44. Jahrgang
datenschutz-berater.de
DSB 06/2020

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Datenschutz im Fokus

Fragen aus der Praxis

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Maria Fetzer, Peter Hense

„Ein Auto, ein Computer, ein Mann“ – Connected Cars zwischen infantiler Vision und Consumer Privacy

Die Evolution des traditionellen Automobils weg vom Fortbewegungsmittel hin zu stark vernetzten Endgeräten stellt den bereits gut regulierten Mobilitäts- und Straßenverkehrssektor vor eine datenschutzrechtliche Mammutaufgabe. War das Automobil früher stets ein Rückzugsort im Autokino, Privatissimum für Dates, Sehnsuchtsobjekt in Road Movies, potentes Statussymbol und nicht nur der Deutschen „liebstes Kind“, so gilt „my home is my car is my castle“ im Jahr 2020 nicht mehr. Fahrzeuge senden, empfangen und verarbeiten große Datenmengen, voneinander, aus ihrer Umwelt, über ihre Fahrer*innen. Der technische Fortschritt hält Gesetzgeber, Wettbewerber, Verbraucherschützer und Behörden auf Touren. Einige Leitplanken für den Grundrechtsschutz in Europa sind Gegenstand dieses Beitrags.

Zurück in die Zukunft

Der gesellschaftliche wie rechtliche Diskurs im Zuge der fortschreitenden Fahrzeugautomatisierung läuft bereits auf Hochtouren. Hochauflösende Sensortechnik, der diffuse Wunschtraum von Level 5-Autonomie („brain off“) für Berufspendler, der Einsatz von vollautonomen Shuttles zum Transport von COVID19-Tests oder gar Flugtaxis bestimmen derzeit das mediale Bild aus Konsumentensicht. Die Vorteile hochautomatisierter Fahrzeuge wären durch die populärkulturellen Vorbilder aus Filmen nicht schwer zu vermitteln, doch ist die Akzeptanz von „Smart Cars“ in der Bevölkerung laut aktuellen Studien nach wie vor verhalten. Bedenken resultieren insbesondere aus dem fehlenden Vertrauen in die dauerhafte Funktionsfähigkeit dieser Fahrzeugsysteme, insbesondere der Angst, dass diese unterwandert oder „gehackt“ werden könnten. Diese Sorge ist angesichts der Masse an verarbeiteten personenbezogenen Daten und der schier unbestimmten Vielzahl externer Dritter, die Zugriff auf generierte Daten in automatisierten Fahrzeugen haben, nicht unbegründet. Der Kampf der Automobilindustrie auf dem Terrain innovativer Informations- und Kommunikationstechnik ist spätestens seit Hinzutreten monopolistischer IT-Unternehmen und Plattformanbieter zu einem Überlebenskampf geworden. Wenig wissenschaftlich werden Daten vielfach plakativ als das „Öl“ des 21. Jahrhunderts apostrophiert, was bereits deshalb falsch ist, weil es sich bei „Öl“ um einen endlichen und toxischen Rohstoff handelt, der mit technisch generierten, beliebig reproduzierbaren Daten, d. h. Geräteinformationen nur wenig gemein hat. Wer „Daten“ sagt, meint in der Regel eher deren Aggregatoren, Plattformen, die bereits heute den Großteil der IT-Infrastruktur und Betriebssysteme dominieren und sich anschicken, Automobilhersteller anzugreifen und sich zwischen Fahrer und Hersteller zu drängen. So hat es die Plattformökonomie bereits mit anderen Dienstleistungs- und Industriebranchen erfolgreich vorgemacht, nicht zuletzt dank großzügiger Haftungsprivilegien, von denen Automobilhersteller nur träumen können. Länderübergreifende datenschutzrechtliche Konzepte und Leitlinien sind essenziell, um nicht nur den technischen Fortschritt zu begleiten, sondern auch die datenschutzrechtlichen Anforderungen im Zusammenhang mit der Entwicklung des autonomen Automobils in geregelte Bahnen zu lenken.

Draft Guidelines des EDPB: Sicherheit geht vor

Der Europäische Datenschutzausschuss („European Data Protection Board“; im Folgenden: EDPB) veröffentlichte am 28.01.2020 den Entwurf für Leitlinien zur Verarbeitung personenbezogener Daten im Zusammenhang mit verbundenen Fahrzeugen und mobilitätsbezogenen Anwendungen. In diesen Guidelines positioniert sich der EDPB insbesondere zu zentralen Themen wie der Ausgestaltung von Datenschutzinformationen im Fahrzeug, dem Erfordernis von Datenschutzfolgeabschätzungen sowie dem Anwendungsbereich der Richtlinie 2002/58/EG („ePrivacy-Richtlinie“). Dies ist zu begrüßen, wenngleich die Leitlinien zentrale Compliance-Themen, wie z. B. die Bild- und Umfelderfassung durch im Fahrzeug integrierte Kamerasysteme oder Dashcams, die eine hohe Datenschutzrelevanz aufweisen, bislang aussparen und somit grundlegende Vorgaben in diesem Bereich (z. B. für „on board data processing“) vermissen lassen. Immerhin setzt der EDPB mit den veröffentlichten vorläufigen Guidelines jedoch ein wichtiges Zeichen und weist Automobilherstellern und weiteren Beteiligten die Richtung auf dem Weg zur Datenschutzkonformität in „Smart Cars“.

IT-Security und hybride Datenverarbeitung

Nahezu alle der in vernetzten Fahrzeugen generierten bzw. verarbeiteten Daten weisen Personenbezug auf, was angesichts des weiten, wenngleich oft bekämpften Begriffs des „Personenbezugs“ nicht verwundert. Gelegentlich überraschend für außereuropäische Marktbegleiter ist, dass auch Punktwolken-Datensets, die durch hochauflösende LiDAR-Sensoren erzeugt werden, in einem georeferenzierten

Koordinatensystem personenbezogene Daten darstellen. Zu den besonders zu schützenden Datenkategorien bei „Smart Cars" zählen laut EDPB vor allem diese Standortdaten, biometrische Daten sowie Daten, die Rechtsverstöße oder Verkehrsverletzungen aufdecken können. Jedoch sind auch technische Daten, z. B. das Bremsverhalten, die Motordrehzahl, aber auch Daten aus Infotainmentsystemen (Adressbuch, Musikvorlieben, Bluetooth-Connections etc.) nicht minder datenschutzrechtlich relevant. All diese Informationen lassen nicht nur Rückschlüsse auf das individuelle Fahrverhalten zu, sondern liefern diversen Interessengruppen (Versicherungen, Herstellern, Car-Sharing-Anbietern etc.) zusätzliche Angaben über Bewegungs- und Verhaltensmuster der Fahrzeugführer, Insassen sowie andere Straßenverkehrsteilnehmer, die sich im Umfeld des Fahrzeugs aufhalten. Im Bereich der Umfeldsensorik wird diesem Risiko seitens der Automobilhersteller mitunter durch hardwareseitige Unkenntlichmachung („Blurring") von Personen und Objekten im Umkreis des Fahrzeugs begegnet, um zumindest eine Reduktion des Erfassungsbereichs sowie einen Einstieg in die privilegierte Verarbeitung pseudonymer Daten zu erreichen. Dabei sind auch schemenhafte Bilder aufgrund der Gesamtumstände der Aufnahmen (Kleidung, Nachbarschaft, Uhrzeit, Standort etc.) oft noch zu einfach personenbeziehbar, um von einer wirkungsvollen Pseudonymisierung i. S. d. Art. 4 Nr. 5 DSGVO zu sprechen.

Die Vielzahl an Diensten, Schnittstellen und Funktionseinheiten in „Smart Cars" erhöhen die Anzahl von Angriffsvektoren und damit die Gefahr von Fremdzugriffen und einer Kompromittierung der Datensätze. Das EDPB betrachtet daher vernetzte Fahrzeuge zurecht als „kritische Systeme", die oft nicht ausreichend gegen unbefugte Zugriffe geschützt sind. Nur liegt mangelnde IT-Sicherheit oft in der Natur der verbauten einzelnen Systeme, denen es an einem integralen Sicherheitskonzept ermangelt. Medienwirksame Horrorszenarien aus den vergangenen Jahren, in denen „Smart Cars" fremdgeöffnet, ferngesteuert oder auf der Autobahn zum abrupten Stillstand gebracht wurden, erodieren das Vertrauen in IT-Sicherheit. Ein guter Teil der Informationen aus dem Fahrzeug wird zudem nicht im Auto selbst, sondern außerhalb des Sicht- und Einflussbereichs der Nutzer an externen Standorten, wie z. B. Cloud-Infrastrukturen verarbeitet. Unsichere Übertragungswege erhöhen das Gefährdungspotential zusätzlich. Das EDPB fordert von den Herstellern daher deutlich eine entsprechende datenschutzgerechte Konfiguration der Fahrzeuge sowie die Implementierung kryptographischer Algorithmen und einer sicheren Anwendungsplattform im Fahrzeug ein, wobei letztere physisch von den sicherheitsrelevanten Fahrzeugfunktionen getrennt sein sollte. Konkret spricht sich der EDPB dafür aus, eine „hybride Verarbeitung" einzurichten, wonach z. B. aus personenbezogenen Daten zum Fahrverhalten unmittelbar numerische Werte bzw. aggregierte Scores erzeugt werden, um einen Zugriff z. B. von Telematik-Versicherungen auf rohe (Fahr) Verhaltensdaten zu verhindern. Dieser Vorschlag stellt neben der ebenso wichtigen physischen Trennung der lebenswichtigen Funktionen des Fahrzeugs von bloßen Infotainmentsystemen sowie hinreichender Redundanz einen wichtigen Baustein auf dem Weg zur datenschutzkonformen Konzeptionierung vernetzter Fahrzeuge dar, die vorrangig die Umsetzung der Grundsätze „privacy by design" und „privacy by default" gem. Art. 25 DSGVO erfordert.

Der Kampf ums Cockpit: Informationspflichten

Bei mobilen Endgeräten bestimmen monopolistische IT-Unternehmen und Plattformanbieter den Markt. Deren Eindringen in den Markt der „Smart Cars" durch „In-Car-Systeme" führt dazu, dass Qualitätsansprüche in Hinblick auf die eingesetzte Soft- und Hardware auf das Niveau von ausfallgeneigten Billighandys absinken. Plattformanbieter scheitern durch ihren Ansatz, „break things first, ask forgiveness later" bereits an einem der ersten datenschutzrechtlichen Grundsätze: Dem Erfordernis hinreichender Transparenz. Besonders bei stark automatisierten und vernetzten Fahrzeugen sind betroffene Fahrzeugnutzer (Fahrer, Halter, Insassen etc.) darauf angewiesen, präzise und korrekte Informationen über die verarbeiteten Daten zu erhalten, die ihnen die Ausübung von Betroffenenrechten ermöglichen. Es ist zu begrüßen, dass sich der EDPB auch zur Problematik der Erfüllung von Informationspflichten nach Art. 12 ff. DSGVO äußert, denn herstellerseitig fehlt es hier bislang an einer einheitlichen Umsetzung datenschutzrechtlicher Vorgaben. Hier soll laut Vorschlag des EDPB eine standardisierte Icon- bzw. Symbollösung helfen, die gut sichtbar z. B. im Bordcomputer integriert werden kann und die Fahrzeugnutzer leicht verständlich und klar auf die jeweilige Verarbeitung hinweist, unabhängig von Fahrzeugmodell oder -marke. Dies schafft Transparenz, die Nutzer gerade in „Smart Cars" oft vergeblich suchen und ist besonders für Carsharing-Anbieter und Autovermietungen von großer Relevanz. In Bezug auf Autovermietungen als potenzielle Joint Controller nach Art. 26 DSGVO fordert der EDPB zusätzlich, dass den Nutzern eine einfache Möglichkeit bereitgestellt werden muss, um die Datenverarbeitung nach Beendigung der Fahrzeugmiete jederzeit deaktivieren bzw. die verarbeiteten Daten löschen zu können, z. B. im Wege einer implementierten Löschtaste.

Zusätzlich sollten nach Ansicht des EDPB auch standardisierte Warnungen an Bord, beispielsweise akustische Signale bei der Verarbeitung besonders sensibler Daten verwendet werden, um Betroffene für die erfolgende Verarbeitung zu sensibilisieren. Das EDPB überträgt darüber hinaus den u. a. bereits von der Art.-29-Datenschutzgruppe in den Leitlinien für Transparenz vom 11.04.2018 empfohlenen Mehrebenen-Ansatz für Datenschutzinformationen

(„Information Layers“) auf vernetzte Fahrzeuge, wonach auf der ersten Informationsebene vor allem die für den Fahrzeugnutzer wichtigsten Informationen, wie z. B. die Zwecke der Verarbeitung, Informationen zur Identität des Verantwortlichen, zu den Empfängern und zu den Betroffenenrechten, bereitgestellt werden sollten. Hierbei sei auch verstärkt auf die Angabe der Art, der Branche und des Sitzes des Empfängers zu achten. Angesichts von länderübergreifenden Mobilitätskonzepten und der zunehmenden Vernetzung zwischen Fahrzeugen und Infrastruktur weist der EDPB zudem auf einen wichtigen, oft vernachlässigten Aspekt hin: Aktualisierte Datenschutzinformationen sind Betroffenen stets auch dann zur Verfügung zu stellen, wenn ein Wechsel der Verantwortlichkeiten erfolgt, z. B. wenn das Fahrzeug über Landesgrenzen hinweg fortbewegt und die Systeme im Fahrzeug, die für die Aufrechterhaltung der Funktionalitäten des Fahrzeugs sorgen, daraufhin von verschiedenen Diensteanbietern und Beteiligten verantwortet werden.

Einwilligung der Fahrzeugnutzer & DSFA

Automatisierten und vernetzten Fahrzeugen ist es immanent, dass sie insbesondere auf den Einsatz von Sensortechnik sowie zellularen Datenverbindungen angewiesen sind, um die Inanspruchnahme der Fahrzeugfunktionalitäten für den Nutzer zu gewährleisten. Daher werden „Smart Cars“ seitens des EDPB als funkgestützte Systeme bzw. „Endgeräte“ eingestuft, die in den Anwendungsbereich von Art. 5 Abs. 3 der „ePrivacy – Richtlinie“ fallen. Demnach erfordert sowohl jede Speicherung von Informationen als auch der Zugang zu bereits gespeicherten Informationen im „Smart Car“, die nicht zwingend erforderlich sind, um den vom Nutzer angeforderten Dienst bereitzustellen, die vorherige Einwilligung des Fahrzeugnutzers. Die Modalitäten der Einholung einer gültigen Einwilligung sind hierbei bereits seit geraumer Zeit Dreh- und Angelpunkt des juristischen Diskurses. Die Einwilligung muss a) individuell, b) zweckgebunden und c) informiert erfolgen und darf laut EDPB nicht mit dem Vertrag über den Kauf oder des Leasings eines neuen Fahrzeugs gekoppelt werden. Dies ist insofern nicht überraschend, hat jedoch weitreichende Folgen für Automobilhersteller und weitere Interessengruppen. Das EDPB betont zurecht, dass auch eine einmal erteilte Einwilligung keine weitere zweckändernde Verarbeitung legitimieren könne, da die Zustimmung informiert und spezifisch sein muss, um wirksam zu sein. Somit stellen die Ausgestaltung der angebotenen Dienste sowie die Gewinnung rechtskonformer Einwilligungen wohl eine der bedeutsamsten Compliance-Anforderung für die Verarbeitung personenbezogener Daten innerhalb von „Smart Cars“ dar. Die Bedeutung der Zweckgebundenheit der Einwilligung zeigt sich insbesondere bei der Verarbeitung von Telemetriedaten, die vordringlich der Wartung des Fahrzeugs dienen, jedoch auch für andere Beteiligte, wie z. B. Kfz-Versicherungsgesellschaften, zur Abrechnung von „pay as you drive“-Tarifen und entsprechender Policen von Bedeutung sind. An einer erneuten Einwilligung führt hier nach Ansicht des EDPB kein Weg vorbei.

Da „Smart Cars“ personenbezogene Daten in großem Umfang verarbeiten, lässt dies grundsätzlich auf ein hohes Risiko für die Rechte und Freiheiten für Betroffene schließen. Eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) je Fahrzeugtyp/-modell ist hierbei nicht nur der Risikominimierung zuträglich, sondern die Ergebnisse der Analyse könnten zudem dazu verwendet werden, datenschutzfreundliche Voreinstellungen bereits in der Konzeptionierung des Fahrzeugs zu etablieren. Zur Reduktion von Angriffspunkten bietet sich an dieser Stelle zudem eine frühzeitige Kooperation mit der jeweils zuständigen Aufsichtsbehörde an, idealerweise bereits in der Konzeptionierungsphase. Von dieser Möglichkeit machen bereits einige Unternehmen Gebrauch, wie ein Beispiel eines Automobilzulieferers aus dem aktuellen Tätigkeitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg zeigt.

Stellungnahme der niederländischen Datenschutzbehörde

Nach aktueller Stellungnahme vom 26.03.2020 entschloss sich auch die niederländische Datenschutzbehörde („Autoriteit Persoonsgegevens“) dazu, die Umsetzung datenschutzrechtlicher Vorgaben in vernetzten Fahrzeugen durch Automobilhersteller zu untersuchen. Dies überrascht nicht, veröffentlichte die niederländische Aufsichtsbehörde zuletzt im Februar 2020 bereits ein Handbuch, welches sich insbesondere der Information der Autofahrer hinsichtlich der Verarbeitungsvorgänge im Fahrzeug widmet und im Wege der Darstellung von Fallszenarien (Miete, Kauf, Leasing) verschiedene Handlungsoptionen für Betroffene beleuchtet. Die niederländische Datenschutzbehörde spricht sich zurecht dafür aus, dass es sich bei modernen Fahrzeugen um Elemente des Internets (of Things) handelt, für die innerhalb des Fahrzeugs gesteigerte Privatsphäre-Einstellungen sowie Lösch- und Widerrufsmöglichkeiten für Fahrzeugnutzer bereitgehalten werden müssen („Opt-in“ statt „Opt-out“). Dies überzeugt mit Blick auf die steigende Anzahl an Funktionalitäten, bereitgestellten Diensten und implementierten Schnittstellen im Fahrzeug, wie z. B. Web (TCP/IP), USB, RFID, Wi-Fi, die insbesondere die Versagens- und Angriffsmöglichkeiten erhöhen, wobei nicht nur personenbezogene Daten von Fahrern, sondern auch von Beifahrern und sonstigen Insassen kompromittiert werden könnten.

Fazit & Ausblick

Den aktuellen Stellungnahmen europäischer Aufsichtsbehörden ist der Appell zu entnehmen, dass sich Automobilhersteller vor allem auf die Umsetzung zentraler daten-

schutzrechtlicher Grundprinzipien wie Datenminimierung, Zweckbindung und Transparenzgebot besinnen sollten. Dies ist gerade im Hinblick auf die zum 05.01.2020 in Kraft getretene Verordnung (EU) 2019/2144 („General Safety Regulation") von Bedeutung, wonach Fahrzeuge beginnend ab dem Jahr 2022 serienmäßig mit weiteren (sicherheitsrelevanten) Fahrassistenzsystemen, wie z. B. Alcohol-Interlock-Systemen oder Geschwindigkeitsassistenten ausgestattet sein werden, welche die Qualität und Quantität an verarbeiteten personenbezogenen Daten zusätzlich erhöhen werden. Der Gefahr einer Aushöhlung des Datenschutzes in „Smart Cars" kann nur durch einheitliche datenschutzrechtliche Konzepte begegnet werden. Diese bieten nicht nur den Vorteil erhöhter Käuferakzeptanz, sondern auch die Chance, sich von anderen Wettbewerbern abzuheben.

Autoren: **Peter Hense ist Rechtsanwalt und Partner bei SPIRIT LEGAL Rechtsanwälte in Leipzig. Seine Tätigkeitsschwerpunkte liegen im Technologie-, Daten- und Wettbewerbsrecht sowie der Prozessführung (Privacy Litigation).**

Maria Fetzer (CIPP/E) ist Rechtsanwältin im Bereich Technologie und Datenschutzrechtmit Schwerpunkt Mobilität bei SPIRIT LEGAL Rechtsanwälte in Leipzig.