www.jusletter-it.eu

Magnus Grünheidt

Selbstfahrende Autos unter datenschutzrechtlicher Perspektive

Technischen Fortschritt zulässig gestalten

The article deals with data protection related aspects connected with self driving cars. Along with an introductory description of the current development status as well as the accruing data of connected cars the question of whether and how the use of self driving cars can be designed in compliance with data protection will be discussed. The focus is on data protection related requirements that must be observed by the manufacturers. The legal design possibilities allowing technical developments to reconcile with data protection will be shown by the author. First and foremost, the statement is based on the EU General Data Protection Regulation (GDPR) that will be in force from 25 Mai 2018. (ah)

Category: Articles
Region: Germany
Field of law: Data Protection; Robotic

Citation: Magnus Grünheidt, Selbstfahrende Autos unter datenschutzrechtlicher Perspektive, in: Jusletter IT 24 November 2016

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

I. Ausgangssituation
II. Betroffene Daten
1. Welche Daten fallen an?
2. Personenbezogene Daten
III. Rechtsgrundlage der Datenverarbeitung
1. Telekommunikationsgesetz und Telemediengesetz
2. Art. 6 Abs. 1 DSGVO
a) Art. 6 Abs. 1 S. 1 lit. b) DSGVO
b) Art. 6 Abs. 1 S. 1 lit. f) DSGVO
3. Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO
IV. Wer ist zugriffsberechtigt?
V. Technischer Schutz
VI. Privacy by Design/Default
VII. Fazit

I. Ausgangssituation

[Rz 1] Um ein Fahrzeug selbstständig in Betrieb zu setzen, werden zahlreiche Daten benötigt, damit für die Fahrzeuginsassen eine sichere Fahrt gewährleistet und Schäden anderer Verkehrsteilnehmer vermieden werden. Denn durch den Einsatz selbstfahrender Autos soll sich vor allem, die Zahl der Unfälle und Verkehrsopfer verringern. Damit dieses Ziel erreicht wird, arbeitet die Automobilindustrie mit Hochdruck daran, den Prozess der Datenerhebung und -verarbeitung zu perfektionieren. Nur wenn die Insassen sich auf die Technik verlassen können, ist es ihnen möglich, die Zeit auch ohne ständige Beobachtung des Fahrverhaltens des Autos anderweitig zu nutzen. Darin liegt ein entscheidender Mehrwert für die Fahrer.

[Rz 2] Nach derzeitigem technischem Stand in Deutschland existieren lediglich solche Modelle, bei denen der Fahrer teilweise noch agieren muss. Die deutsche Bundesanstalt für Straßenwesen unterscheidet dabei unter anderem zwischen dem hochautomatisierten und dem vollautomatisierten Fahren.[1] Beim hochautomatisierten Fahren, das ab 2020 in Deutschland zugelassen werden soll, ist noch ein teilweises Mitwirken des Fahrers erforderlich. Das vollautomatisierte Fahren hingegen ist so ausgeklügelt und derart konzipiert, dass der Fahrer nur noch in Grenzsituationen, also seltener, eingreifen muss. Die deutsche Automobilindustrie gehört laut Bundesverkehrsminister Dobrindt im Bereich selbstfahrender Autos mit zur Weltspitze. Zurzeit wird ein Entwurf zur Änderung des deutschen Straßenverkehrsgesetzes im Zusammenhang mit vollautomatisiertem Fahren erarbeitet.[2] Der Automobilhersteller Ford z.B. will ab 2021 selbstfahrende Autos bauen.[3] Bis dahin muss die derzeitige im Auto zum Einsatz kommende Software entweder mit noch mehr Daten versorgt oder die jetzige Datenmenge technisch besser verknüpft werden.

---

1 ARD Radio Feature von Jörn Klare, 21. September 2016 (Abschied vom Faktor Mensch), http://www.ard.de/home/radio/Abschied_vom_Faktor_Mensch/3377362/index.html (alle Internetquellen zuletzt abgerufen am 15. November 2016).

2 Dietmar Neuerer, SPD verärgert über Dobrindt-Vorstoß, Handelsblatt, 4. November 2016, http://www.handelsblatt.com/politik/deutschland/automatisiertes-fahren-spd-veraergert-ueber-dobrindt-vorstoss/14790978.html; Dobrindt plant rechtliche Grundlage für autonomes Fahren, ZEIT ONLINE, 18. Juli 2016, http://www.zeit.de/mobilitaet/2016-07/bundesregierung-alexander-dobrindt-autonomes-fahren-gesetz.

3 Ford: Ab 2021 selbstfahrende Serien-Autos, AUTO BILD, 19. August 2016, http://www.autobild.de/artikel/ford-ab-2021-selbstfahrende-serien-autos-6061045.html.

[Rz 3] In jedem Fall erfolgt eine umfangreiche Erhebung und Verarbeitung von personenbezogenen Daten. Dadurch wird bereits jetzt erkennbar, dass Fahrzeug-, Fahrer- und Verkehrsdaten einen Rohstoff der Zukunft darstellen. Damit autonomes Fahren auch rechtlich Realität werden kann, muss daher auch das Datenschutzrecht hinreichend beachtet werden.

II. Betroffene Daten

1. Welche Daten fallen an?

[Rz 4] Beim Betrieb eines selbstfahrenden Autos fallen erhebliche Mengen an Daten an. Bereits heute sind in neuen Mittelklassewagen ca. 80 Sensoren verbaut.[4] Dabei fallen bis zu 25 Gigabyte Daten pro Fahrzeug an und zwar pro Stunde. Ein einfaches hochautomatisiertes Fahrzeug, bei dem ein teilweises Eingreifen des Fahrers erforderlich ist, sammelt sogar bis zu 300 Gigabyte Daten pro Stunde.[5]

[Rz 5] Um zu verstehen, wie eine solche Datenmenge anfallen kann, müssen die Datenquellen und -ströme nachvollzogen werden. Die Datenerhebung erstreckt sich von den Fahrzeugparametern, über die verbauten technischen Assistenz- und Entertainmentsysteme bis hin zur Umgebung des Fahrzeugs.

[Rz 6] In allen denkbaren Szenarien können dabei Daten erhoben werden, beispielsweise Daten zum Reifendruck und Ölstand, zur Treibstoffart, Anzahl der belegten Plätze samt Gewicht, angelegte Sicherheitsgurte, Fahrzeugtyp, Kennzeichen und Fahrzeugidentifikationsnummer. Über die Bordelektronik wird gesteuert, ob Fahrerassistenzsystemen, wie z.B. ABS aktiviert werden müssen. Navigationsgeräte können Start-, Fahr- und Ankunftszeit, Wegstrecke sowie die Geschwindigkeit aufzeichnen, konfiguriert wird es bereits jetzt per Sprachbefehl. Das gewählte Radioprogramm oder die von einer CD abgespielte Musik sowie die Lautstärke erzeugen weitere Datensätze. Mithilfe von Drucksensoren im Sitzkissen ist es möglich, die Körperhaltung zu ermitteln, während Sensoren im Lenkrad den Händedruck berechnen können.[6] Mittels eines Atemalkoholtests, der zwingend vor Starten des Motors durchlaufen werden muss, kann der Alkoholgehalt des Fahrers und damit dessen Fahrtauglichkeit geprüft werden. Erst bei Nüchternheit kann der Fahrer das Fahrzeug starten.[7] Eine ins Fahrzeuginnere gerichtete Kamera kann die Insassen überwachen. Die Klimaanlage reguliert sich nach Erfassung der Innentemperaturen selbst. Die Technik, die bei Sprachbefehlen zum Einsatz kommt, wird sich zukünftig noch weiter verbessern, sodass sich so immer mehr Systeme steuern lassen könnten.

[Rz 7] Außerhalb des Autos orientieren sich Laserscanner und Kameras an anderen Verkehrsteilnehmern, Markierungen, dem Fahrbahnrand, Ampeln, Verkehrsschildern und Baustellenbaken. Da das GPS-Signal der Navigationsgeräte zu ungenau ist, kann das selbstständige Fahren nur mithilfe von Außenkameras punktgenau gesteuert werden. Neben den Kameras sind weitere Parameter erforderlich, da die Ermittlung von Abständen und Geschwindigkeiten allein durch Kameras fehleranfällig ist. Daher ist eine Kommunikation des Autos mit anderen Fahrzeugen (Car-to-Car),

4 ARD Radio Feature von Jörn Klare, 21. September 2016 (Fn. 1).

5 Ebd.

6 Christian Wüst, Die Vermessung des Wüterichs, Spiegel ONLINE, 19. Oktober 2009, http://www.spiegel.de/spiegel/a-656024.html.

7 Ebd.

mit der Infrastruktur (Car-to-Infrastructure) sowie mit Unternehmen (Car-to-Enterprise) nötig. Der Austausch kann dabei z.B. jeweils über GSM, d. h. über das im Auto verbaute Mobilfunknetz, oder über das Internet erfolgen. Neue Mittelklassewagen sind bereits heute mit entsprechenden Kommunikationsschnittstellen ausgestattet.

[Rz 8] Durch den Datenaustausch der Fahrzeuge, die sich in unmittelbarer Umgebung befinden, zu Abstand, Fahrrichtung oder Geschwindigkeit, kann ein sichereres Fahren ermöglicht werden. Das Erkennen eines gesetzten Blinkers kann so sogar die voraussichtliche Strecke antizipiert werden mit der Folge, dass die Geschwindigkeit des eigenen Fahrzeugs aus Sicherheitsgründen reduziert wird. Der Austausch mit der Infrastruktur ermöglicht z.B. die Übermittlung der Ampellichtzeichen, von Schildern, Anzeigen von Staumeldungen usw. Unternehmen können entweder über die Infrastrukturobjekte oder per direkter Übermittlung an das eigene Auto weitere Informationen wie z.B. einer gesperrten Autobahn, der Empfehlung von Alternativrouten, oder eines Geisterfahrers übermitteln.

[Rz 9] Die Aufzählung ließe sich noch weiter ausführen, würde an dieser Stelle jedoch den Rahmen sprengen. Abschließend sei nur erwähnt, dass es, datenschutzrechtlich relevant, eine weitere Kommunikationsform, nämlich (Car-to-Home) gibt, die jedoch keinen Sicherheitsaspekten, sondern allein dem Fahrerkomfort dient. So ließe sich etwa bereits unterwegs die Heizung des heimischen Wohnzimmers einstellen (Smart Home), oder es könnte Musik vom PC geladen und abgespielt werden.

[Rz 10] Die Erhebung und Verarbeitung dieser riesigen Datenmenge muss dabei datenschutzkonform erfolgen.

2. Personenbezogene Daten

[Rz 11] Das Datenschutzrecht ist erst dann einschlägig, wenn personenbezogene Daten betroffen sind. Personenbezogene Daten sind nach Art. 4 Abs. 1 der EU-Datenschutzgrundverordnung (DSGVO) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden «betroffene Person») beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

[Rz 12] Personenbezogene Daten im Kontext zu selbstfahrenden Autos liegen demnach dann vor, wenn Rückschlüsse auf Fahrer und Beifahrer möglich sind. Wenn also z.B. auch das Kennzeichen oder die Fahrzeugidentifikationsnummer erhoben werden,[8] kann anhand dieser Angaben auf den Halter und häufig auch auf den Fahrer geschlossen werden. Zudem kann über Start- und Zielpunkte, die in ein Navigationsgerät eingegeben werden, auf Wohnumfeld und Arbeitsort geschlossen werden. Durch Abgleich der Vertragsunterlagen der Fahrzeug- oder Systemhersteller,

[8] So auch die Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26. Januar 2016, https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html.

in denen die Adresse angegeben wurde, kann so mit stetig steigender Wahrscheinlichkeit auf den Fahrer geschlossen werden.

[Rz 13] Die Datenerhebung möglicher Bewegungsprofile stellt einen besonderen Eingriff in das allgemeine Persönlichkeitsrecht dar, da diese dazu geeignet sind, den Tagesablauf des Betroffenen abzubilden und ggfls. zu überwachen. Dadurch ergeben sich für Unternehmen zahlreiche Gelegenheiten, Kaufreize zu setzen. So könnten dem Fahrer auf dem Entertainmentgerät des Fahrzeuges Werbung für umliegende Unternehmen eingeblendet oder durch das Anbieten von Rabatten, z. B. für die nächstgelegene Waschanlage, zusätzliche Kaufimpulse gesetzt werden. Der Fahrer sähe sich in diesem Fall einer permanenten Bewerbung ausgesetzt, die vielleicht sogar erst durch Einsatz eines Werbeblockers verhindert werden könnten.

[Rz 14] Durch den Einsatz von Kameras, die im Fahrzeuginneren Aufnahmen vom Fahrer machen und im Außenbereich andere Verkehrsteilnehmer und Nummernschilder filmen, können die betroffenen Personen ebenfalls identifiziert werden. Wenn ein Abgleich des im System hinterlegten Halters oder Fahrers keine Übereinstimmung ergäbe, könnten so etwaige Diebstähle verhindert und vermeintliche Täter überführt werden. Neben diesem Sicherheitsaspekt hinaus könnte jedoch auch der Gemütszustand der Fahrer, die Müdigkeit und die Fahrweise sowie die Kommunikation mit Insassen, Telefonpartnern oder über Dritte beobachtet werden. Letzteres ist nicht zuletzt wegen der sich ständig verbessernden Spracherkennungssoftware ein denkbares Szenario. Während solch ein Dienst einerseits begrüßenswert ist, indem ein Warnton und das Symbol im Armaturenbrett den Fahrer zu einer Pause anhält, sieht er sich andererseits einer ständigen Beobachtung bzw. einem ständigen Überwachungsdruck ausgesetzt.

[Rz 15] Auch der Fingerabdruck, mit dem ein Auto geöffnet oder gestartet wird, ist ein personenbezogenes Datum.

[Rz 16] Sowohl bei Videoaufnahmen als auch bei Fingerabdrücken handelt es sich um besonders schützenswerte Daten, die nur unter verschärfte Bedingungen zulässig verarbeitet werden dürfen. Nach Art. 4 Abs. 14 DSGVO handelt es sich um «biometrische Daten». Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung dieser Daten grundsätzlich verboten und nur in Ausnahmefällen zulässig.

[Rz 17] Auch die einem Auto zugewiesene IP-Adresse stellt ein personenbezogenes Datum dar, vgl. Art. 4 Abs. 1 DSVGO.

[Rz 18] Durch die Verknüpfung der Fahrzeugsysteme mit den mitgeführten Mobilfunkgeräten, sei es über Internet, oder WLAN, lassen sich so zahlreiche Daten miteinander verknüpfen, bspw. Kontaktdaten.

[Rz 19] Sobald ein Personenbezug herstellbar ist, ermöglichen die oben unter I. 1. genannten technischen Daten weitere Rückschlüsse über den Fahrer, etwa, zu welchem Zeitpunkt er an welchem Ort unterwegs ist, ob er auf Werbung reagiert oder, ob er Kontrollen am Fahrzeug unter erheblichen Sicherheitsbedenken zu lange hinauszögert. Das Fahrverhalten kann so bis ins kleinste Detail analysiert werden, so dass sich dadurch ein hinreichendes Persönlichkeitsprofil erschließen lässt.

[Rz 20] Aufgrund der bestehenden Risiken stellt sich die Frage, ob und falls ja, wie selbstfahrende Autos datenschutzkonform eingesetzt werden können.

III. Rechtsgrundlage der Datenverarbeitung

[Rz 21] Dem Datenschutzrecht liegt das Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des deutschen Grundgesetzes (GG) zugrunde. Dieses gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[9] Vor diesem Hintergrund schreibt Art. 6 Abs. 1 S. 1 lit. a), b) bzw. f) DSGVO u.a. vor, dass die Verarbeitung personenbezogener Daten nur zulässig ist, wenn die betroffene Person ihre Einwilligung erteilt hat oder die Verarbeitung für die Erfüllung eines Vertrags erforderlich bzw. die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (sog. Verbot mit Erlaubnisvorbehalt). Im Folgenden wird zunächst geprüft, ob eine spezielle Rechtsvorschrift Datenverarbeitungen im Kontext mit selbstfahrenden Fahrzeugen erlaubt.

1. Telekommunikationsgesetz und Telemediengesetz

[Rz 22] Grundsätzlich bleiben sowohl das deutsche Telekommunikationsgesetz (TKG) als auch das deutsche Telemediengesetz (TMG) neben der DSGVO bereichsspezifisch anwendbar. Ob und inwieweit das TKG und TMG neben der DSGVO Bestand haben werden, wird sich zeigen. Das TKG ist auch im vorliegenden Fall anwendbar, denn es handelt sich bei den eingesetzten Systemen im Bordcomputer des Autos um einen Telekommunikationsdienst gemäß § 3 Nr. 24 TKG. Telekommunikationsdienste sind in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Für die Systeme, die autonomes Fahren auf Grundalge einer Datenübertragung per GSM und Internet ermöglichen, wird in der Regel ein Entgelt an die Automobilhersteller zu erbringen sein, denn der reibungslose Ablauf des selbstständigen Fahrens wird hohe Kosten verursachen. Nach Schätzungen von Juniper Research wird allein die Automobilindustrie bis 2018 rund 20 Mrd. Dollar in den Telematik-Bereich investieren.[10] Für physische und digitale kommerzielle Dienstleistungen (sog. Smart Services) prognostiziert die Wirtschaftsprüfungsgesellschaft PwC bis 2020 sogar ein Umsatzvolumen von 115 Mrd. Euro.[11]

[Rz 23] Das TKG erfasst jedoch nur Bestands- und Verkehrsdaten. Auch das TMG regelt nur die Erhebung und Verarbeitung von Bestands- und Nutzungsdaten. Die Nutzungsdaten entsprechen dabei den Verkehrsdaten des TKG. Eine Berechtigung zur Erhebung und Speicherung aller sonstigen Daten neben Name, Adresse, Telefonnummer und IP-Adresse, die für ein selbstfahrendes Auto erforderlich sind, bieten damit weder das TKG noch das TMG.

[Rz 24] TKG und TMG können daher nicht als Rechtsgrundlagen herangezogen werden. Dies deckt sich mit dem Willen des Gesetzgebers, der die unter II. 1. und 2 so genannten Inhaltsdaten durch die DSGVO schützen will.

---

9 BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1.

10 Juniper Research, Press Release: Connected Car Opportunity to Reach $20 Billion by 2018 Driven by Soft Revenues, 27 May 2014, https://www.juniperresearch.com/press-release/connected-cars-pr1.

11 ARD Radio Feature von Jörn Klare, 21. September 2016 (Fn. 1).

2. Art. 6 Abs. 1 DSGVO

[Rz 25] Die Verarbeitung von Daten durch die Systemhersteller könnte durch Art. 6 Abs. 1 DSGVO legitimiert sein.

[Rz 26] Im Folgenden wird davon ausgegangen, dass Automobilhersteller gleichzeitig Systembetreiber des das autonome Fahren ermöglichenden Systems sind. Weiter wird angenommen, dass die Daten nicht auf einem internen Server des Autos gespeichert, sondern z.B. über Internet oder GSM übertragen werden, sodass der Hersteller sich die Daten beschafft. Die Datenverarbeitung i.S.d. Art. 4 Abs. 2 DSGVO findet daher durch den Hersteller statt.

a) Art. 6 Abs. 1 S. 1 lit. b) DSGVO

[Rz 27] Nach Art. 6 Abs. 1 S. 1 lit. b) DSGVO ist die Verarbeitung zulässig, wenn sie für die Erfüllung eines Vertrags erforderlich ist. Als Vertrag kommt etwa ein Kauf-, Leasing- oder Mietvertrag in Betracht. Weder für die Begründung noch für die Durchführung oder Beendigung dieser Vertragsverhältnisse ist die Verarbeitung einer Vielzahl von personenbezogenen Daten wie Autokennzeichen, Fahrerroute, IP-Adresse und fahrerbezogenen Daten erforderlich. Vielmehr sind für diese Zwecke die sog. Stammdaten, z.B. Name, Adresse, Telefonnr. und Kontodaten ausreichend, um hiermit die vertragliche Hauptforderung einfordern zu können.

b) Art. 6 Abs. 1 S. 1 lit. f) DSGVO

[Rz 28] In Betracht kommt eine zulässige Datenverarbeitung gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Voraussetzung dafür ist, dass dies zur Wahrung der berechtigten Interessen der Hersteller erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Fahrer überwiegen. Die Hersteller haben ein Interesse daran, möglichst viele personenbezogene Daten zu erheben, um anhand dieser Daten z.B. zielgerichtet Werbung zu schalten und dadurch den unternehmerischen Gewinn zu steigern. Ferner besteht ein Interesse an der Videoüberwachung des Innenraums, um mit dem Service werben zu können, zugunsten des Fahrers Diebstähle zu verhindern oder aufzudecken und durch Beobachtung des Fahrers bei Müdigkeitserscheinungen oder Abgelenktheit Hinweise erteilen zu können.

[Rz 29] Demgegenüber hat der Fahrer jedoch ein schutzwürdiges Interesse daran, nicht durch Werbung belästigt zu werden, nicht überwacht zu werden und selbstbestimmt mit seinen Daten umgehen zu wollen. Hinsichtlich der Erhebung von personenbezogenen Daten wie z.B. Fahrziel, eingelegte Pausen, Fahrzeugidentifikationsnummer, Kennzeichen, Gewicht, Musik und Gesprächsinhalte überwiegen daher die schutzwürdigen Interessen des Fahrers, ungestört und unbeobachtet am Straßenverkehr teilzunehmen und ohne Kenntnis Dritter verschiedene Orte aufzusuchen. Insbesondere vor dem Hintergrund, dass das Auto der Fortbewegung dient, könnte eine ständige Aufzeichnung personenbezogener Daten zu einem permanenten Überwachungsdruck führen, sodass die Notwendigkeit einer jeden Fahrt genau überlegt und die Mobilität dadurch im Ergebnis eingeschränkt werden könnte. Das bloß wirtschaftliche Interesse des Herstellers muss demgegenüber zurückstehen.

[Rz 30] Somit legitimiert auch Art. 6 Abs. 1 S. 1 lit. f) DSGVO nicht die Datenverarbeitung der personenbezogenen Daten.

3. Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO

[Rz 31] Letztlich kann die Datenerhebung und –verarbeitung mangels anderer Rechtsvorschrift nur durch eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a) DSGVO zulässig gestaltet werden, um Rechtssicherheit zu gewährleisten.[12] An eine rechtswirksame Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO bei Einordnung des Bordcomputers als Telemediendienst werden verschiedene Anforderungen gestellt.

[Rz 32] Vor Abgabe der Einwilligung ist der Fahrer nach Art. 5 Abs. 1 lit. a) und b) hinreichend auf die rechtmäßige Verarbeitung und die festgelegten Zwecke der Datenverarbeitung zu informieren. Die Informationspflichten sind im Einzelnen in Art. 13 DSGVO geregelt. Eine transparente Information sollte dabei u.a. Angaben über die verantwortliche Stelle und die Kategorien von Empfängern (auch solche in einem Drittland), enthalten. Außerdem müssen die erhobenen Daten einzeln genannt werden, da nur so eine hinreichende Transparenz[13] erzielt wird. Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden. Der Fahrer ist zudem über die Regelfristen für die Löschung der Daten zu informieren.

[Rz 33] Die Einwilligung muss nach Erwägungsgrund 32 der DSGVO freiwillig abgegeben werden, was dadurch erreicht werden kann, dass der Fahrer verschiedene Zusatzdienste erst nach Zustimmung nutzen kann. Zum Beispiel könnte der Fahrer darüber informiert werden, dass ein hinreichender Diebstahlschutz nur dann gewährleistet ist, wenn die Videoüberwachung des Innenraums aktiviert wird oder zusätzlich die Fahrstrecken aufgezeichnet werden. Außerdem könnte sich der Fahrer entscheiden, ob er aus Sicherheitsgründen und zur schnelleren Auffindbarkeit des Autos sein Nummernschild mitteilt. Durch den Hinweis, dass der Atemalkoholtest zu Beginn der Fahrt dem Selbstschutz dient, könnte auch so eine Einwilligung eingeholt werden. Voraussetzung ist stets, dass der Fahrer nicht in die Irre geführt, sondern transparent informiert wird, sodass eine eigenständige Entscheidung möglich bleibt.

[Rz 34] Eine Kopplung der Abgabe der Einwilligung zur Verarbeitung aller personenbezogenen Daten an die Nutzung des selbstfahrenden Autos wäre unzulässig, da in diesem Fall nicht mehr von einer Freiwilligkeit auszugehen wäre. Dieses «Kopplungsverbot» kommt in Art. 7 Abs. 4 DSGVO zum Ausdruck. Demnach läge keine Freiwilligkeit mehr vor, wenn der Fahrer vor Einsatz des Autos zwingend auch jenen Diensten zustimmen müsste, die personenbezogene Daten verarbeiten, ohne dass diese Dienste für ein selbstfahrendes Auto unbedingt erforderlich sind. Dies umfasst sämtliche «Service»-Dienste: Die Aufzeichnung der Fahrroute, die Kenntnis des Nummernschilds/FIN, Fingerabdrücke, Kamera- und Gesprächsaufzeichnungen, Gewicht des Fahrers, Druckkraft am Lenkrad usw. Diese Angaben sind nicht zwingend erforderlich. Vielmehr sollte das Auto allein durch den Kommunikationsaustausch mit anderen Autos, der Infrastruktur oder Unternehmen selbstständig fahren, sodass es auch anonym eingesetzt werden kann. Ebenso sollten die Dienste jederzeit wieder deaktiviert werden können, während der Einsatz des selbstfahrenden Autos weiterhin möglich bleibt. Die bei der Kommunikation über das Internet erforderliche IP-Adresse sollte an den drei letzten Ziffern unkenntlich gemacht werden.

---

12 So auch die Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_DatenschutzImKfz.pdf?__blob=publicationFile&v=5.

13 Ebd.

[Rz 35] Vor dem Abschluss des Kaufs, der Miete oder Leasings sollte dem Fahrer anschaulich verdeutlicht werden, welche Dienste unabdingbar für den Betrieb des selbstfahrenden Autos sind und bei welchen Diensten es sich um Zusatzdienste handelt, die hinzu- und jederzeit wieder abgewählt werden können und bei denen personenbezogene Daten erhoben und verarbeitet werden. Dass dieses Vorgehen einen hohen Gestaltungsaufwand mit sich bringt, liegt auf der Hand.

[Rz 36] Wenn besonders sensible Datenarten (Fingerabdrücke, Videoaufzeichnungen, aber auch Gesprächsaufzeichnungen über politische Meinungen, religiöse oder weltanschauliche Überzeugungen) verarbeitet werden sollen, muss sich die Einwilligung gem. Art. 9 Nr. 2 lit. a) DSGVO ausdrücklich auch auf die Verarbeitung dieser Daten beziehen.

[Rz 37] Sofern mittels der Aufzeichnung der Fahrroute – wie häufig – ein Rückschluss auf einen Fahrer möglich ist, ist dieses Profiling nur mit ausdrücklicher Einwilligung nach Art. 22 Abs. 2 lit. c) zulässig.

[Rz 38] Sofern die Einwilligung im Rahmen des Autokaufs, des Miet- oder Leasingverhältnisses abgegeben werden soll, ist nach Erwägungsgrund 32 der DSGVO eine eindeutige bestätigende Handlung erforderlich. Neben der Schriftform ist auch die elektronische oder mündliche Form möglich. Zu Beweiszwecken sollte die Einwilligung jedoch schriftlich erfolgen, da dem Hersteller nach Art. 5 Abs. 2 DSGVO die Rechenschaftspflicht obliegt. Zudem sollten die Informationen zur Datenerhebung und –verarbeitung auf einem gesonderten Blatt gegeben werden und nicht in AGB versteckt sein, um die Einwilligung nach Art. 7 Abs. 2 DSGVO hervorzuheben.

[Rz 39] Soweit eine Einwilligung erst am Bordcomputer erteilt werden soll, muss an dieser Stelle die Information erfolgen. Über die Datenverarbeitung i.R.d. Zusatzdienste sollte jedoch in jedem Falle bei der Vertragsverhandlung zumindest im Überblick aufgeklärt werden, damit der Fahrer sensibilisiert ist. Die Einwilligung ist vom Hersteller systemseitig zu protokollieren und der Fahrer muss sie jederzeit abrufen können (Rechenschaftspflicht, vgl. oben).

[Rz 40] Ferner muss der Fahrer gem. Art. 7 Abs. 3 DSGVO darüber informiert werden, dass er die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

[Rz 41] Dem Problem, dass ein anderer Fahrer als zuvor am Steuer Platz nimmt (z.B. bei Carsharing-Anbietern) kann dadurch begegnet werden, dass der Fahrer zu Beginn der Fahrt jeweils die Einwilligungen abgeben muss. Bei Privatautos könnten die Einstellung gespeichert werden, sofern immer der gleiche Fahrer das Auto benutzt. Denkbar ist auch, dass die jeweiligen Fahrereinstellungen mittels PIN oder Fingerabdruckscanner (hinreichende Erklärung wegen biometrischer Daten) geladen werden könnten.

IV. Wer ist zugriffsberechtigt?

[Rz 42] Aufgrund des informationellen Selbstbestimmungsrechts bestimmt allein der Fahrer, wer welche Daten von ihm erhalten darf. So zumindest der Idealzustand. Aus diesem Grund ist der Fahrer hinreichend über etwaige Empfänger zu informieren, damit er entscheiden kann, ob er eine Einwilligung zur Datenerhebung und -verarbeitung abgibt.

[Rz 43] Zu den Datenempfängern bzw. Kommunikationspartnern gehören nach BITKOM z.B.:

- der Fahrer selbst und ggf. Mitfahrer (z.B. Navigation, Car Entertainment, WLAN);
- Fahrassistenzsysteme (z.B. automatisches Einparken, autonomes Fahren);
- andere Fahrer/Fahrzeuge (z.B. Abstandkontrolle, Kollisionswarnung);
- Werkstatt/Hersteller (z.B. Diagnose, Frühwarnung);

- Taxis, Autovermietung, Car-Sharing-Anbieter (z.B. Abrechnung);
- Versicherungen (z.B. Pay as you drive Police);
- Infrastruktur-Betreiber/Verkehrszentrale/Polizei (z.B. Verkehrsmeldungen, Maut, eCall).[14]

[Rz 44] Zudem kommen auch andere Unternehmen in Betracht, die ein Interesse an den Daten der Fahrer haben könnten, um Persönlichkeitsprofile erstellen und personalisierte Werbung anbieten zu können.

V. Technischer Schutz

[Rz 45] Angesichts der großen Datenmenge müssen Hersteller dafür sorgen, dass die Server oder Clouds, auf denen die Daten gespeichert werden, vor Angriffen Dritter oder sonstiger unberechtigter Datenweitergabe geschützt sind. Vor dem Hintergrund der Datensicherheit sind daher entsprechende Sicherheitsmaßnahmen zu treffen.[15] Neben der Verschlüsselung personenbezogener Daten nach Art. 32 Abs. 1 lit. a) DSGVO bieten sich regelmäßige Penetrationstests i.S.d. Art. 32 Abs. 1 lit. d) DSGVO an. Art. 32 Abs. 1 lit. b) DSGVO müssen die technischen und organisatorischen Maßnahmen die Fähigkeit besitzen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Die Systemhersteller müssen nach Art. 32 Abs. 1 lit. c) DSGVO Backups durchführen und die Wirksamkeit der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 lit. d) DSGVO regelmäßig überprüfen. Die zu treffenden Sicherheitsmaßnahmen hängen jeweils vom Stand der Technik ab. Wichtiger als der Einsatz der neusten Methoden ist dabei jedoch, dass es sich um aktuelle und erprobte Maßnahmen handelt. Ein Indiz für die Einhaltung der technischen und organisatorischen Maßnahmen ist sowohl die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO als auch eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DSGVO. Welche konkreten Anforderungen an die Verhaltensregeln zu stellen sind, wird sich noch zeigen müssen.

VI. Privacy by Design/Default

[Rz 46] Die Automobilhersteller sind nach Art. 25 DSGVO dazu angehalten, bei der Entwicklung der Systeme, die autonomes Fahren ermöglichen, die datenschutzrechtlichen Vorgaben von Privacy-by-Design und Privacy-by-Default einzuhalten.[16] Das bedeutet, dass die Systeme derart benutzerfreundlich gestaltet sein müssen, dass von vornherein ein datenschutzkonformer Einsatz gewährleistet ist. Daten dürfen erst dann verarbeitet werden, wenn der Anwender seine Einwilligung erteilt hat. Mittels deutlicher Hervorhebung der datenschutzrelevanten Aspekte, Opt-In-Verfahren und Datensparsamkeit (vgl. auch Art. 5 Abs. 1 lit. c)) können diese Vorgaben eingehalten werden. Es sollten so viele Daten wie möglich anonymisiert werden. Diese Maßnah-

14 Astrid Auer-Reinsdorff/Isabell Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl., Beck Verlag, München 2015, § 34 Rn. 582.

15 So auch die Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg (Fn. 12).

16 So auch die Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg (Fn. 12).

men bedeuten auch für die Hersteller Rechtssicherheit, da das Datenschutzrecht dann nicht einschlägig ist. Voraussetzung ist jedoch, dass die Einschätzung des Vorliegens von anonymen Daten tatsächlich zutreffend ist. Mitunter kommt es aufgrund des für Nichtjuristen schwer zu fassenden Begriffs von personenbezogenen Daten nämlich zu Fehleinschätzungen. Die Einordnung als personenbezogenes oder anonymes Datum ist daher gelegentlich ein schmaler Grat.

[Rz 47] Dieses Jahr ist in Deutschland auch die Änderung des Wiener Übereinkommens über den Straßenverkehr vom 8. November 1968 in Kraft getreten. Danach sind Fahrerassistenzsysteme und automatisierte Fahrfunktionen erlaubt, sofern sie den einschlägigen technischen Regelungen der Vereinten Nationen entsprechen. Anderenfalls müssen sie so gestaltet sein, dass der Fahrer sie jederzeit übersteuern oder abschalten kann.

[Rz 48] Ferner hat der deutsche Bundesverkehrsminister Dobrindt eine Ethik-Kommission eingesetzt, die Leitlinien für die Programmierung automatisierter Fahrsysteme entwickeln soll.[17] Diese ist am 30. September 2016 zu ihrer ersten Sitzung zusammengekommen.

[Rz 49] Damit soll gewährleistet werden, dass der Mensch die Oberhand über die Systeme behält. Die Risiken, die die Technologie 4.0 damit mit sich bringt, sollen dadurch weiterhin beherrschbar bleiben.

VII. Fazit

[Rz 50] Sofern personenbezogenen Daten beim Betrieb von selbstfahrenden Autos nicht anonym erhoben oder verarbeitet werden, kann der Einsatz nur über eine spezielle noch zu schaffende Rechtsgrundlage oder eine Einwilligung des Betroffenen datenschutzrechtlich zulässig gestaltet werden. Dabei müssen die Hersteller ihren Informationspflichten transparent nachkommen und die Systeme getrennt voneinander anbieten. Die datenschutzkonforme Ausgestaltung wird den technischen Ausbau in den nächsten Jahren begleiten.[18]

[Rz 51] Festzuhalten bleibt, dass selbstfahrende Autos geeignet sind, dazu beizutragen, dass durch reibungslosen Verkehrsfluss Staus vermieden, Treibstoff gespart und so die Umwelt geschont wird. Datenschutzrechtlich birgt die Einführung selbstfahrender Autos jedoch ein hohes Risiko. Erst wenn sich Fahrer in vollem Umfang auf die technischen Systeme und einen hinreichenden Datenschutz verlassen können, steht dem Einsatz autonomer Fahrzeuge nichts mehr im Wege, sodass die Zeit am Steuer in Stausituationen, bei längeren Fahrten, beim Passieren enger Gassen oder in allen sonstigen Konstellationen sinnvoll anderweitig genutzt werden kann.

[Rz 52] Mit Spannung abzuwarten bleibt, welche Regelungen das deutsche Straßenverkehrsgesetz in puncto Datenschutz vorsehen wird. In diesem Zusammenhang wird es äußerst interessant sein, ob und wie die Automobilhersteller die datenschutzrechtlichen Vorgaben umsetzen werden. Die DSGVO wird dabei ein gesetzliches Druckmittel sein, da bei Verstößen zukünftig drastische

---

17 Bundesministerium für Verkehr und digitale Infrastruktur, Pressemitteilung: Auftaktsitzung der Ethik-Kommission zum automatisierten Fahren, 30. September 2016, http://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2016/157-dobrindt-ethikkommission.html?linkToOverview=DE/Presse/Pressemitteilungen/pressemitteilungen_node.html%23id233284.

18 Vgl. auch Stefan Randak, Diese Hürden müssen selbstfahrende Autos noch nehmen, manager magazin, 25. Juli 2016, http://www.manager-magazin.de/politik/meinungen/autonomes-fahren-huerden-der-neuen-technik-a-1104515.html.

Sanktionen drohen, sodass das Augenmerk beim autonomen Fahren zwangsläufig auch auf das Datenschutzrecht gerichtet werden muss.

Magnus Grünheidt, Datenschutzberater/Justiziar bei der datenschutz süd GmbH.