

Information des DIN-Verbraucherrates

DIGITALE SICHERHEIT - Daten im Auto – lokal und vernetzt

Am Beispiel eines Autos wird in diesem Dokument exemplarisch die technische Entwicklung hin zum vernetzten Produkt gezeigt. Es gibt einen Einblick in die Datensammlung durch Autos sowie ihre weitere Verwendung – sowohl lokal also auch vernetzt. Des Weiteren wird auf die Verarbeitung sowie die Eigentumsverhältnisse der Daten Bezug genommen und Ausblick auf mögliche Geschäftsmodelle auf Basis der gesammelten Daten gegeben.

Das Ziel ist, die in diesem Dokument aufgezeigten Erkenntnisse und Informationen sinnhaft auch auf andere Produkte mit zunehmender Vernetzung übertragen zu können.

Der Wandel von lokal zu vernetzt

Autos verfügen über eine Vielzahl von Sensoren, mit denen Informationen und Daten gesammelt werden können. Ursprünglich wurden diese Informationen dazu genutzt, bestimmte Funktionen im Fahrzeug – ohne eine Vernetzung nach außen – zu ermöglichen. Beispiele hierfür sind z.B.:

- der Sensor im Gurtschloss (in Verbindung mit der Sitzbelegungserkennung), der anzeigt, ob der Gurt angelegt ist;
- der Raddrehzahlsensor, der ein eventuelles Blockieren des Rades erkennt und somit für die Steuerung des Antiblockiersystems nötig ist.

Mit zunehmender Vernetzung können die durch die Sensoren gesammelten Daten weiterverarbeitet werden. Hierdurch sind Rückschlüsse auf die Fahrer bzw. Insassen möglich. Durch die Nutzung vieler Sensoren und Datenquellen im Auto ergibt sich ein durchaus „erschreckend“ genaues Profil, was mitunter von Verbrauchern nicht gewünscht bzw. ihnen überhaupt nicht bekannt ist. Dieses Bild ist dann möglicherweise nicht mehr nur lokal im Fahrzeug gespeichert, sondern durch die Vernetzung auch von außen zugänglich. Die gesammelten Daten gewinnen auch immer stärker an wirtschaftlicher Bedeutung. Deren Auswertung ermöglicht die Entwicklung neuer Dienste rund um das Auto.

Welche Daten werden heute im Auto gesammelt?

Grundsätzlich können im Auto anfallende Daten in die Kategorien: Umgebungsdaten, fahrzeugbezogene Daten und kundeneigene - beziehungsweise vom Fahrer eingebrachte - Daten eingeteilt werden.

Grundsätzlich kann zwischen Daten unterschieden werden, die offline und online gespeichert werden. Bei der Offline-Speicherung findet die Datenspeicherung und -verarbeitung innerhalb des Fahrzeugs statt. Diese Daten (z. B. technische Fahrzeugdaten) verbleiben im Fahrzeug und werden nicht an den Hersteller oder dritte Anbieter übermittelt.

Bei der Online-Speicherung werden Daten aus dem Fahrzeug heraus übermittelt und anschließend z. B. auf den Backend-Servern der Fahrzeughersteller oder auch der Anbieter von Connectivity-Diensten und -Anwendungen oder in der Cloud gespeichert.

Welche Daten genau, in welchen zeitlichen Abständen und ob automatisch oder per Abruf, übermittelt werden, ist abhängig vom Fahrzeughersteller.

Eine Untersuchung des ADAC hat gezeigt, dass zum Beispiel bei einer Mercedes Benz B-Klasse von 2018 mit „me connect“ folgende Daten gesammelt und verarbeitet werden:

- Übertragung ins Backend des Herstellers:

Daten	erlaubt Rückschlüsse auf
GPS Position und Fahrzeugdaten (z. B. Kilometerstand, Verbrauch, Tankfüllung, Reifendruck und Füllstände von Kühlmittel, Wischwasser oder Bremsflüssigkeit)	Fahrverhalten und Wartung

- Speicherung lokal im Fahrzeug:

Daten	erlaubt Rückschlüsse auf
Anzahl der elektromotorischen Gurtstraffungen	Fahrstil
Informationen über zu hohe Motordrehzahl oder -temperatur	Fahrstil
gefahrte Kilometer auf Autobahnen, Landstraßen und in der Stadt ("highway-conditions", "road-conditions" und "urban-conditions") werden getrennt gespeichert	Nutzungsprofil
Betriebsstunden der Fahrzeugbeleuchtung	Nutzungsprofil
letzten 100 Lade- und Entladezyklen der Starterbatterie mit Uhrzeit und Datum sowie Kilometerstand	Fahr- und Standzeiten

Bei einem BMW der 3er Reihe von 2015 werden darüber hinaus unter Umständen auch die folgenden Daten verarbeitet:

Daten	erlaubt Rückschlüsse auf
erreichte Maximal-Drehzahl des Motors mit jeweiligem Kilometerstand	Fahrstil
Anzahl der Fahrtstrecken zwischen null und fünf, fünf und 20, 20 und 100 sowie über 100 Kilometer	Nutzungsprofil
Dauer, wie lange der Fahrer in verschiedenen Modi des Automatikgetriebes (Dauer/Manuell/Sport) unterwegs war	Fahrstil
Zahl der Verstellvorgänge des elektrischen Fahrersitzes	Anzahl der Fahrer
Anzahl der eingelegten Medien des CD-/DVD-Laufwerks	Intensität der Nutzung

Die gezeigten Listen sind nicht vollständig. Je nach Fahrzeugtyp werden weitere oder andere Daten gesammelt und verarbeitet – sowohl offline im Fahrzeug als auch im Backend des Herstellers.

Derzeit wissen nur die Fahrzeughersteller, welche Daten in Autos erzeugt, verarbeitet, gespeichert und gesendet werden.

Wer möchte Zugriff auf die Daten?

Daten aus dem Fahrzeug sind zum einen Grundlage für Dienste, die sich der Fahrer oder die Fahrerin wünscht, wie zum Beispiel die Navigation. Zum anderen gibt es auch viele Dritte, die gerne Zugriff auf die Fahrzeugdaten haben möchten oder die dies bereits heute haben, um zum Beispiel Ferndiagnosen durchführen zu können. Zu diesen Dritten gehören Werkstätten, Autohändler, Autohersteller, Dienstleister wie Autovermietungen, Behörden und Versicherer.

Wem gehören die Daten?

Daten gelten als personenbezogen, wenn sie „Einzelangaben über persönliche oder sachliche Verhältnisse“ eines Nutzers enthalten und damit einen Rückschluss auf dessen Person zulassen.

Bei Daten, die den Nutzern weder unmittelbar noch mittelbar zugeordnet werden können, handelt es sich um anonyme und somit um keine personenbezogenen Daten.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist der Auffassung, dass alle Kfz-Daten (Fahrzeugsystem-, -betriebs- und -standortdaten) einen Personenbezug aufweisen, da sie mit der Fahrzeugidentifikationsnummer oder mit dem Kfz-Kennzeichen verknüpft werden können und auf diese Weise Rückschlüsse auf den Fahrer oder zumindest den Halter des Fahrzeugs erlauben.

Besonders brisant kann es werden, wenn Daten mehrerer Sensoren zusammengeführt und kombiniert werden (Sensorfusion). Dadurch könnten auf Basis von vermeintlich unverfänglichen Daten umfangreiche Nutzerprofile gebildet werden, die unter anderem Rückschlüsse auf Fahrverhalten, Lebensgewohnheiten, Wohnort oder persönliche Interessen des Nutzers erlauben.

Erhebung, Verarbeitung und Nutzung von Daten

Für den reinen Fahrbetrieb ist nach Ansicht der Datenschützer in der Regel keine Datenspeicherung erforderlich. Werden Daten zwischen Fahrzeugen (Car-to-Car-Kommunikation) ausgetauscht, müssen sie wirksam verschlüsselt bzw. vor unbefugter Nutzung geschützt werden. Dies gilt auch bei einer Datenübertragung auf Server (z. B. der Hersteller). Die Daten müssen auf solchen Back-End-Systemen sicher gespeichert werden und nach Nutzungsende gelöscht werden. Auch darf ein Zugriff durch unbefugte Dritte auf die entsprechenden Schnittstellen im Fahrzeug, oder auch der Back-End-Systeme nicht möglich sein. Den Nutzern muss es möglich sein, personenbezogene Daten zu löschen, soweit die Speicherung nicht gesetzlich notwendig ist.

Grundsätzlich ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach deutschem Datenschutzrecht nur erlaubt, wenn hierfür eine Erlaubnis durch Rechtsvorschrift vorliegt oder aber eine Einwilligung seitens des Betroffenen erteilt wurde. Hierbei ist auch die Nutzung des Autos durch eine andere Person zu beachten, wenn durch das Auto personenbezogene Daten gesammelt werden (z. B. durch Nutzung eines telematikbasierten Versicherungstarifs).

Eine Erlaubnis durch Rechtsvorschrift bedeutet z. B.:

- Datenverarbeitung wird als Mittel unter den in der Rechtsvorschrift genannten Voraussetzungen für die Erfüllung eigener Geschäftszwecke eingesetzt;
- Verarbeitung der Daten ist zulässig, wenn die verantwortliche Stelle ein berechtigtes Interesse an den Daten hat, das gewichtiger ist als mögliche schutzwürdige Interessen des Betroffenen. Ein Beispiel hierfür wäre die Information über mögliche Gefahrenstellen auf der Straße (Stau, Glatteis).

Daten dürfen auch verarbeitet werden, wenn sie öffentlich zugänglich sind und keine schutzwürdigen Interessen einer Verwendung entgegenstehen.

Grundsätzlich ist es in der Praxis mitunter schwierig festzustellen, ob nur so viele Daten erhoben werden, wie für die Erfüllung der Leistung tatsächlich notwendig sind. Bei der Datenerhebung beziehungsweise -nutzung auf Grundlage einer Einwilligung besteht die Gefahr, dass die Einwilligung vorschnell abgegeben wird oder nicht wirklich selbstbestimmt erfolgt. Darüber hinaus muss die Einwilligung zur Datenerhebung auf klaren und transparenten Grundlagen erfolgen. Derzeit sind generische Zustimmungen häufig anzutreffen, die nicht transparent darstellen, welche Daten erhoben und wofür sie verwendet werden.

Verantwortlichkeiten für die Daten

Eine gemeinsame Erklärung der Datenschutzbeauftragten von Bund und Ländern und des Verbandes der Automobilindustrie (VDA) differenziert zwischen offline und online gespeicherten Daten.

Demnach wird bei *offline gespeicherten Daten* derjenige zur verantwortlichen Stelle, der personenbezogene Daten aus dem Fahrzeug ausliest und verarbeitet (z. B. bei Wartung und Reparatur). In der Regel sind das die Werkstätten. Auch wenn Fahrzeughersteller die offline gespeicherten Daten nicht selbst erheben, sind sie für den Schutz und die Sicherheit der Daten im Fahrzeug verantwortlich (Schutz der Schnittstellen nach außen gegen unbefugten Zugriff. Darüber hinaus gilt das Gebot so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen (Datensparsamkeit).

Bei *online gespeicherten Daten* sind diejenigen für den Schutz und die Sicherheit der Daten verantwortlich, die personenbezogene Daten erhalten, beziehungsweise aus dem Auto heraus übermittelt bekommen. In der Regel sind das die Fahrzeughersteller und Anbieter von digitalen Diensten.