Datum
2. August 2019

Gemeinsame Position zur Ausgestaltung des Fahrmodusspeichers (DSSAD)

Moderne Kraftfahrzeuge werden zunehmend mit hoch- und vollautomatisierten Fahrfunktionen ausgestattet sein, die in der Lage sind, die Fahrzeugführung für einen gewissen Zeitraum bzw. komplett zu übernehmen.

Der Fahrzeugführer gewinnt hierdurch immer mehr Freiheit, indem er sich unter bestimmten Voraussetzungen dauerhaft vom Verkehrsgeschehen abwenden kann und die Fahraufgabe vollständig an das Fahrzeug delegiert. Zugleich wird die fortschreitende Automatisierung und Vernetzung der Fahrzeuge dazu führen, dass Fahrzeughersteller oder Infrastrukturbetreiber zunehmend in den Vordergrund rücken, wenn es um die Frage geht, wer für einen Unfall oder einen Verkehrsverstoß verantwortlich ist.

Der deutsche Gesetzgeber hat diese Problematik frühzeitig erkannt und im Rahmen der Novellierung des Straßenverkehrsgesetzes mit § 63a StVG erstmals eine Regelung zur Datenverarbeitung im Kraftfahrzeug inklusive einer Datenaufzeichnung im Sinne eines Fahrmodusspeichers eingeführt. Hierdurch soll dem Fahrzeugführer die Möglichkeit gegeben werden, sich gegenüber dem Fahrzeughersteller oder dem Infrastrukturbetreiber zu entlasten.

Darüber hinaus wird das „Weltforum für die Harmonisierung von fahrzeugtechnischen Vorschriften“ zunächst im Zusammenhang mit der Änderung der Erarbeitung der neuen ALKS UN ECE Regelung, die den Spurhalteassistenten Level 3 regeln soll, bis März 2020 in der informellen Arbeitsgruppe DSSAD / EDR die technischen Anforderungen des sogenannten „Data Storage System for Automated Driving“, kurz „DSSAD“ festlegen.

Im Hinblick auf den begrenzten zeitlichen Rahmen und die international sehr unterschiedlichen Anforderungen an den Datenschutz werden nicht alle Fragen des Speichermediums Inhalt der UN ECE Regulierung sein können. Insbesondere detaillierte Zugriffsregelungen und die genaue Ausgestaltung des Speicherortes werden durch den europäischen und nationalen Gesetzgeber zu regulieren sein.

Auf dieser Basis stellen die Unterzeichner an die Ausgestaltung des Fahrmodusspeichers folgende Anforderungen:

1. **Um eine datenschutzkonforme und manipulationssichere Speicherung zu gewährleisten, muss der im Fahrzeug gespeicherte Datensatz - auf ein neutrales (hoheitliches) Backend übertragen werden.**

Begründung: Die erforderlichen Daten müssen in der Hand eines neutralen und unabhängigen Dritten sein.

Die Speicherung allein in einem crashsicheren lokalen Fahrzeugspeicher bietet keinen ausreichenden Schutz vor unberechtigten Zugriffen etwa bei einem Verkauf des Fahrzeugs. Mithin kann eine Verfügbarkeit im Falle der Zerstörung oder Diebstahl des Fahrzeugs nicht gewährleistet werden. Es ist daher zwingend eine Übertragung auf einen neutralen Backend-Server erforderlich.

Die internationalen Vorschriften schließen bereits heute für vernetzte Fahrzeuge eine externe Speicherung nicht aus.

Für die Ausgestaltung der externen Speicherung auf internationaler Ebene ist es essentiell, dass Akteure, die ein eigenes Interesse an den Daten haben, faktisch kein Monopol auf die Hoheit über die Fahrzeugdaten erhalten dürfen.

Es muss daher sichergestellt sein, dass nicht etwa der Fahrzeughersteller oder der Infrastrukturbetreiber als potentielle Haftungsgegner den Datenzugang verwalten.

Allein die Speicherung der Daten auf einem unabhängigen Backend, das von einer neutralen und hoheitlichen Stelle überwacht wird, gewährleistet einen fairen Zugang für alle autorisierten Parteien unter denselben rechtlichen Voraussetzungen.

Die redundante und neutrale Speicherung garantiert darüber hinaus die Authentizität, Integrität und Verfügbarkeit der Daten und gewährleistet damit eine manipulationssichere und transparente Feststellung, wer oder was die Fahrzeugsteuerung innehatte.

Die Speicherung bei einer neutralen und unabhängigen Stelle ist eine notwendige Grundlage für eine effiziente und zweckgebundene Nutzung der Daten im Sinne der Fahrzeugnutzer unter Wahrung der datenschutzrechtlichen Prinzipien „privacy by design“ und „privacy by default“.

2. Die Verwaltung des Zugangs für berechtigte Dritte zu einem unabhängigen Backend muss über eine hoheitliche Stelle erfolgen.

Begründung: In Zeiten der Digitalisierung muss dem Verbraucher ein einfacher und datenschutzkonformer Zugang zu seinen Daten gewährt werden. Die Authentifizierung und Autorisierung der Zugriffsberechtigung über eine mit hoheitlichen Aufgaben beliehene Stelle ermöglicht es dem Fahrzeugnutzer, auf einfache, schnelle und kostengünstige Weise zu prüfen, ob er sich beispielsweise gegen den Vorwurf einer Geschwindigkeitsübertretung entlasten kann, weil das System die Fahrzeugsteuerung innehatte.

Demgegenüber ist das Auslesen der Daten aus dem Fahrzeug mit einem hohen Aufwand und zusätzlichen Kosten für Verbraucher und Behörden verbunden.

Der einfach handhabbare Zugriff über einen Web-Service gibt dem Verbraucher die Möglichkeit, seine Rechte effektiv wahrzunehmen. Der Fahrzeugnutzer bleibt Herr seiner Daten und kann deren Übermittlung entsprechend § 63a Abs. 3 StVG eigens und direkt veranlassen.

Hierdurch werden die Kosten für Verbraucher und Behörden erheblich reduziert.

Die Speicherung auf einem neutralen Backend hat mithin Vorteile bei der Datenverarbeitung. Der Betreiber des neutralen Backends hat selbst keine Lese- und Schreibrechte für die Daten. Die Daten werden verschlüsselt und für den Betreiber anonymisiert gespeichert.

In Bezug auf Abfragen und Zugangsrechte trägt die Verwendung von Berechtigungszertifikaten zur Datensicherheit bei. Die Daten werden verschlüsselt und nur für eindeutig bestimmte Zwecke oder mit ausdrücklicher Einwilligung des Fahrzeugnutzers an autorisierte Parteien übermittelt.

Auf diese Weise wird ein datenschutzkonformes und verbraucherfreundliches Management des Datenzugangs gewahrt.

3. Zum Schutz vor unberechtigten Zugriffen bei Wechsel des Halters des Fahrzeuges sind die Daten nach erfolgreicher Übertragung auf das neutrale Backend im fahrzeuginternen Speicher zu löschen.

Begründung: Im Anwendungsbereich der Europäischen Datenschutz-Grundverordnung dürfen die personenbezogenen Daten des alten Fahrzeughalters bei einem Verkauf eines Fahrzeugs für den neuen Halter nicht mehr zugänglich sein. Hierfür könnte eine Löschung, beispielsweise durch das Zurücksetzen des Fahrzeugs auf Werkseinstellungen durchgeführt werden.

Sofern während der Speicherfrist ein Zugriff auf die Daten erforderlich wird, ist dies für den alten Fahrzeughalter faktisch ausgeschlossen. Die lokale Speicherung führt damit zu unlösbaren Situationen.

Hier gewährleistet die neutrale und datenschutzkonforme Speicherung auf einem Backend unter Einhaltung höchster IT-Sicherheitsstandards eine interessengerechte Lösung für alle Parteien, indem Daten nur an den autorisierten Zugangsberechtigten herausgegeben werden.

Der alte Fahrzeughalter hat auch nach einem Fahrzeugverkauf die Möglichkeit, innerhalb der Speicherfrist auf seine alten Fahrzeugdaten zuzugreifen; beispielsweise für die Beweisführung seiner Unschuld bei einem angeblichen Verkehrsverstoß.

Die Löschung des internen Speichers nach erfolgreicher Datenübertragung verhindert effektiv Möglichkeiten des Datenmissbrauchs und wahrt darüber hinaus den Grundsatz der Datenminimierung.

Ferner wird der notwendige Einbau eines internen Speichermediums zu höheren Herstellungskosten führen, die üblicherweise im Ergebnis der Verbraucher zu tragen hat. Die mit der vorzeitlichen Übertragung und Löschung der Daten einhergehende Speicherplatzminimierung für den internen Speicher bewirkt hingegen eine Kostenminimierung für Verbraucher.

4. **Um seine Rechte effektiv wahrzunehmen, muss der Fahrzeugführer die Möglichkeit haben, Daten über einen Web-Service abzurufen**

Begründung: Carsharing-Angebote werden zunehmend populärer, sodass auch über einen relativ kurzen Zeitraum mit einem häufigen Fahrerwechsel zu rechnen ist. Kommt es zu einem Verkehrsverstoß leitet das Carsharing- oder Mietwagenunternehmen als Fahrzeughalter den Bußgeldbescheid an den jeweiligen Fahrzeugführer/ -nutzer weiter. Der Fahrzeugführer kann in der Regel bei Erhalt des Bußgeldbescheides mangels Verfügungsgewalt über das Fahrzeug keine Daten mehr auslesen lassen. Das Angebot, Fahrzeugdaten über einen Web-Service abzurufen gibt dem Fahrzeugführer hingegen eine effektive Möglichkeit an die Hand, die Erfolgsaussichten eines Einspruchs gegen den Bußgeldbescheid selbst zu prüfen.

Er kann eruieren lassen, ob zum Zeitpunkt des vorgeworfenen Verstoßes bspw. das System die Fahrzeugsteuerung übernommen hatte oder ein falsches Signal einer C-ITS Station gesendet wurde.

5. **Allgemeine Zugriffsrechte zur Überprüfung der Funktionsfähigkeit auf den fahrzeuginternen Fahrzeugspeicher sind zu regulieren**

Begründung: Das mit Einführung des Datenspeichers verfolgte Ziel, Haftungsfragen eindeutig zu klären, setzt eine ausreichende Qualität der Mess-Sensorik und eine Genauigkeit der Datensätze voraus.

Die Plausibilität (Zeitstempel/Position) und die Genauigkeit des Datensatzes müssen barriere- und diskriminierungsfrei über den gesamten Fahrzeuglebenszyklus im Rahmen der Fahrzeuguntersuchung zu überprüfen sein. Dazu muss mindestens der zuletzt gespeicherte Datensatz über eine elektronische Fahrzeugschnittstelle auslesbar sein.

Sofern zum Auslesen des Datensatzes entsprechende Zugriffsschutzmaßnahmen implementiert werden, sind für die gesetzliche Fahrzeuguntersuchung entsprechende Zugriffsrechte (z. B. über ePTI-Zertifkate) zu gewähren.

6. **Der Vorgang des Zugangs auf den fahrzeuginternen Datenspeicher ist in den internationalen Vorschriften zu verankern und mittelfristig zu standardisieren.**

Begründung: Für einen sicheren und praktikablen Zugang muss der Zugriff über die fahrzeuginternen Schnittstellen standardisiert erfolgen. Zertifikate, die von einer neutralen Stelle verwaltet werden, gewährleisten darüber hinaus die Einhaltung aktuellster IT-Sicherheitsstandards.

7. **Der Datensatz kann nach Ablauf der gesetzlichen Verjährungsfrist des entsprechenden Landes der Datenerhebung gelöscht werden.**

Begründung: Die Festschreibung der o.g. Speicherfristen ist erforderlich, um zu gewährleisten, dass die erforderlichen Daten zur Feststellung, wer oder was die Fahrzeugsteuerung innehatte, bei Ordnungswidrigkeiten und Unfallereignissen innerhalb der gesetzlichen Verjährungsfrist zur Verfügung stehen. Dabei sind die landesspezifischen Verjährungsfristen zu berücksichtigen.

Die neutrale Stelle ist für die Einhaltung der Speicherfristen auf dem Backend-System verantwortlich und stellt sicher, dass Daten erst nach Ablauf der Fristen unwiderruflich gelöscht werden.

8. **Der Datensatz ist mit Zeit- und Positionsangaben zu speichern.**

Begründung: Ziel der verpflichtenden Einführung eines Fahrmodusspeichers ist die Feststellung, wer oder was die Fahrzeugsteuerung innehatte oder ob der Fahrzeugführer zur Übernahme der Fahrzeugsteuerung aufgefordert wurde, um anhand dieser Daten die Haftungsfrage zwischen Fahrer und System eindeutig zu klären.

Die Beurteilung der Haftungsfrage wird insbesondere in der Übernahmephase von verschiedenen Faktoren (rechtzeitige Aufforderung durch das System, Reaktionszeit des Fahrzeugführers, etc.) abhängen, die vornehmlich die Gerichte zu klären haben.

Für die Beurteilung, ob noch das System oder schon der Fahrzeugführer die Fahrzeugsteuerung innehatte ist ebenfalls entscheidend, ob der Fahrzeugführer beispielsweise wegen schlechter Wetterverhältnisse, wegen einer plötzlich auftretenden technischen Störung eines automatisierten Fahrerassistenzsystems oder eines unplausiblen C-ITS-Signals zur Übernahme aufgefordert wurde.

Die Genauigkeit des GPS/GNSS soll sich zunächst an den technischen Anforderungen der UN/ECE Regelung 144 (AECS) orientieren.

Für eine eindeutige Feststellung ist daher die Speicherung folgender Inhalte mit der jeweiligen Zeit- und Positionsangabe erforderlich:

- Status des Systems SAE - Level 3 und höher (z. B. Ein/Aus)
- Übernahmefähigkeit des Fahrzeugführers
- Übernahmeaufforderung
- Minimal Risk Manouvres
- Übernahme der Fahrzeugsteuerung
- Grund für die Übernahmeaufforderung
- Empfang C-ITS-Signale