baum ▪ reiter & collegen
RECHTSANWÄLTE

baum ▪ reiter & collegen Benrather Schlossallee 101 · D-40597 Düsseldorf

Düsseldorf, den 01.12.2016
MET

Rechtsgutachten zum Thema „Kontrolle der Daten bei vernetzten und automatisierten Pkw“

Zusammenfassung der Ergebnisse

Im Rechtsgutachten wurde untersucht, wie der Anspruch von Verbrauchern auf Datensouveränität und Kontrolle der eingesetzten Software und Programmierungen im Auto durch Rechtsanpassungen und Gesetzesinitiativen durchgesetzt werden kann. Datenschutz-, Datensicherheits- und Haftungsfragen werden in dem Gutachten behandelt.

Die Ergebnisse des Gutachtens sind nachfolgend zusammengefasst.

Gerhart R. Baum
Bundesminister a. D.*
Rechtsanwalt

Prof. Dr. iur. Julius Reiter
Professor für Wirtschaftsrecht**
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Informationstechnologierecht

Dr. iur. Olaf Methner
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Arbeitsrecht
Fachanwalt für Informationstechnologierecht
Lehrbeauftragter FH**

Andrea Burghard, LL.M.
Fachanwältin für Bank- und Kapitalmarktrecht
Fachanwältin für Arbeitsrecht
Zertifizierte Datenschutzbeauftragte

Sylvia Klotzky
Rechtsanwältin

Bénédict Schenkel
Maîtrise en droit, Mag. iur.
Rechtsanwalt
Zertifizierter Datenschutzbeauftragter

Vitalija Mickeviciute
Rechtsanwältin

Sonja Steigerwald
Rechtsanwältin

Christian Leuchter
Rechtsanwalt

Sarah Behrendt
Rechtsanwältin
Zertifizierte Datenschutzbeauftragte

Paiman Manguri
Rechtsanwältin

Marc H. Sundermann
Rechtsanwalt

Benrather Schlossallee 101
40597 Düsseldorf
Fon: +49-(0) 211-836 805.70
Fax: +49-(0) 211-836 805.78
www.baum-reiter.de
kanzlei@baum-reiter.de

* Ubierring 50 · D-50678 Köln
** FOM Hochschule für Oekonomie & Management

Die Ergebnisse des Rechtsgutachtens im Überblick:

1. **Wem gehören die Fahrzeugdaten? Wer sind Betroffene/Verfügungsberechtigte?**

Alle Daten, die mit der Fahrzeugidentifikationsnummer (FIN) oder dem Kfz-Kennzeichen verknüpfbar sind, sind bei der Nutzung von Fahrzeugen als personenbezogen und damit datenschutzrechtlich relevant anzusehen.

Mit der zunehmenden Vernetzung des Fahrzeugs wird auch der Kreis der datenschutzrechtlich Betroffenen erweitert. Hierbei handelt es sich sowohl um den Fahrzeughalter als auch um den jeweiligen Fahrer. Dass im Fahrzeug keine personenbezogenen oder –beziehbaren Daten von Fahrern, Fahrzeughalter und Passanten erhoben, gespeichert oder verarbeitet werden, muss technisch sichergestellt werden.

Außer dem Betroffenen darf eine Verfügungsberechtigung über die personenbezogenen Fahrzeugdaten grundsätzlich nur in Ausnahmefällen eingeräumt werden:

- Dritten aufgrund einer informierten, freiwilligen und widerrufbaren Einwilligung des Betroffenen;
- Herstellern, Werkstätten, Verkehrsinfrastrukturbetreibern in Bezug auf Daten, die für die Sicherheit und die Funktionalität des Verkehrs notwendig sind, wenn diese Daten sicher anonymisiert werden;
- Behörden und ggf. Unfallbeteiligten nur unter Beachtung des „nemo-tenetur-Grundsatzes“

2. **Rechtsanpassungen zur Einhaltung von Mindeststandards von Datenschutz und Datensicherheit in Fahrzeugen**

a) **Nationale Gestaltungsspielräume**

Für die Gewährleistung eines effektiven Daten- und Verbraucherschutzes muss die Einhaltung der festgelegten Mindeststandards von Datenschutz und Datensicherheit bereits Voraussetzung für die Verkehrstauglichkeit und damit die Zulassung von Fahrzeugen sein. Datenschutz und Datensicherheit sind für den Straßenverkehr von zunehmender Relevanz, sodass eine Ermächtigungsgrundlage für das Verkehrsministerium geschaffen werden muss, um entsprechende Maßnahmen zu erlassen. Hierzu könnte in der Ermächtigungsnorm des § 6 Abs. 1 Nr. 2 StVG ergänzt werden, dass in der StVZO bei der Zulassung neben der Gewährleistung der Verkehrssicherheit auch auf die Gewährleistung der Datensicherheit und des Datenschut-

zes zu beachten sind. Das Gleiche gilt für die Verordnungsermächtigung über die regelmäßigen Hauptuntersuchungen der Fahrzeuge, die ebenso jedenfalls die Datensicherheit zum Gegenstand haben müssen.

Auch nach Inkrafttreten der DSGVO besteht neben der Zuständigkeit des Europäischen Gesetzgebers eine diesbezügliche Gesetzgebungskompetenz des nationalen Gesetzgebers, denn durch gesetzgeberische Maßnahmen im Zulassungsrecht wird lediglich die Einhaltung der DSGVO (u.a. die Einhaltung der Grundsätze des „Privacy by Design“ und „Privacy by Default“) zur Voraussetzung für die Zulassung eines Fahrzeugs für den Straßenverkehr gemacht. Damit werden erst die europarechtlichen Vorschriften der DSGVO im Kfz-Zulassungsrecht umgesetzt. Das von der DSGVO voll harmonisierte Datenschutzrecht wird hierbei inhaltlich nicht berührt.

b) Regelung in einer EU-Verordnung über die Betriebserlaubnisse von Kfz

Derzeit befindet sich ein neues Regelwerk auf europäischer Ebene für die Typgenehmigung von Kraftfahrzeugen in Bearbeitung. Hierin ist der Themenkomplex „Datensicherheit und Datenschutz“ zusätzlich zu den Umwelt- und Sicherheitszielen bzw. –anforderungen aufzunehmen. Dabei sind folgende Aspekte zu regeln:

- Zum *Schutz der Verkehrsteilnehmer vor Missbrauch ihrer Daten* sollten die Fahrzeughersteller den Grundsatz der Datenschutzgrundverordnung „eingebauter Datenschutz“ („privacy by design“) umsetzen und bei der Entwicklung entsprechende technische Vorrichtungen zur Sicherheit des Datenschutzes in die bordeigenen Systeme einbauen.
- Zur *Vermeidung von Fälschung, Manipulation und unbefugter Verwendung der Daten*, die von im und am Fahrzeug verbauten Systemen erfasst werden, müssen diese Systeme nachprüfbar geschützt sein. Sollte es doch zu einer sicherheitsrelevanten Fahrzeugdaten-Panne kommen, muss sichergestellt sein, dass das Fahrzeug eigenständig mit einem Notsystem an den Fahrbahnrand fährt und anhält.
- Zur *Vermeidung des Abfangens von Daten und der unbefugten Übernahme der Kontrolle über das Fahrzeug* muss jedes Fahrzeug, das Zugangspunkte zu elektronischen Systemen bietet, mit Fahrfunktionen ausgestattet sein, die derartige Angriffe sofort entdecken, melden und stoppen können. Diese Funktionen müssen regelmäßig gemäß geltender IT-Security-Standards auf Sicherheitslücken überprüft werden.

Um verlässliche Aussagen für Verbraucher treffen zu können, muss zudem gewährleistet sein, dass Zertifizierungsdienste geeignete inhaltliche und organisatorische Vorkehrungen für

Datenschutzzertifizierungen entsprechend der DSGVO im Fahrzeug treffen, um eine sachgerechte und unabhängige Bewertung vorzunehmen.

c) Transparenz

Jedes Fahrzeug ist hinsichtlich des Inhalts und Umfangs der vorhandenen Datensicherheits- und Datenschutzsysteme durch eine standardisierte Grafik zu kennzeichnen, um den Nutzer auf eine leicht verständliche Weise hierüber zu informieren. Die EU-Kommission sollte in diesem Zusammenhang von der ihr eingeräumten Befugnis nach Art. 12 Nr. 8 DSGVO Gebrauch machen und delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole im Bereich des Fahrzeugdatenschutzes und der Fahrzeugdatensicherheit darzustellen sind, und der Verfahren für die Bereitstellung der standardisierten Bildsymbole erlassen.

d) Verknüpfung von Typengenehmigung und PTI : Regelmäßige technische Überwachung

Die Vorschriften zur regelmäßigen technischen Fahrzeugüberwachung (PTI = Periodical Technical Inspection) basieren auf der Richtlinie 2014/45/EU. In eine Neufassung dieser Richtlinie ist aufzunehmen, dass die Fahrzeuge so konstruiert werden, dass moderne elektronische Fahrzeugsysteme im Rahmen der regelmäßigen technischen Überwachung auch über die elektronische Fahrzeugschnittstelle untersucht werden können.

Die Typengenehmigungsbehörde und der technische Dienst müssen Zugang zur Software und den Algorithmen des Fahrzeugs haben. Entsprechende Vorschriften sollten dahingehend ergänzt werden, dass die genannten Stellen ebenso Zugang zu den Quellcodes des Fahrzeugs erhalten.

Zudem ist die Erfüllung der Anforderungen für die Prüfung der sicherheits- und umweltrelevanten Systeme, Bauteile und Funktionen über die Fahrzeugschnittstelle bereits bei der Fahrzeuggenehmigung nachzuweisen, um die Effizienz der Fahrzeuguntersuchungen und so die (Daten-)Sicherheit und den Datenschutz der zukünftig im Verkehr befindlichen Fahrzeuge sicherzustellen. Zudem sollten die geprüften und zertifizierten Sachbereiche für die Kunden so umschrieben werden, dass sie die Reichweite der Prüfaussage ohne Fachkenntnisse dem Zertifikat entnehmen können.

3. Best Practice für EU-Mitgliedsstaaten: Aufbau und der Betrieb einer Connected-Car-Infrastruktur

Mit intelligenten Verkehrssystemen können eine Vielzahl personenbezogener Daten erhoben und verarbeitet werden, sodass bei unzureichender Klärung der rechtlichen Rahmenbedingungen die Gefahr besteht, dass der Datenschutz ins Hintertreffen gerät. Andererseits ist die bislang mangelhafte Zusammenführung und Bereitstellung relevanter Verkehrsdaten ein zentrales Hemmnis für die vollumfängliche Nutzung der digitalen Möglichkeiten. Es bedarf daher des Aufbaus eines Kompetenzzentrums, das als neutrale Instanz mit den zuständigen Akteuren für die Bereitstellung, Pflege und Aktualität der Verkehrsdaten sorgt.

Der österreichische Autobahnbetreibergesellschaft ASFINAG beispielsweise sammelt bereits heute sämtliche Verkehrsdaten und stellt sie über seine zentrale Datendrehscheibe bereit. Darüber hinaus beteiligt sie sich an verschiedenen Projekten zur Planung und Erforschung von Verkehrsmanagementsystemen und hat hierzu u.a. bereits auf dem Testfeld Telematik eine Vielzahl von Sensoren eingerichtet, um eine effiziente Erfassung von Verkehrsdaten zu ermöglichen.

In Deutschland könnte ebenfalls eine Finanzierungsgesellschaft gegründet werden, die sich an dem Beispiel der ASFINAG orientiert und der im Interesse des Bundes konkrete Aufgaben zur effektiven Planung und Einrichtung intelligenter Verkehrssysteme übertragen werden.

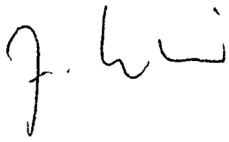
Entsprechend dem österreichischen Modell sollte darüber hinaus frühzeitig eine Stelle zur außergerichtlichen Streitbeilegung eingerichtet werden.

4. Vertrauen schaffen – Kernaufgabe eines unabhängigen „Trust Centers“

Zur Schaffung einer transparenten und gleichzeitig geschützten Verwaltung der Fahrzeugdaten sollte ein unabhängiges „Trust Center“ eingerichtet werden, das Fahrzeug- und Verkehrsdaten für das reibungslose Funktionieren der intelligenten Verkehrsinfrastruktur verwaltet, verarbeitet und bereitstellt und dabei die Datensicherheits- und Datenschutzstandards einhält. Als vertrauenswürdiger und neutraler Datentreuhänder für Fahrzeug- und Verkehrsdaten kann ein Trust Center daneben eine Vermittlerposition zwischen den Dateninhabern/-betroffenen und berechtigten Dritten einnehmen, um berechtigte Datenanforderungen zu prüfen und ggf. zu erfüllen.

Rechtsanwälte Baum · Reiter & Collegen
durch:

Gerhart R. Baum
Rechtsanwalt
Bundesminister a.D.



Prof. Dr. Julius Reiter
Rechtsanwalt
FA für IT-Recht

Dr. Olaf Methner
Rechtsanwalt
FA für IT-Recht