Positionspapier

des Gesamtverbandes der Deutschen Versicherungswirtschaft

„Datenkranz beim automatisierten Fahren gemäß § 63a StVG – externe Speicherung bei einem Datentreuhänder“

Gesamtverband der Deutschen
Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5320
Fax: +49 30 2020-6320

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Dr. Tibor S. Pataki
Kraftfahrtversicherung, Kfz-Technik,
Statistik und Kriminalitätsbekämpfung

E-Mail: t.pataki@gdv.de

www.gdv.de

Das automatisierte Fahren wird den Straßenverkehr der Zukunft grundlegend verändern. Praktisch alle Automobilhersteller und viele Zulieferer arbeiten derzeit an Lösungen, die Fahraufgaben zunehmend ohne das Eingreifen des Fahrers bewältigen können. Die deutschen Automobilhersteller und Zuliefererbetriebe haben in diesem zukunftsträchtigen Segment einen beachtlichen Vorsprung gegenüber anderen Anbietern. Damit auch zukünftig das Verkehrsopfer bei Verkehrsunfällen mit Fahrzeugen mit automatisierten Fahrsystemen umfassend geschützt ist, greift die Gefährdungshaftung nach § 7 StVG wie schon bisher unabhängig davon ein, ob der Fehler beim Fahrer oder im Fahrzeug – beispielsweise beim automatisierten Fahrsystems – liegt. Damit bietet dieses Haftungssystem die ideale rechtliche Grundlage für eine stufenweise Fahrzeugautomatisierung, ohne dass eine Haftungslücke zulasten des Verkehrsopfers entsteht. Diese Sichtweise hat der Gesetzgeber in seiner neuen Regelung zum automatisierten Fahren im Straßenverkehrsgesetz bestätigt. Auch der Verkehrsgerichtstag in Goslar hat 2018 die Auffassung vertreten, dass es beim automatisierten Fahrsystem keine Änderung des Haftungssystems bedarf. Die europäische Kommission bestätigt dieses in ihrem Vorschlag für eine neue KH-Richtlinie sowie im Dritten Mobilitätspaket.

Heute wird die ganz überwiegende Zahl der Unfälle durch menschliche Fehler verursacht. Mit einem steigenden Automatisierungsgrad der Fahrzeuge wird sich dieses Verhältnis verändern. Es muss deshalb in Zukunft aufklärbar sein, wer die Verantwortung für den Unfall trägt: Das automatisierte Fahrsystem oder der Fahrer. Der Gesetzgeber hat in § 63a StVG einen Datenkranz definiert, der vom automatisierten Fahrsystem gespeichert werden muss und Aufschluss über die Verantwortung Mensch/Maschine gibt.

Das Straßenverkehrsgesetz regelt die Zulässigkeit der Übermittlung von Daten, ohne dabei zu bestimmen, an welchem Speicherort dieses erfolgen soll – im Fahrzeug und/oder an externer Stelle.

Die deutsche Versicherungswirtschaft schlägt vor, dass diese Speicherung nicht nur im Kraftfahrzeug, sondern zugleich an einer externen Stelle erfolgt, die durch einen Datentreuhänder verwaltet wird, der die datenschutzrechtlichen sowie datensicherheitsrechtlichen Themen verantworten würde.

1. Speicherung des Datenkranzes gemäß § 63 a StVG

Am 21. Juni 2017 ist das Straßenverkehrsgesetz um Regelungen zum automatisierten Fahren ergänzt worden. Mit dieser Novellierung werden die Zulässigkeit und Voraussetzungen des automatisierten Fahrens, die Pflichten des Fahrzeugführers und der Schutz personenbezogener Daten geregelt. Das Gesetz sieht vor, dass Fahrzeuge, die mittels hoch- oder vollautomatisierter Fahrfunktion betrieben werden, die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben speichern müssen, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt. Außerdem erfolgt eine derartige Speicherung, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt.

Im Falle eines Unfalles haben u. a. auch Versicherungsgesellschaften ein Interesse daran, die im Fahrzeug gespeicherten oder von diesem an einen Dritten übermittelten Daten in einem Zivilverfahren – z. B. einem Regress gegen den Hersteller – zu verwenden.

Diese Fallkonstellation hat der Gesetzgeber erkannt und in § 63a Abs. 3 StVG geregelt. Danach ist der Fahrzeughalter verpflichtet, die Übermittlung von Positions- und Zeitangaben an Dritte zu veranlassen, wenn die Daten zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit einem Unfall im Sinne von § 7 Abs. 1 StVG erforderlich sind und das entsprechende Kraftfahrzeug mit automatisierter Fahrfunktion an diesem Ereignis beteiligt war.

Noch ungelöst ist die Frage, wie die Berechtigten technisch Zugriff erhalten können und insbesondere an welchem Ort die Speicherung der Daten erfolgen soll. Diese Frage lässt das Gesetz unbeantwortet und enthält in § 63 b StVG lediglich eine Ermächtigungsgrundlage für das Bundesministerium für Verkehr und digitale Infrastruktur zur technischen Ausgestaltung des Speichermediums, zur Bestimmung des Ortes des Speichermediums sowie zur Art und Weise der Datenspeicherung.

Als mögliche Lösungen sind die Einführung eines Datenaufzeichnungsgerätes („Black Box“) im Fahrzeug selbst und/oder eine Datenübertragung auf einen externen Server, der durch einen neutralen Datentreuhänder verwaltet wird, denkbar. Der Datenspeicher für die Beweissicherung muss gegen unberechtigten Zugriff geschützt, also nicht manipulierbar sein und sämtliche Zugriffe protokollieren. Die Aufzeichnung der Steuerungseingriffe sollte verschlüsselt, gesichert und insb. über alle Fabrikate standardisiert erfolgen.

2. Gesetzliche Grundlage im StVG für externe Speicherung vorhanden

§ 63 a StVG regelt in Absatz 1, dass das Kraftfahrzeug den gesetzlich vorgegebenen Datenkranz speichern muss. Damit ist der Ort der Speicherung jedoch nicht determiniert.

Der Wortlaut des Absatz 2 spricht jedoch unseres Erachtens dafür, dass der Datenkranz auf einem externen Server gespeichert werden soll. Es heißt dort: „Die gemäß Absatz 1 gespeicherten Daten dürfen den nach Landesrecht für die Ahndung von Verkehrsverstößen zuständigen Behörden auf deren Verlangen übermittelt werden." Es handelt sich hierbei um die Berechtigung der externen Stelle, die Daten an die staatlichen Stellen zu übermitteln. Würden die Daten im Kraftfahrzeug selbst in einer Blackbox gespeichert sein, hätte der Gesetzgeber zum einen die Verpflichtung des Halters aufnehmen müssen, diese Daten „herauszugeben". Der Regelungsbereich des Absatzes 2 hätte dementsprechend in den Absatz 3 integriert werden müssen. Darüber hinaus würde die Auslegung des Absatz 2 in Richtung auf eine „Blackbox" dem vom Gesetzgeber intendierten Zweck nicht entsprechen. Die Zurverfügungstellung der Daten aus einer Blackbox für behördliche Ermittlungen wäre nicht umsetzbar. Der Kraftfahrzeughalter wäre zum einen nach dem Wortlaut des Gesetzes nicht verpflichtet, an einer derartigen Datenherausgabe mitzuwirken, zum anderen müsste die Ordnungsbehörde den Datenkranz „händisch" auslesen. Hierfür benötigt die Ordnungsbehörde jedoch den Zugriff auf das Kraftfahrzeug, den der Kraftfahrzeughalter unproblematisch verzögern könnte, um bspw. die Verjährung eines Bußgeldanspruches zu erlangen. Der Gesetzgeber ist u. E. davon ausgegangen, dass der Datenkranz bei einem externen Dritten gespeichert ist.

Der Wortlaut des Absatzes 3 spricht auch nicht dafür, dass die Daten ausschließlich im Kraftfahrzeug gespeichert sein müssten. Ganz im Gegenteil: Hier hat der Fahrzeughalter die Übermittlung der Daten unter bestimmten Voraussetzungen zu „veranlassen", was bedeutet, dass der Fahrzeughalter gegenüber einem Dritten die Freigabe der Daten – zur Übermittlung – erklären, sprich: veranlassen muss.

Eindeutig geht Absatz 5 davon aus, dass die Daten an einer externen Stelle gespeichert werden müssen. Absatz 5 spricht davon, dass im Zusammenhang mit einem Unfall die Daten in anonymisierter Form zu Zwecken der Unfallforschung an Dritte übermittelt werden können. Die Anonymisierung derartiger Daten kann jedoch nicht durch den Kraftfahrzeughalter vorgenommen werden, sondern einzig durch eine externe Speicherstelle. Diese wird gemäß § 63a Abs. 5 dazu berechtigt, eine derartige Anonymisierung vorzunehmen und das anonymisierte Ergebnis zu Zwe-

cken der Unfallforschung an Dritte zu übermitteln. Nur dadurch ist sichergestellt, dass der Gedanke des Gesetzgebers, der Unfallforschung zum Zwecke einer präventiven Aufklärung von Entwicklungen beim automatisierten Fahrsystem den Datenkranz in anonymisierter Form zur Verfügung zu stellen, gewahrt ist.

3. Datenübertragungssicherheit (kein Zugriff Unberechtigter)

Von besonderer Wichtigkeit ist, dass der Datenkranz gemäß § 63 a StVG alle Anforderungen an einen hohen Standard der Datensicherheit erfüllt.

Daher muss sichergestellt werden, dass die Übertragungssicherheit der Daten jederzeit sichergestellt ist. Die Speicherung bei einem Datentreuhänder würde diese Voraussetzung erfüllen. Der Datentreuhänder wäre in der Lage, mit den erforderlichen technischen Sicherungsmaßnahmen eine sichere Datenübertragung zu ermöglichen.

Die Speicherung des Datenkranzes bei einem Datentreuhänder würde auch keine Gefahr eines großen „Datenpools“ ergeben, da nur eine selektive Speicherung der „Umschaltpunkte“ – beispielsweise Umschaltung von Fahrerfahren zu Systemfahren – erfolgt, woraus keine Streckenverfolgung bzw. Erfassung von Bewegungsprofilen möglich ist.

4. Beweismittelsicherheit

Die Datenerfassung muss auch im Falle eines Unfalles gewährleistet sein.

Eine Speicherung allein im Kraftfahrzeug wird die vom Gesetzgeber beabsichtigte Nachvollziehbarkeit der Letztverantwortung (Fahrer oder System) nicht umfassend sicherstellen können. Das Verlustrisiko der Daten, die einzig im Fahrzeug selbst gespeichert werden, ist ausgesprochen hoch. Das Fahrzeug kann zerstört sein oder der Halter kann das Fahrzeug veräußert haben. In beiden Fällen wäre nicht sichergestellt, dass die berechtigten Personen, wie beispielsweise Bußgeldstellen, Staatsanwaltschaften, das Verkehrsunfallopfer oder ein Versicherer, die gesetzlich bestehenden Datenzugangsrechte durchsetzen könnten. Bekanntermaßen werden Kraftfahrzeuge nach einem Verkehrsunfall häufig und schnell veräußert. Der Erwerber des Kraftfahrzeuges, der neue Halter, wäre nicht verpflichtet, einem berechtigten Dritten Zugang zu den im Fahrzeug selbst allein gespeicherten Daten zu gewähren. § 63 a StVG ist in dieser Hinsicht nicht eindeutig, da eine entsprechende Verpflichtung des Erwerbers zur Herausgabe bzw. Veranlassung der Datenübertragung nicht ausdrücklich geregelt wurde – gerade wenn man die Fälle sich vor Augen hält, in denen das Fahrzeug ins Ausland verbracht wurde. Darüber hinaus würde

die Speicherung der Daten in einer „Blackbox“ Manipulationsmöglichkeiten beim Auslesevorgang der Daten ermöglichen.

Eine externe Speicherung würde hingegen gewährleisten, dass infolge der schnellen Übertragung des Datensatzes die Gefahr einer Manipulation der Daten auf ein Minimum reduziert wird. Ferner besteht in einem solchen Fall auch nicht das Risiko, dass die entsprechenden Daten durch Zerstörung, Veräußerung oder „Verschwinden“ des Kraftfahrzeuges verlustig gehen.

5. Cyber-Sicherheit

Selbstverständlich muss sichergestellt werden, dass die Speicherung des Datenkranzes bei einem Datentreuhänder den höchsten Anforderungen der Datensicherheit entspricht.

Dieses kann schrittweise dadurch gewährleistet werden, dass die Erstübertragung der Daten aus dem Kraftfahrzeug über die Server-Plattform des Herstellers an eine zentrale Stelle erfolgt, so dass auch der Datentreuhänder keinen direkten Zugriff auf das Kraftfahrzeug hat. Dadurch ist gewährleistet, dass die Fahrzeughersteller die klare Verantwortlichkeit für die Funktionsfähigkeit der Technik haben. Dieses Konzept steht damit auch im Einklang mit den technischen Anforderungen der Kraftfahrzeughersteller.

Die Umsetzung einer derartigen Konzeption kann auch mit den Interessen der Beteiligten datenschutzrechtlich in Einklang gebracht werden. Denkbar sind Modelle der Auftragsdatenverarbeitung bzw. der gemeinsamen Verantwortlichkeit.

Die Speicherung des Datenkranzes gemäß § 63 a StVG bei einem externen Datentreuhänder würde auch zu keiner datenschutzrechtlich nachteiligen Situation des Kfz-Halters – eine Speicherung im Kraftfahrzeug unterstellt – führen. Selbstverständlich bedürfte es auch bei der Datentreuhänder-Lösung der Zustimmung des Kfz-Halters, wenn ein berechtigter Dritter gemäß § 63 a Abs. 3 StVG die Übermittlung der Daten fordert. Sollte der Kfz-Halter dieser Forderung nicht entsprechen, müsste die Zustimmung des Kfz-Halters – als Voraussetzung der Datenübertragung seitens des Datentreuhänders – im Zivilverfahren durch den berechtigten Dritten eingeklagt werden.

6. Praktikabilität des Ausleseprozesses

Eine Speicherung des Datenkranzes ausschließlich im Kraftfahrzeug selbst würde auch zu erheblichen Kosten für alle Beteiligten führen.

Schon aus Eigeninteresse fühlte sich der Kfz-Halter verpflichtet, seine „erfahrenen“ Daten bei einer Veräußerung seines Kraftfahrzeuges zu sichern. Nur dadurch könnte er sicherstellen, dass er sich über diesen Datenkranz im Bedarfsfall exkulpieren kann. Hat er nämlich sein Kraftfahrzeug veräußert, hat er in der Regel keinen Zugriff mehr auf dieses Kraftfahrzeug – und dementsprechend auf den dort gespeicherten Datenkranz.

Gleichzeitig wird sich der Kfz-Halter bei der Veräußerung des Kraftfahrzeuges eventuell veranlasst sehen, die bis dahin gespeicherten Daten zu löschen. Auch in einem solchen Fall würde er die Möglichkeit verlieren, sich mithilfe dieser Daten zu exkulpieren. Ferner stünde dagegen das entgegengesetzte Interesse berechtigter Dritter, wie beispielsweise der Behörden. Diese benötigen den Zugriff auf den entsprechenden Datenkranz im Ordnungswidrigkeiten- oder Strafverfahren.

In Zeiten, in denen die Digitalisierung in aller Munde ist, erscheint ein „analoges Auslesen“ mittels Lesegerät anachronistisch und unpraktikabel. Ungeachtet der Tatsache, dass das Kraftfahrzeug zerstört oder beispielsweise im Ausland sein könnte, würde der Medienbruch naturgemäß auch kostensteigernd wirken. Hinzu kommt die Kostenbelastung, die auf die bisherigen Kfz-Halter zukommt, wenn dieser eine Auslesung/Datenspeicherung vornehmen möchte.

7. Konzeption des Datentreuhänders

Der Datentreuhänder und dessen technische Infrastruktur würden zusammen mit der Politik und Verwaltung sowie mehreren interessierten Stakeholdern erfolgen, um eine ökonomische, datensichere sowie neutrale Plattform zu schaffen. Die konkrete Umsetzung, wie beispielsweise die Frage einer Beleihung, müsste im weiteren Umsetzungsprozess erörtert werden.

8. Abschlussbetrachtung

Eine „isolierte“ Blackbox im Fahrzeug ist für die Zwecke des § 63a StVG nicht geeignet. Diese eröffnet Manipulationsmöglichkeiten vor und nach dem Auslesen. Der Auslesevorgang am Fahrzeug selbst ist nicht nur aufwendig, sondern erfordert Abstimmungsaufwand mit mehreren Beteiligten und ist z. B. nach besonders schweren Unfällen, Bränden, einem Fahrzeugstandort im Ausland oder einer schnellen Veräußerung häufig un-

möglich. Insbesondere die Zurverfügungstellung der Daten für behördliche Ermittlungen ist über eine Blackbox nicht umsetzbar. Auch die Zwecke einer anonymisierten Statistik nach Absatz 5 lassen sich so nicht erreichen.
Der Gesetzgeber geht in § 63a Abs. 2 StVG selbst von einer externen Plattform aus, da in Absatz 2 keine Mitwirkungspflicht des Halters vorgesehen ist.

Die Erfüllung aller im Gesetz genannten Speicherzwecke kann aus Sicht der deutschen Kraftfahrtversicherer nur durch eine neutrale und zentrale Datenplattform in Gestalt eines Datentreuhänders gewährleistet werden. Dieser kann einen fairen Datenzugang für alle Berechtigten mit definierten digitalen Schnittstellen zur Verfügung stellen. Weitere Vorteile wären ein kostengünstiger Prozess, die sofortige Datenspeicherung auf einem zentralen Server, damit gleichzeitig Datensicherheit und Schutz vor Manipulation.

Folgende Übersicht verdeutlicht die Vorteile der Datentreuhänderlösung:

Kriterien	Blackbox	Datentreuhänderlösung	Begründung
Eignung für die gesetzl. Speicherzwecke (§ 63 StVG)	☒	✓	Die Erfüllung aller im Gesetz genannten Speicherzwecke kann nur durch eine neutrale und zentrale Datenplattform (nachfolgend Treuhänderlösung) gewährleistet werden. Insbesondere die Zurverfügungstellung der Daten für behördliche Ermittlungen (Absatz 2) sind über eine Blackbox nicht umsetzbar. Der Gesetzgeber geht in § 63a Abs. 2 StVG selbst von einer externen Plattform aus, da darin keine Mitwirkungspflicht des Halters vorgesehen ist („Daten dürfen übermittelt werden...“). Auch die Zwecke der anonymisierten Statistik nach Absatz 5 lassen sich nur über eine Treuhänderlösung erreichen.
Datenverfügbarkeit	☒	✓	Eine Blackbox gewährlistet nicht in allen Situationen die Verfügbarkeit (Beispiele: Veräußerung des Fahrzeuges, Zerstörung). Die Treuhänderlösung hingegen gewährleistet, dass die einmal übertragenen Daten stets verfügbar sind.
Manipulationssicherheit	☒	✓	Eine Blackbox eröffnet Manipulationsmöglichkeiten vor und nach dem Auslesen. Bei der Treuhänderlösung werden die Daten maschinell in die Sphäre des neutralen Treuhänders übertragen und sind vor Manipulationen Dritter geschützt.
Cyber-Sicherheit	✓	✓	Bei beiden Modellen lässt sich eine sichere Umgebung herstellen.
Praktikabilität + Kosten	☒	✓	Ein voraussichtlich häufiges Auslesen der Daten direkt aus dem Fahrzeug vor Ort ist für die Berechtigten nicht praktikabel und steht im Widerspruch zu den Digitalisierungsprojekten der Bundesregierung (z. B. i-Kfz). Zudem verursacht die Blackbox-Lösung erhebliche – über die Gesetzesbegründung hinausgehende – Kosten, da der Zeitaufwand für das manuelle Auslesen erheblich ist (Terminvereinbarung, Zeit vor Ort, Anfahrt).
Normierung des Datensatzes	✓	✓	Bei beiden Modellen möglich.

Berlin, den 27. August 2018