

## Presse – Information

### Arbeitskreis I: Fahrzeugdaten

- Datensammlung durch moderne Kraftfahrzeuge und Ihre Verwendung
- Daten- und Verbraucherschutz bei Verwertung von Fahrzeugdaten
- Grenzübergreifende Nutzung von Fahrzeugdaten aus polizeilicher Sicht

- Leitung** **Dr. Hans-Joseph Scholten**, Rechtsanwalt, Vors. Richter OLG Düsseldorf a. D., Gladbeck
- Referent** **Dr. Tibor S. Pataki**, M. Jur. (Oxford), Rechtsanwalt (Syndikusrechtsanwalt), Leiter Kraftfahrtversicherung, Kfz-Technik, Statistik und Kriminalitätsbekämpfung, Gesamtverband der Deutschen Versicherungswirtschaft e.V., Berlin
- Referent** **Dr. Ralf Scheibach**, LL.M., Leiter Abteilung Recht und Compliance, Verband der Automobilindustrie e.V., Berlin
- Referentin** **Marion Jungbluth**, Leiterin Team Mobilität und Reisen, Geschäftsbereich Verbraucherpolitik, Verbraucherzentrale Bundesverband e.V., Berlin
- Referent** **Volker Orben**, Polizeioberrat, Innenministerium des Landes Rheinland-Pfalz, Präsident des Netzwerks der europäischen Verkehrspolizeien (ROADPOL), Münster/Mainz

#### **In Kürze:**

**Moderne Fahrzeuge sammeln schon heute eine Vielzahl von Daten, die zum Betrieb vernetzter Fahrzeuge notwendig oder sinnvoll sind. Der technische Fortschritt, insbesondere bei der Entwicklung automatisierter oder autonomer Fahrsysteme, wird dafür sorgen, dass die Menge der gesammelten Daten weiter zunimmt. Bereits jetzt ist in einigen Fahrzeugen eine Umfeldüberwachung durch Videoaufzeichnungen verbaut. Mit dem Data Act will die EU eine grenzüberschreitende einheitliche Regelung schaffen, die Verfügbarkeit von Daten erleichtern und Vorschriften über den Zugang zu Daten schaffen, welche durch die Nutzung von vernetzten Produkten – etwa vernetzten Fahrzeugen – erzeugt werden. Fraglich ist, ob der Entwurf des Data Act den Besonderheiten des Verkehrs gerecht wird und für Rechtssicherheit zu sorgen vermag. Der Arbeitskreis beschäftigt sich mit der Frage, wie bestimmte Daten moderner Fahrzeuge sicher generiert und auch von Dritten verwertet werden können und dennoch den berechtigten Interessen möglichst aller Beteiligten gerecht werden kann.**

#### Im Einzelnen:

Die Verwendung und berechtigte Weitergabe von Daten soll mit dem Data Act vereinheitlicht und vereinfacht werden. Er beinhaltet beispielsweise eine Verpflichtung des Herstellers zur Datenweitergabe an Dritte, sofern dieses die Inhaber:innen des Fahrzeuges fordern. So werden etwa bei der Umfeldüberwachung Ton- und Bildaufnahmen gefertigt, ohne dass die Aufgenommenen dies bemerken oder Ihr Einverständnis erklärt haben. Mit den vom Fahrzeug insgesamt gewonnen Daten können z.B. Unfälle rekonstruiert, Gesetzesverstöße aufgezeigt und Fahrzeuge und damit auch deren Nutzer:innen überwacht werden. Wie wird mit den so gewonnen Daten umgegangen? Welche Daten werden von Fahrzeugen noch erfasst? Wo und wie werden sie gespeichert? Wer hat Zugriff auf diese Daten? Wie werden die berechtigten Interessen v.a. von Verbraucher:innen, Versicherungswirtschaft, Automobilindustrie, Behörden und Mobilitätsanbietern geschützt? Mit diesen Fragen befasst sich der Arbeitskreis.

## Presse – Information

### Arbeitskreis I

I / 1

### Kurzfassung des Referats

Fahrzeugdaten

#### Dr. Tibor S. Pataki

M. Jur. (Oxford) | Leiter Kraftfahrtversicherung, Kfz-Technik, Statistik und Kriminalitätsbekämpfung  
| Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV)

---

Die Mobilität mittels des vernetzten Kfz benötigt und produziert große Datenmengen. Damit der Wettbewerb in diesem neu entstehenden Markt belebt wird, muss die Hoheit der Daten bei den Verbrauchern liegen.

#### 1. Grenzen des ADAXO-Konzepts des VDA

Die aktuelle Entwicklung läuft diesem Ziel entgegen: Die Autohersteller etablieren derzeit ein System, nach dem Verbraucher die Daten vernetzter Fahrzeuge nur eingeschränkt und über die Server des Herstellers einem dritten Dienstleister weiterleiten können. So bleibt die Kontrolle über die Datenflüsse bei den Herstellern – vernetzt ist so nicht der Verkehr oder das Fahren; vernetzt sind nur die Fahrzeuge mit den jeweiligen Herstellern. Sie allein haben einen direkten Draht zu den Verbrauchern und direkten Zugriff auf die Daten. Alle anderen Marktteilnehmer – Versicherer, Kfz-Werkstätten, Automobilclubs und andere – werden am direkten Kontakt zu den Autobesitzern gehindert; und zwar ohne, dass diese dabei ein Mitspracherecht hätten.

#### 2. Verbraucher sollen einfach über ihre Daten verfügen können

Die ideale Lösung für den Datenzugang ist eine „Sichere Onboard Telematik-Plattform“, die es Verbrauchern ermöglicht, die Apps verschiedener Anbieter direkt im Fahrzeugsystem zu integrieren. Hersteller wie andere wären – was den Datenzugriff angeht – gleichgestellt. Diese Apps könnten dann automatisiert auf die vom Verbraucher freigegebenen Daten zugreifen, sie verarbeiten und direkt an den Anbieter senden. Ohne „doppelte“ Speicherung beim Kfz-Hersteller – die Datensparsamkeit wäre gewährleistet. Die Apps würden vom Kfz-Hersteller geprüft und freigegeben – wie es bei Smartphones und dem Zugriff auf die App-Stores heute auch üblich ist („Apple-Prinzip“).

#### 3. Der Entwurf des Data Acts stellt keine Lösung dar – sektorspezifische Regelung erforderlich

Der momentan auf europäischer Ebene diskutierte Data Act bietet keine ausreichende Lösung, da damit keine Regelungen zu den Funktionen und Ressourcen des Fahrzeuges verbunden sind. Es muss eine sektorspezifische Lösung kommen, die die Kfz-Hersteller rechtlich bindet, das bestehende Datenmonopol aufzugeben.

## Presse – Information

### Arbeitskreis I

1 / 2

#### Kurzfassung des Referats

Digitalisierung der Mobilität

#### Dr. Ralf Scheibach, LL.M.

Leiter Recht und Compliance / Verband der Automobilindustrie e.V.

---

Die Automobilindustrie bietet schon heute umfassende Datenangebote für kundenbezogene Anwendungen und vielfältige technische Zugriffsmöglichkeiten auf Daten. Folgende Rahmenbedingungen müssen gegeben sein:

#### 1. Zugang zu Daten im Fahrzeug (VDA-Konzept ADAXO) nach FRAND-Bedingungen

Fahrzeugdaten sind eine Quelle für Innovationen und ein Grundpfeiler für moderne Mobilität. Der VDA hat mit dem zum Teil bereits im Markt eingeführten ADAXO-Konzept ein zeitgemäßes und zukunftssicheres Verfahren für den Austausch von fahrzeug-generierten Daten vorgelegt. ADAXO ist die Abkürzung für „Automotive Data Access, extended and open“ und bedeutet „erweiterter und offener Fahrzeugdaten-zugriff“ auf Basis der vom EuGH eingeführten FRAND- (fair, reasonable and non-discriminatory) Grundsätze.

#### 2. Datenzugang nach EU-Recht (Data Act) auf im Fahrzeug verfügbare Daten bezogen

Mit dem Data Act sind pauschale Regelungen für die Weiterleitung von Daten getroffen worden. Fahrzeugdaten können Dritten nur in dem Maße zur Verfügung stehen, wie die Hersteller sie auch zur Erbringung ihrer eigenen Services nutzen.

#### 3. Datenzugang über sicheren neutralen Server – Verkehrssicherheit hat Vorrang

Der Hersteller leitet die Daten über ein OEM-Backend (sicherer Zugang ins Fahrzeug - Extended Vehicle – ExVe) weiter. Das (Ende-zu-Ende-) Berechtigungsmanagement muss zentral, konsistent und einfach zu bedienen sein und somit beim Hersteller als zentralem Ansprechpartner der Datenerhebung liegen. Die Freigabe der Daten und das Management von Fahrzeugressourcen (z.B. Bandbreiten für Datenübertragungen im Fahrzeug) können nur durch das für die Zertifizierung des Fahrzeugs verantwortliche Unternehmen erfolgen.

#### 4. Weiterleitung von Daten nur nach Maßgabe der EU-DSGVO

Die Datensouveränität liegt beim Kunden. Die Verfügbarkeit von Daten für Dritte muss daher datenschutzrechtlich konform nach Maßgabe seiner Einwilligung gestaltet werden. Hierzu hat der VDA bereits 2016 mit den Datenschutzbehörden des Bundes und der Länder eine gemeinsame Erklärung herausgegeben.

## Presse – Information

### Arbeitskreis I

1 / 3

#### **Kurzfassung des Referats**

Mobilitätsdatenwächter – Überblick und Kontrolle über Mobilitätsdaten in die Hände der Verbraucher:innen legen

#### **Marion Jungbluth**

Leiterin Team Mobilität und Reisen, Geschäftsbereich Verbraucherpolitik beim Verbraucherzentrale Bundesverband (vzbv)

---

Seit dem 25. Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DSGVO). Diese Verordnung markiert nicht weniger als eine Zeitenwende im nationalen und europäischen Datenschutz.<sup>1</sup> Im Lichte dieser neuen Ordnung ist der nächste logische Schritt, die datenschutzrechtliche Emanzipierung der Betroffenen – also insbesondere der Verbraucher:innen – konsequent weiter zu verfolgen und auf den wichtigen Mobilitätssektor auszuweiten. Die Verkehrswende muss zwingend von einer Mobilitätsdatenwende vorbereitet und begleitet werden.

Fahrzeuge sowie deren Mobilität erzeugen eine Vielzahl von Daten. Diese werden derzeit faktisch von den Autoherstellern kontrolliert und genutzt. Diese Gatekeeper-Position der Autohersteller muss enden. Fahrzeugführende dürfen nicht auf eine Datenquellfunktion reduziert bleiben. Denn das würde konterkarieren, wofür sich der Datenschutz seit Jahrzehnten stark macht.

Um die Neuordnung des Mobilitätsdatensektors zu erreichen und diesen mit der europäischen Datenordnung zu harmonisieren, bedarf es eines neuen Datenmanagementsystems. Der vzbv sieht dabei die Zukunft in einem Mobilitätsdatenwächtermodell. Das Datenwächtermodell wird im Wesentlichen von einem Dreiklang gebildet: von einem Datentreuhänder (Zugang zum Fahrzeug, Datenweiterleitung), einem Datenwächter (Autorisierung) und den Betroffenen. Ein PIMS (Personal Information Management System) ermöglicht dabei den Fahrzeugnutzer:innen einen anwenderfreundlichen Überblick über die Mobilitätsdatenströme, die darüber auch gesteuert werden können. Die Datenkontrolle wird somit erstmals seit Beginn der Digitalisierung im Mobilitätssektor dort liegen, wo sie hingehört: bei den Verbraucher:innen und nicht mehr beim Fahrzeughersteller.

---

<sup>1</sup> Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: DSGVO – BDSG Texte und Erläuterungen, 2022, Seite 8, Bonn.

## Presse – Information

### Arbeitskreis I

1 / 4

#### **Kurzfassung des Referats**

Unfallrekonstruktion und Verfolgung von Verkehrsverstößen aus polizeilicher Sicht im Zusammenhang mit dem Data Act

#### **Volker Orben**

Polizeioberrat, Netzwerk der europäischen Verkehrspolizeien ROADPOL e.V.

---

In allen europäischen Ländern wird von der Polizei erwartet, dass sie bei einem Verkehrsunfall Beweise für das Straf- und Zivilverfahren sichert. Das ist in erster Linie im Interesse der am Verkehrsunfall Beteiligten. Hier gibt es in der Regel einen Verursacher und ein Opfer, dessen Rechte durch die polizeiliche Unfallaufnahme gewahrt werden. Zivilprozesse zum Ersatz von materiellen, körperlichen und psychischen Schäden nach einem Unfall ziehen sich zum Teil über Jahre hin. Je weniger konkret und beweissicher die Polizei die Ursachen eines Unfalls ermitteln kann, desto schwerer fällt es dem Opfer, später seine Ansprüche durchzusetzen. Beweissichere Ermittlungen sind somit gelebter Opferschutz.

In einem grenzenlosen Europa fahren jetzt schon vernetzte Fahrzeuge und künftig auch mehr und mehr automatisiert fahrende Kfz. Bei Verkehrsunfällen muss die Polizei in allen Ländern mit einfachen Maßnahmen in der Lage sein, auch digitale Spuren wie die Fahrzeugdaten zu sichern. Und dieser Bedarf besteht nicht erst in der Zukunft. Schon jetzt ist festzustellen, dass sich Unfälle ohne das Auslesen der Datenspeicher oft nicht mehr in Gänze aufklären lassen. Etwa Unfälle, bei denen die Fahrer behaupten, Fehlfunktionen von Fahrerassistenzsystemen seien Ursache für den Unfall.

Deshalb braucht die Polizei – gegebenenfalls mit Unterstützung von externen Experten – verlässlichen und geregelten Zugang zu den in den Fahrzeugen generierten digitalen Daten. Die Erhebung und Auswertung der Daten ist Voraussetzung für die hoheitliche Entscheidung, wer einen Verkehrsunfall verursacht hat, und damit Grundlage für die strafrechtlichen und zivilrechtlichen Folgen.

Es geht um Datenzugriff bei mitunter schwersten Verkehrsunfällen. Die Polizei hat einen konkreten Tatverdacht und die Polizei kennt bereits den Tatverdächtigen, also den Fahrer eines unfallbeteiligten Fahrzeugs. Es besteht eine sehr hohe und sehr konkrete Auffindevermutung bezüglich unfallrelevanter Daten. Auch der Zeitausschnitt ist sehr konkret – in der Regel reichen fünf Sekunden vor und 350 Millisekunden nach dem Crash für die Unfallrekonstruktion aus. Von Big Brother, der heimlich und ohne Verdacht willkürlich alle Bürgerinnen und Bürger überwacht, kann also keine Rede sein.