheberrecht als Pate für ein Datenverwertungsrecht, Recht der Datenverarbeitung (RDV) 2015, S. 221-230, zitiert als: Schwartmann/Hentsch, RDV 2015.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl, Baden-Baden 2014, zitiert als: Bearbeiter, in: Simitis, BDSG.

Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien, 3. Aufl. München 2015, zitiert als: Spindler/Schuster/Bearbeiter, TKG.

Steidle, Roland, Datenschutz bei Nutzung von Location Based Services im Unternehmen, Multimedia und Recht (MMR) 2009, zitiert als: Steidle, MMR 2009.

Störing, Marc, Mein Auto, meine Daten?, c’t 2016, S. 123-131, zitiert als: Störing, c’t 2016.

Strubbe, Thomas/Thenée, Nicolas/Wieschebrink, Christian, IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen, Datenschutz und Datensicherheit (DuD) 2017, S. 233-226, zitiert als: Strubbe/Thenée/Wieschebrink, DuD 2017.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar zum BDSG, 4. Aufl., Frankfurt am Main 2010, zitiert als: Taeger/Gabel/Bearbeiter, BDSG.

Weichert, Thilo, Datenschutz im Auto –Teil 1, Straßenverkehrsrecht (SVR), 2014, S. 201-207, zitiert als: Weichert, SVR 2014.

Weichert, Thilo, Car-to-Car-Communicaton zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung, Straßenverkehrsrecht (SVR), 2016, S. 361-367, zitiert als: Weichert, SVR 2016, 361.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck’scher Online-Kommentar Datenschutzrecht, 18. Edition Stand 01.11.2016, München 2016, zitiert als: Wolff/Brink/Bearbeiter, BeckOK DatenSR.