
# Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen

**Version 2.0**

**Angenommen am 9. März 2021**

## Versionsverlauf

| | | |
|---|---|---|
| Version 2.0 | 9. März 2021 | Annahme der Leitlinien nach öffentlicher Konsultation |
| Version 1.0 | 28. Januar 2020 | Annahme der Leitlinien für die öffentliche Konsultation |

# Inhaltsverzeichnis

## Der Europäische Datenschutzausschuss —

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung —

**HAT FOLGENDE LEITLINIEN ANGENOMMEN:**

# 1 EINLEITUNG

1. Als Symbol der Wirtschaft des 20. Jahrhunderts gehört das Automobil zu den Massenkonsumgütern, die die Gesellschaft insgesamt beeinflusst haben. Automobile werden häufig nicht als ein reines Transportmittel angesehen, sondern gemeinhin mit dem Begriff der Freiheit verbunden. Tatsächlich stellen sie einen privaten Bereich dar, in dem die Menschen eine Form der Entscheidungsfreiheit genießen können, ohne von außen beeinflusst zu werden. Doch da sich vernetzte Fahrzeuge immer stärker etablieren, entspricht diese Vorstellung heute nicht mehr der Realität. Die Konnektivität im Fahrzeug breitet sich rasant aus – von Luxusmodellen und Premium-Marken bis hin zu großvolumigen Mittelklassemodellen – und die Fahrzeuge werden zu massiven Datenzentren. Aber nicht nur die Fahrzeuge, sondern auch Fahrer und Insassen werden immer stärker vernetzt. Tatsächlich sind in vielen Modellen, die in den vergangenen Jahren auf den Markt gekommen sind, Sensoren und vernetzte Bordgeräte integriert, die unter anderem die Motorleistung, die Fahrgewohnheiten, die besuchten Orte und möglicherweise sogar die Augenbewegungen des Fahrers, seinen Puls oder biometrische Daten erheben und erfassen können, um eine natürliche Person eindeutig zu identifizieren.[2]

2. Diese Datenverarbeitung findet in einem komplexen Ökosystem statt, das nicht nur auf die traditionellen Akteure der Automobilindustrie beschränkt ist, sondern auch durch das Auftreten neuer Akteure aus der digitalen Wirtschaft geprägt wird. Diese neuen Akteure können Informations- und Unterhaltungsdienste wie Online-Musik, Straßenzustands- und Verkehrsinformationen anbieten oder Fahrerassistenzsysteme und -dienste wie Autopilot-Software, Aktualisierungen über den Fahrzeugzustand, nutzungsabhängige Versicherungen oder dynamisches Kartenmaterial zur Verfügung stellen. Da die Fahrzeuge über

[1] Soweit in diesen Leitlinien auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

[2] Infografik „Data and the connected car“ (Daten und das vernetzte Fahrzeug) des Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

elektronische Kommunikationsnetze verbunden sind, spielen die an diesem Prozess beteiligten Straßeninfrastrukturbetreiber und Telekommunikationsanbieter auch eine wichtige Rolle im Hinblick auf die potenziellen Vorgänge, mit denen die personenbezogenen Daten von Fahrern und Fahrzeuginsassen verarbeitet werden.

3. Darüber hinaus generieren vernetzte Fahrzeuge immer größere Datenmengen, von denen die meisten als personenbezogene Daten betrachtet werden können, da sie sich auf Fahrer oder Insassen beziehen. Auch wenn die von einem vernetzten Fahrzeug erhobenen Daten nicht direkt mit einem Namen, sondern mit technischen Aspekten und Merkmalen des Fahrzeugs verknüpft sind, betreffen sie den Fahrer oder die Insassen des Fahrzeugs. Zur Veranschaulichung: Daten über den Fahrstil oder die zurückgelegte Strecke, Daten über die Abnutzung von Fahrzeugteilen, Standortdaten oder von Kameras erhobene Daten können das Verhalten des Fahrers ebenso betreffen wie Informationen über andere Personen, die sich im Fahrzeug aufhalten, oder über betroffene Personen, an denen das Fahrzeug vorbeifährt. Solche technischen Daten werden von einer natürlichen Person erzeugt und ermöglichen ihre direkte oder indirekte Identifizierung durch die Person, die für die Verarbeitung der Daten verantwortlich ist (im Folgenden „Verantwortlicher“), oder durch eine andere Person. Das Fahrzeug kann als Endgerät betrachtet werden, das von verschiedenen Nutzern verwendet werden kann. Wie bei einem Personal Computer (PC) hat diese mögliche Vielzahl von Nutzern daher keinen Einfluss auf den persönlichen Charakter der Daten.

4. Im Jahr 2016 führte die Fédération Internationale de l'Automobile (FIA) eine europaweite Studie zum Thema „Mein Auto – Meine Daten“ durch, um ein Stimmungsbild darüber zu erhalten, wie die Europäer über vernetzte Autos denken.[3] Sie ergab, dass einerseits bei den Fahrern ein großes Interesse an Konnektivität besteht, andererseits aber auch in Bezug auf die Nutzung der von den Fahrzeugen erzeugten Daten Wachsamkeit geboten ist und der Einhaltung der Rechtsvorschriften zum Schutz personenbezogener Daten eine große Bedeutung zukommt. Daher besteht die Herausforderung für jeden Interessenträger darin, die Dimension „Schutz personenbezogener Daten“ bereits in der Phase der Produktgestaltung einzubeziehen und sicherzustellen, dass den Fahrzeugnutzern gemäß Erwägungsgrund 78 DSGVO Transparenz und Kontrolle in Bezug auf ihre Daten gewährleistet wird. Eine solche Vorgehensweise trägt dazu bei, das Vertrauen der Nutzer und damit die langfristige Entwicklung dieser Technologien zu stärken.

## 1.1 Themenbezogene Arbeiten

5. Vernetzte Fahrzeuge sind in den vergangenen zehn Jahren zu einem wichtigen Thema für die Aufsichtsbehörden geworden, wobei in den letzten Jahren ein starker Anstieg zu verzeichnen war. Auf nationaler und internationaler Ebene wurden daher verschiedene Arbeiten veröffentlicht, die sich mit der Sicherheit und der Privatsphäre in Bezug auf vernetzte Fahrzeuge befassen. Mit diesen Verordnungen und Initiativen sollen die bestehenden Rahmen zu Datenschutz und Privatsphäre durch sektorspezifische Vorschriften ergänzt bzw. den Fachkräften Anleitungen zur Verfügung gestellt werden.

[3] Kampagne „My Car My Data“ (Mein Auto – Meine Daten); http://www.mycarmydata.eu/

### 1.1.1 Initiativen auf europäischer und internationaler Ebene

6. Seit dem 31. März 2018 müssen alle neuen Fahrzeugtypen der Klassen M1 und N1 (Personenkraftwagen und leichte Nutzfahrzeuge) über ein auf dem 112-Notruf basierendes bordeigenes eCall-System verfügen.[4,5] Bereits im Jahr 2006 hatte die Artikel-29-Datenschutzgruppe ein Arbeitsdokument mit dem Titel „Eingriffe in den Datenschutz und die Privatsphäre im Rahmen der Initiative eCall" angenommen.[6] Darüber hinaus hat die Artikel-29-Datenschutzgruppe, wie bereits erwähnt, im Oktober 2017 eine Stellungnahme zur Verarbeitung personenbezogener Daten im Zusammenhang mit kooperativen intelligenten Verkehrssystemen (C-ITS) angenommen.

7. Im Januar 2017 veröffentlichte die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) eine Studie, die sich vor allem mit der Cybersicherheit und Resilienz intelligenter Personenkraftwagen befasst und eine Aufstellung der sensiblen Anlagen sowie der entsprechenden Bedrohungen, Risiken, Faktoren zur Risikominderung und möglichen Sicherheitsmaßnahmen enthält.[7] Im September 2017 erließ die Internationale Konferenz der Datenschutz- und Privatsphärebeauftragten (ICDPPC) einen Beschluss zu vernetzten Fahrzeugen.[8] Und schließlich verabschiedete die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation (IWGDPT) im April 2018 ebenfalls ein Arbeitspapier über vernetzte Fahrzeuge.[9]

### 1.1.2 Nationale Initiativen der Mitglieder des Europäischen Datenschutzausschusses (EDSA)

8. Im Januar 2016 veröffentlichten in Deutschland die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Verband der Automobilindustrie (VDA) eine gemeinsame Erklärung zu Datenschutz-Prinzipien für vernetzte und nicht vernetzte Fahrzeuge.[10] Im August 2017 veröffentlichte das britische Centre for Connected and Autonomous Vehicles (CCAV) einen Leitfaden, in dem die Grundsätze der Cybersicherheit für vernetzte und automatisierte Fahrzeuge dargelegt werden, um das

[4] The interoperable EU-wide eCall (Das interoperable EU-weite eCall-System); https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_de

[5] Beschluss Nr. 585/2014/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über die Einführung des interoperablen EU-weiten eCall-Dienstes (Text von Bedeutung für den EWR). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014D0585

[6] Arbeitsdokument: Eingriffe in den Datenschutz und die Privatsphäre im Rahmen der Initiative eCall; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_de.pdf

[7] „Cyber security and resilience of smart cars" (Cybersicherheit und Resilienz intelligenter Personenkraftwagen); https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[8] „Resolution on data protection in automated and connected vehicles" (Beschluss zum Datenschutz in automatisierten und vernetzten Fahrzeugen); https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

[9] Arbeitspapier „Vernetzte Fahrzeuge"; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/

[10] Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge; https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Gemeinsames%20Papier%20DSK%20und%20VDA_0.pdf

Bewusstsein für dieses Thema innerhalb der Automobilbranche zu schärfen.[11] Im Oktober 2017 veröffentlichte die französische Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) ein Compliance-Paket für vernetzte Fahrzeuge, um die Interessenträger bei der Einbindung des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen zu unterstützen, damit die betroffenen Personen eine wirksame Kontrolle über ihre Daten haben.[12]

## 1.2 Geltendes Recht

9. Der maßgebliche EU-Rechtsrahmen ist die DSGVO. Sie gilt in jedem Fall, in dem die Datenverarbeitung im Zusammenhang mit vernetzten Fahrzeugen die Verarbeitung personenbezogener Daten natürlicher Personen beinhaltet.

10. Zusätzlich zur DSGVO legt die Richtlinie 2002/58/EG in der überarbeiteten Fassung 2009/136/EG (im Folgenden „Datenschutzrichtlinie für elektronische Kommunikation" oder „ePrivacy-RL") einen **spezifischen Standard für alle Akteure fest, die auf einem Endgerät eines Teilnehmers oder eines Nutzers im Europäischen Wirtschaftsraum (EWR) gespeicherte Informationen speichern oder darauf zugreifen möchten.**

11. Während die meisten Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation (Artikel 6, Artikel 9 usw.) nur für Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze und -dienste gelten, ist Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation eine allgemeine Bestimmung. Sie gilt nicht nur für elektronische Kommunikationsdienste, sondern auch für alle privaten oder öffentlichen Einrichtungen, die Informationen auf einem Endgerät (im Folgenden auch „Endeinrichtung") ablegen oder lesen, unabhängig von der Art der gespeicherten oder abgerufenen Daten.

12. Der Begriff *„Endeinrichtung"* wird in der Richtlinie 2008/63/EG[13] definiert. Gemäß Artikel 1 Nummer 1 Buchstabe a sind Endeinrichtungen *„direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtungen zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet; b) Satellitenfunkanlagen mit ihren Einrichtungen";*

[11] Principles of cyber security for connected and automated vehicles (Grundsätze der Cybersicherheit für vernetzte und automatisierte Fahrzeuge); https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[12] Compliance package for a responsible use of data in connected cars (Compliance-Paket für einen verantwortungsvollen Umgang mit Daten in vernetzten Fahrzeugen); https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

[13] Richtlinie 2008/63/EG der Kommission vom 20. Juni 2008 über den Wettbewerb auf dem Markt für Telekommunikationsendeinrichtungen (kodifizierte Fassung) (Text von Bedeutung für den EWR); https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32008L0063&from=EN

13. Sofern die oben genannten Kriterien erfüllt sind, sollten das vernetzte Fahrzeug und das damit verbundene Gerät als *„Endeinrichtung“* betrachtet werden (genau wie ein Computer, ein Smartphone oder ein Smart-TV) und gegebenenfalls die Bestimmungen des Artikels 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation gelten.

14. Wie der EDSA in seiner Stellungnahme 5/2019 zum Zusammenspiel zwischen der ePrivacy-RL und der DSGVO[14] dargelegt hat, sieht Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation vor, dass in der Regel und vorbehaltlich der unter Randnummer 17 der vorliegenden Leitlinien genannten Ausnahmen von dieser Regel eine vorherige Einwilligung zur Speicherung von Informationen oder für den Zugriff auf bereits gespeicherte Informationen auf dem Endgerät eines Teilnehmers oder Nutzers erforderlich ist. Soweit es sich bei den auf dem Endgerät des Nutzers gespeicherten Informationen um personenbezogene Daten handelt, hat Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation in Bezug auf die Tätigkeit der Speicherung oder des Zugriffs auf diese Informationen Vorrang vor Artikel 6 DSGVO.[15] Jegliche Verarbeitungsvorgänge personenbezogener Daten, die im Anschluss an die vorgenannten Verarbeitungsvorgänge erfolgen, einschließlich der Verarbeitung personenbezogener Daten, die durch den Zugriff auf Informationen im Endgerät gewonnen werden, bedürfen einer Rechtsgrundlage gemäß Artikel 6 DSGVO, um rechtmäßig zu sein.[16]

15. Da der Verantwortliche, der eine Einwilligung zur Speicherung oder zum Zugriff auf Informationen gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation einholen will, die betroffene Person dabei über alle Zwecke der Verarbeitung informieren muss, einschließlich jeglicher Verarbeitung, die im Anschluss an die vorgenannten Verarbeitungsvorgänge erfolgt (d. h. die „nachfolgende Verarbeitung“), ist eine Einwilligung gemäß Artikel 6 DSGVO im Allgemeinen die am besten geeignete Rechtsgrundlage, um eine Verarbeitung personenbezogener Daten im Anschluss an diese Vorgänge zu erfassen (soweit der Zweck der anschließenden Verarbeitung von der Einwilligung der betroffenen Person erfasst wird, siehe Randnummern 53 und 54 der vorliegenden Leitlinien). Die Einwilligung wird daher wahrscheinlich sowohl für die Speicherung und den Zugriff auf bereits gespeicherte Informationen als auch für die nachfolgende Verarbeitung personenbezogener Daten die Rechtsgrundlage bilden.[17] Tatsächlich sollte bei der Beurteilung der Einhaltung des Artikels 6 DSGVO berücksichtigt werden, dass die Verarbeitung insgesamt spezifische Tätigkeiten beinhaltet, für die die Gesetzgebung in der EU einen zusätzlichen Schutz angestrebt hat.[18] Darüber hinaus müssen

[14] Europäischer Datenschutzausschuss, Stellungnahme 5/2019 zum Zusammenspiel zwischen der ePrivacy-RL und der DSGVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden, angenommen am 12. März 2019 (im Folgenden „Stellungnahme 5/2019“), Rn. 40.
[15] Ebd., Rn. 40.
[16] Ebd., Rn. 41.
[17] Die Einwilligung, die nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erforderlich ist, und die Einwilligung, die als Rechtsgrundlage für die Verarbeitung von Daten (Artikel 6 DSGVO) für denselben spezifischen Zweck erforderlich ist, können gleichzeitig eingeholt werden (z. B. durch Ankreuzen eines Kästchens, das eindeutig angibt, wozu die betroffene Person ihre Einwilligung erteilt).
[18] Stellungnahme 5/2019, Rn. 41.

die Verantwortlichen bei der Ermittlung der geeigneten Rechtsgrundlage die Auswirkungen auf die Rechte der betroffenen Personen berücksichtigen, um den Grundsatz der Angemessenheit zu wahren.[19] Somit kann Artikel 6 DSGVO von den Verantwortlichen nicht herangezogen werden, um den zusätzlichen Schutz, der durch Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation geboten wird, zu verringern.

16. Der EDSA erinnert daran, dass der Begriff der Einwilligung im Sinne der ePrivacy-RL dem Begriff der Einwilligung nach der DSGVO entspricht und alle Anforderungen einer Einwilligung nach Artikel 4 Nummer 11 und Artikel 7 DSGVO erfüllen muss.

17. Obgleich die Einwilligung der Grundsatz ist, lässt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation zu, die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät gespeichert sind, von der Anforderung der Einwilligung nach Aufklärung auszunehmen, wenn sie eines der folgenden Kriterien erfüllen:

    - **Ausnahme 1:** wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist;
    - **Ausnahme 2:** soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

18. In solchen Fällen beruht die Verarbeitung personenbezogener Daten, einschließlich der personenbezogenen Daten, die durch den Zugriff auf Informationen im Endgerät gewonnen werden, auf einer der Rechtsgrundlagen gemäß Artikel 6 DSGVO. Beispielsweise ist keine Einwilligung erforderlich, wenn die Datenverarbeitung notwendig ist, um von der betroffenen Person angeforderte GPS-Navigationsdienste zur Verfügung zu stellen, wenn diese Dienste als Dienste der Informationsgesellschaft eingestuft werden können.

## 1.3 Geltungsbereich

19. Der EDSA weist darauf hin, dass die vorliegenden Leitlinien die Einhaltung der Vorschriften bei der Verarbeitung personenbezogener Daten, die von der breiten Palette der in diesem Umfeld tätigen Akteure durchgeführt wird, erleichtern sollen. Es ist jedoch nicht vorgesehen, dass sie alle in diesem Zusammenhang möglichen Anwendungsfälle abdecken oder Hinweise zu jeder möglichen spezifischen Situation geben.

20. Der Geltungsbereich der vorliegenden Leitlinien umfasst insbesondere die Verarbeitung personenbezogener Daten im Zusammenhang mit der nichtgewerblichen Nutzung vernetzter Fahrzeuge durch betroffene Personen: beispielsweise auf Fahrer, Insassen, Fahrzeughalter, andere Verkehrsteilnehmer usw. Insbesondere bezieht es sich auf die folgenden personenbezogenen Daten: i) Daten, die im Fahrzeug verarbeitet werden, ii) Daten, die zwischen dem Fahrzeug und den mit ihm verbundenen persönlichen Geräten (z. B. dem Smartphone des Nutzers) ausgetauscht werden und iii) Daten, die lokal im Fahrzeug erhoben und zur Weiterverarbeitung an externe Einrichtungen (z. B.

[19] Europäischer Datenschutzausschuss, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0 vom 8. Oktober 2019, Absatz 1.

Fahrzeughersteller, Infrastrukturbetreiber, Versicherungsgesellschaften, Autowerkstätten) übertragen werden.

21. Die Begriffsbestimmung eines „vernetzten Fahrzeugs“ muss in diesen Leitlinien als umfassendes Konzept verstanden werden. Es kann als ein Fahrzeug definiert werden, das mit vielen elektronischen Steuergeräten (ECU) ausgestattet ist, die über ein fahrzeuginternes Netzwerk miteinander verbunden sind, sowie mit Konnektivitätseinrichtungen, die es ermöglichen, Informationen mit anderen Geräten sowohl innerhalb als auch außerhalb des Fahrzeugs auszutauschen. Auf diese Weise können Daten zwischen dem Fahrzeug und den daran angeschlossenen persönlichen Geräten ausgetauscht werden, was beispielsweise die Spiegelung mobiler Anwendungen auf die im Armaturenbrett des Fahrzeugs integrierte Informations- und Unterhaltungseinheit ermöglicht. Auch die Entwicklung eigenständiger, d. h. vom Fahrzeug unabhängiger, mobiler Anwendungen (z. B. durch die alleinige Nutzung des Smartphones) zur Unterstützung des Fahrers fällt in den Geltungsbereich dieser Leitlinien, da diese zu den Konnektivitätskapazitäten des Fahrzeugs beitragen, auch wenn sie möglicherweise nicht tatsächlich auf einer Übertragung von Daten mit dem Fahrzeug per se beruhen. Anwendungen für vernetzte Fahrzeuge sind vielfältig und können Folgendes umfassen[20]:

22. *Mobilitätsmanagement:* Funktionen, die es dem Fahrer ermöglichen, ein Ziel schnell und kosteneffizient zu erreichen, indem sie rechtzeitig Informationen über die GPS-Navigation, potenziell gefährliche Umgebungsbedingungen (z. B. vereiste Straßen), Verkehrsstaus oder Straßenbauarbeiten, Unterstützung bei der Parkplatz- oder Werkstattsuche oder zur Optimierung des Kraftstoffverbrauchs oder der Straßenbenutzungsgebühren bereitstellen.

23. *Fahrzeugmanagement:* Funktionen, die dem Fahrer helfen sollen, die Betriebskosten zu senken und den Bedienkomfort zu verbessern, wie beispielsweise Benachrichtigungen über den Fahrzeugzustand und Erinnerungen an fällige Servicearbeiten, Übertragung von Nutzungsdaten (z. B. für Fahrzeugreparaturdienste), maßgeschneiderte nutzungsabhängige Versicherungen, ferngesteuerte Bedienungen (z. B. der Heizungsanlage) oder Konfiguration einzelner Profile (z. B. der Sitzposition).

24. *Verkehrssicherheit:* Funktionen, die den Fahrer vor externen Gefahren und internen Reaktionen warnen, wie beispielsweise Kollisionsschutz, Warnungen vor Gefahren, Spurhaltewarnungen, Erkennung von Müdigkeit des Fahrers, Notruf (eCall-System) oder Fahrtenschreiber zur Unfalluntersuchung (Unfalldatenspeicher).

25. *Unterhaltung:* Funktionen zur Information und Unterhaltung des Fahrers und der Insassen wie beispielsweise Smartphone-Schnittstellen (Freisprechanlage, sprachgenerierte Textnachrichten), WLAN-Hotspots, Musik, Video, Internet, soziale Medien, mobiles Büro oder intelligente Haustechnik.

26. *Fahrerassistenz:* Funktionen des teil- oder vollautomatisierten Fahrens wie Betriebsassistenz oder Autopilot bei dichtem Verkehr, beim Einparken oder auf Autobahnen.

[20] PwC Strategy 2014. „In the fast lane. The bright future of connected cars.“ (Auf der Überholspur. Die glänzende Zukunft vernetzter Personenkraftwagen.): https://carrealtime.com/wp-content/uploads/2016/11/Strategyand_In-the-Fast-Lane-1.pdf

27. *Wohlbefinden:* Funktionen, die den Komfort, die Fähigkeit und die Fahrtauglichkeit des Fahrers überwachen, wie beispielsweise Müdigkeitserkennung oder medizinische Hilfe.

28. Somit können Fahrzeuge auf natürliche Weise verbunden sein oder nicht, und personenbezogene Daten können auf verschiedene Weise erhoben werden, unter anderem mithilfe von: i) Fahrzeugsensoren, ii) Telematikboxen oder iii) mobilen Anwendungen (z. B. Zugriff von einem Gerät des Fahrers). Um in den Geltungsbereich der vorliegenden Leitlinien zu fallen, müssen mobile Anwendungen mit der Fahrumgebung im Zusammenhang stehen. So fallen beispielsweise GPS-Navigationsanwendungen in den Geltungsbereich. Anwendungen, deren Funktionalitäten dem Fahrer lediglich Orte von Interesse (Restaurants, historische Stätten usw.) vorschlagen, fallen hingegen nicht in den Geltungsbereich dieser Richtlinien.

29. Viele der Daten, die von einem vernetzten Fahrzeug erzeugt werden, beziehen sich auf eine natürliche Person, die identifiziert oder identifizierbar ist, und stellen somit personenbezogene Daten dar. Zu den Daten gehören beispielsweise direkt identifizierbare Daten (z. B. die vollständige Identität des Fahrers) sowie indirekt identifizierbare Daten wie die Detailangaben der zurückgelegten Fahrten, die Fahrzeugnutzungsdaten (z. B. Daten über den Fahrstil oder die zurückgelegte Strecke) oder die technischen Daten des Fahrzeugs (etwa zum Verschleiß von Fahrzeugteilen), die anhand von Querverweisen zu anderen Dateien und insbesondere anhand der Fahrzeug-Identifizierungsnummer (VIN) einer natürlichen Person zugeordnet werden können. Personenbezogene Daten in vernetzten Fahrzeugen können auch Metadaten wie beispielsweise den Wartungsstatus des Fahrzeugs enthalten. Mit anderen Worten fallen daher alle Daten, die einer natürlichen Person zugeordnet werden können, in den Geltungsbereich der vorliegenden Leitlinien.

30. Das Ökosystem des vernetzten Fahrzeugs umfasst ein breites Spektrum von Interessenträgern. Konkret umfasst dieses Ökosystem traditionelle Akteure der Automobilindustrie sowie aufstrebende Akteure der digitalen Industrie. Daher richten sich die vorliegenden Leitlinien an Fahrzeughersteller, Fahrzeugausrüstungshersteller und Automobilzulieferer, Reparaturwerkstätten, Autohäuser, Fahrzeugdienstleister, Flottenmanager, Kfz-Versicherungsgesellschaften, Unterhaltungsanbieter, Telekommunikationsbetreiber, Straßeninfrastrukturbetreiber und Behörden sowie betroffene Personen. Der EDSA unterstreicht, dass sich die Arten der betroffenen Personen von Dienst zu Dienst unterscheiden (z. B. Fahrer, Fahrzeughalter, Insassen usw.). Hierbei handelt es sich um eine nichterschöpfende Liste, da das Ökosystem eine breite Palette von Diensten umfasst, darunter Dienste, für die eine direkte Authentifizierung oder Identifizierung erforderlich ist, und Dienste, für die dies nicht erforderlich ist.

31. Einige Datenverarbeitungen, die von natürlichen Personen innerhalb des Fahrzeugs durchgeführt werden, fallen unter die *„Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“* und somit nicht in den Geltungsbereich der DSGVO[21]. Dies betrifft insbesondere die Nutzung personenbezogener Daten in den Fahrzeugen durch die alleinigen betroffenen Personen, die diese Daten in das Armaturenbrett des Fahrzeugs eingegeben haben. Der EDSA erinnert jedoch daran, dass die DSGVO gemäß Erwägungsgrund 18 *„für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung*

[21] Siehe DSGVO Artikel 2 Absatz 2 Buchstabe c.

*personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen"* gilt.

### 1.3.1 Außerhalb des Geltungsbereichs dieser Leitlinien

32. Arbeitgeber, die ihren Mitarbeitern Firmenwagen zur Verfügung stellen, möchten möglicherweise die Tätigkeiten ihrer Mitarbeiter überwachen (z. B. um die Sicherheit des Mitarbeiters, der Waren oder der Fahrzeuge zu gewährleisten, Ressourcen zuzuordnen, eine Dienstleistung zu verfolgen und abzurechnen oder die Arbeitszeit zu kontrollieren). Die von Arbeitgebern in diesem Zusammenhang durchgeführte Datenverarbeitung wirft besondere Fragen zum Beschäftigungskontext auf, die möglicherweise auf nationaler Ebene durch Arbeitsgesetze geregelt werden, die in den vorliegenden Leitlinien nicht im Einzelnen aufgeführt werden können.[22]

33. Wenngleich die Datenverarbeitung im Zusammenhang mit gewerblich genutzten Fahrzeugen (z. B. öffentlichen Verkehrsmitteln) und gemeinsam genutzten Transportmitteln sowie „Mobility-as-a-Service"-Lösungen (MaaS-Lösungen) möglicherweise Anlass zu besonderen Erwägungen gibt, die nicht in den Geltungsbereich dieser allgemeinen Leitlinien fallen, sind viele der hier dargelegten Grundsätze und Empfehlungen auch auf diese Arten der Verarbeitung anwendbar.

34. Da es sich bei vernetzten Fahrzeugen um funkfähige Systeme handelt, unterliegen sie einer passiven Verfolgung wie beispielsweise über Wi-Fi oder Bluetooth. In diesem Sinne unterscheiden sie sich nicht von anderen vernetzten Geräten und fallen in den Geltungsbereich der Datenschutzrichtlinie für elektronische Kommunikation, die gegenwärtig überarbeitet wird. Ausgeschlossen ist somit auch die großflächige Verfolgung von mit Wi-Fi ausgestatteten Fahrzeugen[23] durch ein dichtes Netz von Umstehenden, die gängige Smartphone-Ortungsdienste nutzen. Diese melden routinemäßig alle erkennbaren Wi-Fi-Netzwerke an zentrale Server. Da eingebautes Wi-Fi als sekundäre Fahrzeugkennung betrachtet werden kann[24], besteht die Gefahr einer systematischen fortlaufenden Erhebung vollständiger Fahrzeugbewegungsprofile.

35. Fahrzeuge sind zunehmend mit Bildaufzeichnungsgeräten (z. B. mit Parkkamerasystemen oder Dashcams) ausgestattet. Da es hier um die Frage des Filmens öffentlicher Orte geht, die eine Bewertung des einschlägigen Rechtsrahmens erfordert, der von Mitgliedstaat zu Mitgliedstaat unterschiedlich ist, fällt diese Datenverarbeitung nicht in den Geltungsbereich der vorliegenden Leitlinien.

---

[22] Die Artikel-29-Datenschutzgruppe hat dies in ihrer Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz (WP249) näher ausgeführt; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

[23] Weitere Einzelheiten unter: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html

[24] Markus Ullmann, Tobias Franz und Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proceedings (Fahrzeugerkennung auf der Grundlage von sekundärer Fahrzeugkennung – Analyse und Messungen im Handlungsverlauf), VEHICULAR 2017, Sechste Internationale Konferenz zum Thema Fortschritte bei Fahrzeugsystemen, -technologien und -anwendungen, Nizza, Frankreich, 23. bis 27. Juli 2017, S. 32-37.

36. Die Verarbeitung von Daten, die kooperative intelligente Verkehrssysteme (C-ITS) ermöglichen – wie in der Richtlinie 2010/40/EU[25] definiert –, wurde in einer besonderen Stellungnahme der Artikel-29-Datenschutzgruppe behandelt.[26] Während die Bestimmung des Begriffs „C-ITS“ in der Richtlinie keine technischen Spezifikationen enthält, konzentriert sich die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme auf die Kommunikation über kurze Entfernungen, d. h. auf Kommunikation, die keine Intervention eines Netzbetreibers erfordert. Insbesondere liefert sie eine Analyse für bestimmte Anwendungsfälle, die für eine Ersteinführung der C-ITS erstellt wurden, und verpflichtet sich, zu einem späteren Zeitpunkt die neuen Fragen zu bewerten, die sich zweifellos stellen werden, wenn ein höherer Automatisierungsgrad eingeführt wird. Da die datenschutzrechtlichen Auswirkungen im Zusammenhang mit C-ITS sehr spezifisch sind (beispiellose Mengen an Standortdaten, kontinuierliche Übertragung personenbezogener Daten, Datenaustausch zwischen Fahrzeugen und anderen Straßeninfrastruktureinrichtungen usw.) und auf europäischer Ebene noch erörtert werden, fällt die Verarbeitung personenbezogener Daten in diesem Zusammenhang nicht in den Geltungsbereich der vorliegenden Leitlinien.

37. Und schließlich sollen die vorliegenden Leitlinien nicht alle denkbaren Fragen und Probleme lösen, die durch vernetzte Fahrzeuge aufgeworfen werden können, und kann daher nicht als erschöpfend angesehen werden.

## 1.4 Begriffsbestimmungen

38. Die **Verarbeitung** personenbezogener Daten umfasst alle Vorgänge, die personenbezogene Daten betreffen, wie beispielsweise das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Abrufen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, die Verbreitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung sowie die Einschränkung, das Löschen oder das Vernichten der Daten.[27]

39. Als **betroffene Person** gilt eine natürliche Person, auf die sich die von der Verarbeitung betroffenen Daten beziehen. Im Zusammenhang mit vernetzten Fahrzeugen kann dies insbesondere der Fahrer (Haupt- oder Gelegenheitsfahrer), ein Insasse oder der Halter des Fahrzeugs sein.[28]

40. Der **Verantwortliche** ist die Person, die über den Zweck und die Mittel der Verarbeitung, die in vernetzten Fahrzeugen stattfindet, entscheidet.[29] Zu den Verantwortlichen können

[25] Richtlinie 2010/40/EU vom 7. Juli 2020 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32010L0040

[26] Artikel-29-Datenschutzgruppe – Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

[27] Siehe DSGVO Artikel 4 Nummer 2.

[28] Siehe DSGVO Artikel 4 Nummer 1.

[29] Siehe DSGVO Artikel 4 Nummer 7 und Europäischer Datenschutzausschuss, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und Auftragsverarbeiters in der DSGVO) (im Folgenden „Leitlinien 07/2020“).

Dienstleister gehören, die Fahrzeugdaten verarbeiten, um dem Fahrer Verkehrsinformationen, Informationen über umweltbewusstes Fahren oder Warnmeldungen zu den Funktionen des Fahrzeugs zu senden, Versicherungsgesellschaften, die nutzungsabhängige Verträge („*Pay As You Drive*“) anbieten, oder Fahrzeughersteller, die Daten über den Verschleiß von Fahrzeugteilen erheben, um die Fahrzeugqualität zu verbessern. Gemäß Artikel 26 DSGVO können zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen und somit als gemeinsam Verantwortliche betrachtet werden. In diesem Fall müssen sie ihre jeweiligen Verpflichtungen eindeutig festlegen, insbesondere in Bezug auf die Wahrnehmung der Rechte der betroffenen Personen und die Informationspflichten gemäß den Artikeln 13 und 14 DSGVO.

41. Als **Auftragsverarbeiter** gilt jede Person, die personenbezogene Daten für den und im Auftrag des Verantwortlichen verarbeitet.[30] Der Auftragsverarbeiter erhebt und verarbeitet Daten auf Anweisung des Verantwortlichen, ohne die Daten für eigene Zwecke zu nutzen. Beispielsweise können in vielen Fällen Fahrzeugausrüstungshersteller und Automobilzulieferer Daten im Auftrag von Fahrzeugherstellern verarbeiten (was nicht bedeutet, dass sie nicht auch für andere Zwecke ein Verantwortlicher sein können). Neben der Verpflichtung der Auftragsverarbeiter, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein an das Risiko angepasstes Sicherheitsniveau zu gewährleisten, legt Artikel 28 DSGVO die Pflichten des Auftragsverarbeiters fest.

42. Der **Empfänger** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.[31] Beispielsweise ist ein Geschäftspartner des Dienstleisters, der vom Dienstleister personenbezogene Daten erhält, die vom Fahrzeug erzeugt wurden, ein Empfänger personenbezogener Daten. Unabhängig davon, ob er als neuer Verantwortlicher oder als Auftragsverarbeiter agiert, muss er alle von der DSGVO auferlegten Pflichten erfüllen.

43. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger[32]; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung. Beispielsweise sind Strafverfolgungsbehörden berechtigte Dritte, wenn sie im Rahmen einer Ermittlung gemäß dem Recht der Europäischen Union oder der Mitgliedstaaten personenbezogene Daten anfordern.

[30] Siehe DSGVO Artikel 4 Nummer 8 und Leitlinien 07/2020.
[31] Siehe DSGVO Artikel 4 Nummer 9 und Leitlinien 07/2020.
[32] DSGVO Artikel 4 Nummer 9 und Erwägungsgrund 31.

## 1.5 Risiken in Bezug auf Privatsphäre und Datenschutz

44. Die Artikel-29-Datenschutzgruppe hat bereits mehrere Bedenken im Hinblick auf Systeme des Internets der Dinge geäußert, die auch auf vernetzte Fahrzeuge zutreffen können.[33] Die bereits im Zusammenhang mit dem Internet der Dinge hervorgehobenen Fragen der Datensicherheit und -kontrolle sind bei vernetzten Fahrzeugen sogar noch heikler, da sie Bedenken hinsichtlich der Sicherheit im Straßenverkehr mit sich bringen – und die körperliche Unversehrtheit des Fahrers beeinträchtigen können – in einer Umgebung, die traditionell als isoliert und als vor externen Störungen geschützt wahrgenommen wird.

45. Darüber hinaus werfen vernetzte Fahrzeuge erhebliche Bedenken hinsichtlich Datenschutz und Privatsphäre in Bezug auf die Verarbeitung von Standortdaten auf, da diese zunehmend stark in Datenschutz bzw. Privatsphäre eingreift und die derzeitig bestehenden Möglichkeiten, die Anonymität zu wahren, beeinträchtigen kann. Der EDSA möchte besonders betonen und das Bewusstsein der Beteiligten dafür schärfen, dass der Einsatz von Ortungstechnologien besondere Vorkehrungen erfordert, um die Überwachung von Personen und den Missbrauch der Daten zu verhindern.

### 1.5.1 Mangelnde Kontrolle und Informationsasymmetrie

46. Die Fahrer und Insassen eines Fahrzeugs werden möglicherweise nicht immer ausreichend über die Verarbeitung von Daten informiert, die in einem vernetzten Fahrzeug stattfindet oder durch ein vernetztes Fahrzeug verursacht wird. Es kann sein, dass die Informationen nur an den Fahrzeughalter weitergegeben werden, der möglicherweise nicht der Fahrer ist, und es kann auch sein, dass sie nicht rechtzeitig zur Verfügung gestellt werden. Somit besteht das Risiko, dass nicht genügend Funktionalitäten oder Optionen angeboten werden, um die Kontrolle auszuüben, die erforderlich ist, damit die betroffenen Personen von ihren Rechten in Bezug auf Datenschutz und Privatsphäre Gebrauch machen können. Dieser Aspekt ist von Bedeutung, da Fahrzeuge während ihrer Nutzungsdauer mehr als einem Fahrzeughalter gehören können, entweder, weil sie verkauft werden, oder weil sie nicht gekauft, sondern geleast werden.

47. Zudem können Kommunikationsvorgänge im Fahrzeug sowohl automatisch als auch standardmäßig ausgelöst werden, ohne dass die Person davon Kenntnis hat. Da es keine Möglichkeit gibt, die Interaktion zwischen dem Fahrzeug und der vernetzten Ausrüstung wirksam zu steuern, wird es zwangsläufig für den Nutzer außerordentlich schwierig, den Datenfluss zu kontrollieren. Noch schwieriger wird es sein, die spätere Verwendung zu kontrollieren und damit eine mögliche schleichende Ausweitung der Funktionen zu verhindern.

### 1.5.2 Qualität der Einwilligung des Nutzers

48. Der EDSA unterstreicht, dass alle Kriterien einer gültigen Einwilligung erfüllt sein müssen, wenn die Datenverarbeitung auf einer Einwilligung beruht; die Einwilligung muss also eine freiwillig für den bestimmten Fall und in informierter Weise abgegebene Willensbekundung

[33] Artikel-29-Datenschutzgruppe – Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_de.pdf

der betroffenen Person sein, wie in den Leitlinien zur Einwilligung des EDSA ausgelegt wird.[34] Die Verantwortlichen müssen sorgfältig auf die Art und Weise achten, auf die sie eine gültige Einwilligung von den verschiedenen Teilnehmern, wie z. B. Fahrzeughaltern oder Fahrzeugnutzern, erhalten. Eine solche Einwilligung muss jeweils gesondert für bestimmte Zwecke erteilt werden und darf nicht mit dem Kauf- oder Leasingvertrag eines neuen Kraftfahrzeugs gebündelt werden. Die Einwilligung muss ebenso leicht widerrufen werden können, wie sie erteilt wird.

49. Gleiches gilt, wenn eine Einwilligung erforderlich ist, um die Datenschutzrichtlinie für elektronische Kommunikation einzuhalten, beispielsweise wenn es um die Speicherung von Informationen oder den Zugriff auf bereits im Fahrzeug gespeicherte Informationen geht, wie es in bestimmten Fällen gemäß Artikel 5 Absatz 3 der ePrivacy-RL gefordert wird. Wie vorstehend dargelegt, muss die Einwilligung in diesem Zusammenhang gemäß DSGVO ausgelegt werden.

50. In vielen Fällen ist dem Nutzer die in seinem Fahrzeug durchgeführte Datenverarbeitung möglicherweise nicht bekannt. Ein solcher Mangel an Informationen stellt ein erhebliches Hindernis für den Nachweis einer gültigen Einwilligung gemäß DSGVO dar, da die Einwilligung in informierter Weise erfolgen muss. Unter diesen Umständen kann die Einwilligung nicht als Rechtsgrundlage für die entsprechende Datenverarbeitung gemäß DSGVO herangezogen werden.

51. Klassische Mechanismen, mit denen die Einwilligung von Personen eingeholt wird, können im Zusammenhang mit vernetzten Fahrzeugen schwierig anzuwenden sein, was zu einer Einwilligung von „geringer Qualität“ aufgrund unzureichender Informationen oder zu einer faktischen Unmöglichkeit führt, eine genau abgestimmte Einwilligung gemäß den von Einzelpersonen geäußerten Präferenzen vorzulegen. In der Praxis könnte es auch schwierig sein, eine Einwilligung von Fahrern und Fahrzeuginsassen zu erhalten, die in keiner Beziehung zu dem Fahrzeughalter stehen, beispielsweise wenn es sich um gebraucht gekaufte, geleaste, gemietete oder geliehene Fahrzeuge handelt.

52. Wenn die Datenschutzrichtlinie für elektronische Kommunikation keine Einwilligung der betroffenen Person erfordert, liegt es dennoch in der Verantwortung des Verantwortlichen, die Rechtsgrundlage gemäß Artikel 6 DSGVO zu wählen, die für die Verarbeitung personenbezogener Daten am besten geeignet ist.

### 1.5.3 Weiterverarbeitung personenbezogener Daten

53. Wenn Daten auf der Grundlage einer Einwilligung gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation oder aufgrund einer der Ausnahmen nach Artikel 5 Absatz 3 erhoben und anschließend gemäß Artikel 6 DSGVO verarbeitet werden, dürfen sie nur dann weiterverarbeitet werden, wenn der Verantwortliche entweder eine zusätzliche Einwilligung zu diesem anderen Zweck einholt oder nachweisen kann, dass die Weiterverarbeitung auf einer Rechtsvorschrift der Union

[34] Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1 vom 4. Mai 2020 (im Folgenden „Leitlinien 05/2020“).

oder eines Mitgliedstaats beruht, um die in Artikel 23 Absatz 1 DSGVO genannten Ziele zu wahren.[35] Der EDSA ist der Ansicht, dass eine Weiterverarbeitung auf der Grundlage einer Vereinbarkeitsprüfung nach Artikel 6 Absatz 4 DSGVO in solchen Fällen nicht möglich ist, da sie den Datenschutzstandard der ePrivacy-RL untergraben würde. Tatsächlich muss die Einwilligung, soweit sie nach der Datenschutzrichtlinie für elektronische Kommunikation erforderlich ist, für den bestimmten Fall und in informierter Weise erfolgen, d. h. die betroffenen Personen müssen über jeden Zweck der Datenverarbeitung informiert sein und das Recht haben, bestimmte Zwecke zu verweigern.[36] In Anbetracht der Tatsache, dass die Weiterverarbeitung auf der Grundlage einer Vereinbarkeitsprüfung gemäß Artikel 6 Absatz 4 DSGVO möglich ist, würde somit der in der aktuellen Richtlinie dargelegte eigentliche Grundsatz der Einwilligungsverpflichtung umgangen werden.

54. Der EDSA erinnert daran, dass die ursprüngliche Einwilligung niemals eine weitere Verarbeitung legitimiert, da die Einwilligung für den bestimmten Fall und in informierter Weise erfolgen muss, um gültig zu sein.

55. So dürfen beispielsweise Telemetriedaten, die während der Nutzung des Fahrzeugs zu Wartungszwecken erhoben werden, nicht ohne Einwilligung des Nutzers an Kfz-Versicherungsgesellschaften weitergegeben werden, um Fahrerprofile zu erstellen, die für das Angebot fahrverhaltensabhängiger Versicherungspolicen genutzt werden.

56. Darüber hinaus können von vernetzten Fahrzeugen erhobene Daten von Strafverfolgungsbehörden verarbeitet werden, um Geschwindigkeitsüberschreitungen oder andere Verstöße festzustellen, wenn die spezifischen Bedingungen der Strafverfolgungsrichtlinie erfüllt sind. In diesem Fall wird davon ausgegangen, dass sich diese Daten auf strafrechtliche Verurteilungen und Straftaten gemäß den in Artikel 10 DSGVO festgelegten Bedingungen und den geltenden nationalen Rechtsvorschriften beziehen. Die Hersteller können den Strafverfolgungsbehörden solche Daten zur Verfügung stellen, wenn die spezifischen Bedingungen für eine solche Verarbeitung erfüllt sind. Der EDSA weist darauf hin, dass die Verarbeitung personenbezogener Daten zum alleinigen Zweck der Erfüllung von Anfragen der Strafverfolgungsbehörden keinen festgelegten, eindeutigen und legitimen Zweck im Sinne des Artikels 5 Absatz 1 Buchstabe b DSGVO darstellt. Wenn Strafverfolgungsbehörden von Rechts wegen befugt sind, könnten sie Dritte im Sinne des Artikels 4 Nummer 10 DSGVO sein; in diesem Fall wären die Hersteller berechtigt, ihnen alle zur Verfügung stehenden Daten zu übermitteln, sofern die einschlägigen rechtlichen Rahmenbedingungen in jedem Mitgliedstaat eingehalten werden.

### 1.5.4 Übermäßige Erhebung von Daten

57. Mit der ständig zunehmenden Anzahl von Sensoren, die in vernetzten Fahrzeugen eingesetzt werden, besteht ein sehr hohes Risiko einer übermäßigen Erhebung von Daten im Vergleich zu dem, was zur Erreichung des Zwecks erforderlich ist.

[35] Siehe auch Europäischer Datenschutzausschuss, Leitlinien 10/2020 zu Beschränkungen gemäß Artikel 23 DSGVO.

[36] Leitlinien 05/2020, Abschnitte 3.2 und 3.3.

58. Die Entwicklung neuer Funktionalitäten und insbesondere solcher, die auf Algorithmen für maschinelles Lernen basieren, kann eine große Datenmenge erfordern, die über einen langen Zeitraum erhoben wird.

#### 1.5.5 Sicherheit personenbezogener Daten

59. Aufgrund der vielfältigen Funktionalitäten, Dienste und Schnittstellen (z. B. Internet, USB, RFID, Wi-Fi) vernetzter Fahrzeuge weisen diese eine große Angriffsfläche und dementsprechend auch viele potenzielle Schwachstellen auf, durch die personenbezogenen Daten gefährdet werden könnten. Im Gegensatz zu den meisten Geräten des Internets der Dinge sind vernetzte Fahrzeuge kritische Systeme, bei denen eine Sicherheitsverletzung das Leben der Nutzer und der Menschen in ihrer Umgebung gefährden kann. Umso wichtiger ist es, dem Risiko von Hackern entgegenzuwirken, die versuchen, die Schwachstellen vernetzter Fahrzeuge auszunutzen.

60. Darüber hinaus müssen personenbezogene Daten, die in Fahrzeugen und/oder an externen Orten (z. B. in der Cloud-Computing-Infrastruktur) gespeichert sind, angemessen vor unbefugtem Zugriff geschützt werden. Beispielsweise muss ein Fahrzeug zur Wartung an einen Techniker übergeben werden, der Zugriff auf einige technische Daten des Fahrzeugs benötigt. Obgleich der Techniker Zugriff auf die technischen Daten haben muss, besteht auch die Möglichkeit, dass er versucht, auf alle im Fahrzeug gespeicherten Daten zuzugreifen.

# 2 ALLGEMEINE EMPFEHLUNGEN

61. Um die vorstehend genannten Risiken für die betroffenen Personen zu mindern, sollten die folgenden allgemeinen Empfehlungen von Fahrzeug- und Ausrüstungsherstellern, Dienstleistern oder anderen Interessenträgern befolgt werden, die in Bezug auf vernetzte Fahrzeuge als Verantwortliche oder Auftragsverarbeiter fungieren können.

## 2.1 Datenkategorien

62. Wie in der Einleitung erwähnt, werden die meisten Daten im Zusammenhang mit vernetzten Fahrzeugen als personenbezogene Daten betrachtet, sofern es möglich ist, sie mit einer oder mehreren identifizierbaren Personen zu verknüpfen. Dazu gehören technische Daten über die Bewegungen des Fahrzeugs (z. B. Geschwindigkeit, zurückgelegte Strecke) sowie über den Fahrzeugzustand (z. B. Temperatur des Motorkühlmittels, Motordrehzahl, Reifendruck). Bestimmten Daten, die von vernetzten Fahrzeugen erzeugt werden, sollte aufgrund ihrer Sensibilität und/oder potenziellen Auswirkungen auf die Rechte und Interessen der betroffenen Personen ebenfalls besondere Aufmerksamkeit gewidmet werden. Gegenwärtig hat der EDSA drei Arten personenbezogener Daten ermittelt, denen Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstig Verantwortliche besondere Beachtung schenken sollten: Standortdaten, biometrische Daten (und alle besonderen Datenkategorien gemäß Artikel 9 DSGVO) sowie Daten, die Straftaten oder Verkehrsvergehen aufdecken könnten.

### 2.1.1 Standortdaten

63. Bei der Erhebung personenbezogener Daten sollten Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstige Verantwortliche berücksichtigen, dass Standortdaten besonders viel Aufschluss über die Lebensgewohnheiten der betroffenen Personen geben. Die durchgeführten Fahrten sind insofern sehr charakteristisch, als sie Rückschlüsse auf den

Arbeits- und Wohnort sowie auf die Interessenschwerpunkte (Freizeit) des Fahrers zulassen und möglicherweise auf sensible Informationen wie die Religion (über den Ort der Religionsausübung) oder die sexuelle Orientierung (aufgrund der besuchten Orte) schließen lassen. Dementsprechend sollten Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstige Verantwortliche besonders darauf achten, keine Standortdaten zu erheben, außer wenn dies für den Zweck der Verarbeitung unbedingt erforderlich ist. Wenn die Verarbeitung beispielsweise darin besteht, die Bewegung des Fahrzeugs zu erfassen, reicht das Gyroskop aus, um diese Funktion zu erfüllen, ohne dass Standortdaten erhoben werden müssten.

64. Im Allgemeinen unterliegt die Erhebung von Standortdaten auch der Einhaltung folgender Grundsätze:

- angemessene Konfiguration der Zugriffshäufigkeit auf Standortdaten und des Detaillierungsgrads der erhobenen Standortdaten in Bezug auf den Verarbeitungszweck. Beispielsweise sollte eine Wetteranwendung auch mit Einwilligung der betroffenen Person nicht jede Sekunde auf den Standort des Fahrzeugs zugreifen können;
- Bereitstellung genauer Informationen über den Zweck der Verarbeitung (z. B.: Wird der Standortverlauf gespeichert? Wenn ja, zu welchem Zweck?);
- Einholung einer gültigen (freiwillig für den bestimmten Fall und in informierter Weise erteilten) Einwilligung, die sich von den allgemeinen Verkaufs- oder Nutzungsbedingungen unterscheidet, z. B. im Bordcomputer, sofern die Verarbeitung auf einer Einwilligung beruht;
- Aktivierung des Standorts nur dann, wenn der Nutzer eine Funktion betätigt, die eine Kenntnis des Standorts erfordert, und nicht standardmäßig und kontinuierlich, wenn das Fahrzeug angelassen wird;
- Information des Nutzers über die Aktivierung des Standorts, insbesondere durch Verwendung von Symbolen (z. B. eines Pfeils, der sich über den Bildschirm bewegt);
- Möglichkeit, den Standort jederzeit zu deaktivieren;
- Festlegung einer begrenzten Speicherdauer.

### 2.1.2 Biometrische Daten

65. Im Zusammenhang mit vernetzten Fahrzeugen können biometrische Daten, die zum Zweck der eindeutigen Identifizierung einer natürlichen Person verwendet werden, im Rahmen des Artikels 9 DSGVO und der nationalen Ausnahmen verarbeitet werden, um unter anderem den Zugang zu einem Fahrzeug zu ermöglichen, den Fahrer/Fahrzeughalter zu authentifizieren und/oder den Zugriff auf die Profileinstellungen und Präferenzen eines Fahrers zu ermöglichen. Wenn die Verwendung biometrischer Daten in Betracht gezogen wird, bedeutet die Gewährleistung der vollständigen Kontrolle der betroffenen Person über ihre Daten zum einen, dass eine nichtbiometrische Alternative (z. B. die Verwendung eines physischen Schlüssels oder eines Codes) ohne zusätzliche Einschränkungen möglich ist (d. h., die Verwendung biometrischer Daten sollte nicht zwingend vorgeschrieben sein), und zum anderen, dass die biometrische Vorlage in verschlüsselter Form nur lokal gespeichert und verglichen wird, wobei die biometrischen Daten nicht von einem externen Lese-/Vergleichsterminal verarbeitet werden.

66. Bei biometrischen Daten[37] muss sichergestellt werden, dass die biometrische Authentifizierungslösung hinreichend zuverlässig ist, indem insbesondere die folgenden Grundsätze beachtet werden:

- die Einstellung der eingesetzten biometrischen Lösung (z. B. die Rate der falsch positiven und falsch negativen Meldungen) ist an das Sicherheitsniveau der erforderlichen Zugangskontrolle angepasst;
- die eingesetzte biometrische Lösung basiert auf einem Sensor, der gegen Angriffe resistent ist (z. B. die Verwendung eines Flachabdrucks für die Fingerabdruckerkennung);
- die Anzahl der Authentifizierungsversuche ist begrenzt;
- die biometrische Vorlage/das biometrische Modell wird in verschlüsselter Form unter Verwendung eines kryptografischen Algorithmus und einer Schlüsselverwaltung, die dem Stand der Technik entsprechen, im Fahrzeug gespeichert;
- die zur Erstellung der biometrischen Vorlage und zur Nutzerauthentifizierung verwendeten Rohdaten werden in Echtzeit verarbeitet, ohne dass sie jemals, auch nicht lokal, gespeichert werden.

### 2.1.3 Daten zur Aufdeckung von Straftaten und sonstigen Verstößen

67. Für die Verarbeitung von Daten, die sich auf mögliche Straftaten im Sinne des Artikels 10 DSGVO beziehen, empfiehlt der EDSA, auf eine lokale Verarbeitung der Daten zurückzugreifen, bei der die betroffene Person die volle Kontrolle über die in Rede stehende Verarbeitung hat (siehe Erörterung der lokalen Verarbeitung in Abschnitt 2.4). Tatsächlich ist – von einigen Ausnahmen abgesehen (siehe die nachstehend in Abschnitt 3.3 dargestellte Fallstudie zur Unfallforschung) – die externe Verarbeitung von Daten, die Straftaten oder andere Verstöße aufdecken, untersagt. Entsprechend der Sensibilität der Daten müssen daher strenge Sicherheitsmaßnahmen, wie in Abschnitt 2.7 beschrieben, getroffen werden, um Schutz vor unrechtmäßigem Zugriff sowie unrechtmäßiger Änderung und Löschung dieser Daten zu bieten.

68. Tatsächlich könnten einige Arten personenbezogener Daten aus vernetzten Fahrzeugen Aufschluss darüber geben, ob eine Straftat oder ein sonstiger Verstoß begangen wurde oder wird („strafrechtlich relevante Daten“), und daher besonderen Beschränkungen unterliegen (z. B. Daten, die darauf hinweisen, dass das Fahrzeug eine weiße Linie überfahren hat, die aktuelle Geschwindigkeit eines Fahrzeugs in Kombination mit genauen Standortdaten). Insbesondere für den Fall, dass diese Daten von den zuständigen nationalen Behörden zum Zwecke der strafrechtlichen Ermittlung und Verfolgung von Straftaten verarbeitet werden, gelten die in Artikel 10 DSGVO vorgesehenen Garantien.

## 2.2 Zwecke

69. Personenbezogene Daten können für eine Vielzahl von Zwecken im Zusammenhang mit vernetzten Fahrzeugen verarbeitet werden, darunter Fahrersicherheit, Versicherung, effizienter Verkehr, Unterhaltungs- oder Informationsdienste. Im Einklang mit der DSGVO müssen die Verantwortlichen sicherstellen, dass ihre Zwecke „festgelegt, eindeutig und

[37] Der Verbotsgrundsatz nach Artikel 9 Absatz 1 DSGVO bezieht sich nur auf *„biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person“*.

legitim“ sind, dass die Daten nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist, und dass es eine gültige Rechtsgrundlage gemäß Artikel 5 DSGVO für die Verarbeitung gibt. Einige konkrete Beispiele für Zwecke, die von Verantwortlichen im Zusammenhang mit vernetzten Fahrzeugen verfolgt werden können, werden in Teil III dieser Leitlinien, in Verbindung mit spezifischen Empfehlungen für jede Art der Verarbeitung, erörtert.

## 2.3 Bedeutung und Datenminimierung

70. Um den Grundsatz der Datenminimierung[38] einzuhalten, sollten Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstige Verantwortliche besonders darauf achten, welche Datenkategorien sie von einem vernetzten Fahrzeug benötigen, da sie nur personenbezogene Daten erheben dürfen, die für die Verarbeitung angemessen und notwendig sind. So greifen beispielsweise Standortdaten besonders stark in die Privatsphäre ein und können Aufschluss über viele Lebensgewohnheiten der betroffenen Personen geben. Dementsprechend sollten die Branchenbeteiligten besonders darauf achten, keine Standortdaten zu erheben, außer wenn dies für den Zweck der Verarbeitung unbedingt erforderlich ist (siehe Erörterung zu Standortdaten vorstehend in Abschnitt 2.1).

## 2.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

71. In Anbetracht des Umfangs und der Vielfalt der von vernetzten Fahrzeugen erzeugten personenbezogenen Daten stellt der EDSA fest, dass die Verantwortlichen sicherstellen müssen, dass die - im Zusammenhang mit vernetzten Fahrzeugen - eingesetzten Technologien so konfiguriert sind, dass die Privatsphäre des Einzelnen gewahrt bleibt, indem sie die Verpflichtungen zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Artikel 25 DSGVO einhalten. Technologien sollten so gestaltet sein, dass sie die Erhebung personenbezogener Daten minimieren, mit dem Schutz der Privatsphäre konforme Standardeinstellungen bieten und sicherstellen, dass die betroffenen Personen gut informiert sind und die Möglichkeit haben, Konfigurationen, die mit ihren personenbezogenen Daten verbunden sind, leicht zu ändern. Spezifische Anleitungen zu der Art und Weise, wie Hersteller und Dienstleister den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen einhalten können, könnten für die Branche und für Drittanbieter von Anwendungen von Vorteil sein.

72. Bestimmte allgemeine Praktiken, die im Folgenden beschrieben werden, können ebenfalls dazu beitragen, die mit vernetzten Fahrzeugen verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu mindern.[39]

### 2.4.1 Lokale Verarbeitung personenbezogener Daten

73. Im Allgemeinen sollten Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstige Verantwortliche nach Möglichkeit Prozesse verwenden, die weder personenbezogene Daten noch die Übertragung personenbezogener Daten außerhalb des Fahrzeugs beinhalten (d. h. die Daten werden intern verarbeitet). Vernetzte Fahrzeuge bergen jedoch per

[38] DSGVO Artikel 5 Absatz 1 Buchstabe c.

[39] Siehe auch Europäischer Datenschutzausschuss, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020 (im Folgenden „Leitlinien 4/2019“).

definitionem Risiken wie die Möglichkeit von Angriffen auf die lokale Verarbeitung durch externe Akteure oder das Durchsickern lokaler Daten im Zusammenhang mit dem Verkauf von Fahrzeugteilen. Daher sollten entsprechende Aufmerksamkeit und Sicherheitsmaßnahmen berücksichtigt werden, um sicherzustellen, dass die lokale Verarbeitung auch lokal bleibt. Dieses Szenario bietet den Vorteil, dass dem Nutzer die alleinige und vollständige Kontrolle über seine personenbezogenen Daten garantiert wird, und es somit „durch Technikgestaltung" weniger privatsphärebezogene Risiken birgt, insbesondere durch das Verbot jeglicher Datenverarbeitung durch Interessenträger ohne das Wissen der betroffenen Person. Es ermöglicht auch die Verarbeitung sensibler Daten, wie beispielsweise biometrischer Daten oder Daten im Zusammenhang mit Straftaten oder anderen Verstößen, sowie detaillierter Standortdaten, die ansonsten strengeren Regeln unterliegen würden (siehe unten). Außerdem birgt es weniger Cybersicherheitsrisiken und hat eine geringe Latenzzeit, wodurch es sich besonders für automatisierte Fahrerassistenzfunktionen eignet. Einige Beispiele für diese Art von Lösung könnten sein:

- Anwendungen für umweltbewusstes Fahren, die Daten im Fahrzeug verarbeiten, um Hinweise zur umweltbewussten Fahrweise in Echtzeit auf dem Bordbildschirm anzuzeigen;

- Anwendungen, bei denen personenbezogene Daten unter der vollen Kontrolle des Nutzers (z. B. über Bluetooth oder Wi-Fi) an ein Gerät wie ein Smartphone übertragen werden und bei denen die Fahrzeugdaten nicht an die Anbieter der Anwendung oder die Fahrzeughersteller übertragen werden. Dies würde beispielsweise die Kopplung von Smartphones zur Nutzung des Fahrzeugdisplays, der Multimediasysteme, des Mikrofons (oder anderer Sensoren) für Telefongespräche usw. einschließen, sofern die erhobenen Daten unter der Kontrolle der betroffenen Person bleiben und ausschließlich zur Erbringung des von ihr angeforderten Dienstes verwendet werden;

- Anwendungen zur Erhöhung der Fahrzeugsicherheit, z. B. Anwendungen, die akustische Signale oder Vibrationen des Lenkrads auslösen, wenn ein Fahrer ein Fahrzeug ohne Blinksignal überholt oder weiße Linien überfährt, oder die Warnmeldungen über den Fahrzeugzustand liefern (z. B. eine Warnung über den Verschleiß der Bremsbeläge);

- Anwendungen zum Entsperren, Starten und/oder Aktivieren bestimmter Fahrzeugbefehle unter Verwendung der im Fahrzeug gespeicherten biometrischen Daten des Fahrers (z. B. Gesichts- oder Spracherkennungsmodelle oder Minutien des Fingerabdrucks).

74. Bei Anwendungen wie den vorstehend genannten handelt es sich um Verarbeitungen, die zur Ausübung rein persönlicher Tätigkeiten durch eine natürliche Person durchgeführt werden (d. h. ohne die Übertragung personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter). Gemäß Artikel 2 Absatz 2 DSGVO **fallen diese Anwendungen daher nicht in den Geltungsbereich der DSGVO**.

75. Gilt die DSGVO jedoch nicht für die Verarbeitung personenbezogener Daten durch eine natürliche Person im Rahmen einer ausschließlich persönlichen oder familiären Tätigkeit, so gilt sie gemäß Erwägungsgrund 18 DSGVO für Verantwortliche oder Auftragsverarbeiter, die die Mittel zur Verarbeitung personenbezogener Daten für diese persönlichen oder familiären Tätigkeiten bereitstellen (Automobilhersteller, Dienstleister usw.). Wenn sie als Verantwortlicher oder Auftragsverarbeiter agieren, müssen sie daher unter gebührender Berücksichtigung des Grundsatzes des Datenschutzes durch Technikgestaltung und der privatsphärefreundlichen Voreinstellungen eine sichere bordeigene Anwendung

entwickeln. In jedem Fall gilt gemäß Erwägungsgrund 78 DSGVO: *„In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.“*[40] Das wird einerseits die Entwicklung nutzerorientierter Dienste fördern und andererseits jede weitere künftige Nutzung erleichtern und absichern, die in den Geltungsbereich der DSGVO fallen könnte. Insbesondere empfiehlt der EDSA die Entwicklung einer sicheren bordeigenen Anwendungsplattform, die physisch von sicherheitsrelevanten Fahrzeugfunktionen getrennt ist, damit der Zugriff auf Fahrzeugdaten nicht von unnötigen externen Cloud-Funktionen abhängt.

76. Die lokale Datenverarbeitung sollte nach Möglichkeit von Automobilherstellern und Dienstleistern in Betracht gezogen werden, um die potenziellen Risiken der Cloud-Verarbeitung zu mindern, wie die Artikel-29-Datenschutzgruppe in ihrer veröffentlichten Stellungnahme zum Cloud Computing unterstreicht.[41]

77. Im Allgemeinen sollte der Nutzer kontrollieren können, auf welche Weise seine Daten im Fahrzeug erhoben und verarbeitet werden:

- Informationen über die Verarbeitung müssen in der Sprache des Fahrers zur Verfügung gestellt werden (Handbuch, Einstellungen usw.).

- Der EDSA empfiehlt, dass standardmäßig nur Daten verarbeitet werden, die für die Funktionsweise des Fahrzeugs unbedingt erforderlich sind. Die betroffenen Personen sollten die Möglichkeit haben, die Datenverarbeitung für jeden anderen Zweck und jeden anderen Verantwortlichen/Auftragsverarbeiter zu aktivieren oder zu deaktivieren und die betreffenden Daten unter Berücksichtigung des Zwecks und der Rechtsgrundlage der Datenverarbeitung zu löschen.

- Daten sollten nicht an Dritte weitergegeben werden (d. h. der Nutzer hat alleinigen Zugriff auf die Daten).

- Daten sollten nur so lange gespeichert werden, wie dies für die Erbringung der Dienstleistung erforderlich oder anderweitig durch Unionsrecht oder das Recht der Mitgliedstaaten vorgeschrieben ist.

- Die betroffenen Personen sollten die Möglichkeit haben, personenbezogene Daten dauerhaft zu löschen, bevor die Fahrzeuge zum Verkauf angeboten werden.

- Die betroffenen Personen sollten nach Möglichkeit einen direkten Zugriff auf die von diesen Anwendungen erzeugten Daten haben.

[40] Für weitere Empfehlungen zu Datenschutz durch Technikgestaltung und zu privatsphärefreundlichen Voreinstellungen siehe auch Leitlinien 4/2019.

[41] Artikel-29-Datenschutzgruppe – Stellungnahme 5/2012 zum Cloud Computing; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf

78. Und schließlich ist es zwar nicht immer möglich, für jeden Anwendungsfall auf die lokale Datenverarbeitung zurückzugreifen, es kann jedoch häufig eine „hybride Verarbeitung“ eingerichtet werden. Im Rahmen einer nutzungsabhängigen Versicherung könnten beispielsweise personenbezogene Daten zum Fahrverhalten (wie die auf das Bremspedal ausgeübte Kraft, die gefahrene Kilometerleistung usw.) entweder im Fahrzeug oder vom Telematikdienstleister im Auftrag der Versicherungsgesellschaft (dem Verantwortlichen) verarbeitet werden, um numerische Bewertungen zu erzeugen, die regelmäßig (z. B. monatlich) an die Versicherungsgesellschaft übermittelt werden. Auf diese Weise erhält die Versicherungsgesellschaft keinen Zugriff auf die Rohdaten zum Verhalten, sondern nur auf die insgesamt erreichte Bewertung, die das Ergebnis der Verarbeitung ist. Damit ist sichergestellt, dass der Grundsatz der Datenminimierung durch Technikgestaltung erfüllt wird. Es bedeutet auch, dass der Nutzer die Möglichkeit haben muss, sein Recht auszuüben, wenn Daten von anderen Parteien gespeichert werden: Beispielsweise sollte ein Nutzer die Möglichkeit haben, Daten, die in den Systemen einer Fahrzeugwerkstatt oder eines Autohauses gespeichert sind, unter den Bedingungen des Artikels 17 DSGVO zu löschen.

### 2.4.2 Anonymisierung und Pseudonymisierung

79. Wenn die Übermittlung personenbezogener Daten außerhalb des Fahrzeugs vorgesehen ist, sollte in Erwägung gezogen werden, diese vor der Übermittlung zu anonymisieren. Bei der Anonymisierung sollte der Verantwortliche alle Verarbeitungen berücksichtigen, die möglicherweise zu einer erneuten Identifizierung der Daten führen könnten, wie z. B. die Übermittlung lokal anonymisierter Daten. Der EDSA erinnert daran, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.[42] Sobald ein Datensatz tatsächlich anonymisiert ist und Personen nicht mehr identifizierbar sind, gilt das europäische Datenschutzgesetz nicht mehr. Infolgedessen kann die Anonymisierung gegebenenfalls eine gute Strategie sein, um die Vorteile zu wahren und die Risiken in Bezug auf vernetzte Fahrzeuge zu mindern.

80. Wie in der Stellungnahme der Artikel-29-Datenschutzgruppe zu Anonymisierungstechniken dargelegt, können verschiedene Verfahren – bisweilen kombiniert – angewendet werden, um eine Anonymisierung der Daten zu erreichen.[43]

81. Andere Techniken wie die Pseudonymisierung[44] können dazu beitragen, die durch die Datenverarbeitung entstehenden Risiken zu minimieren, wobei zu berücksichtigen ist, dass in den meisten Fällen keine direkt identifizierbaren Daten erforderlich sind, um den Zweck der Verarbeitung zu erreichen. Wenn die Pseudonymisierung durch Sicherheitsvorkehrungen verstärkt wird, verbessert sie den Schutz personenbezogener Daten, indem sie das Risiko eines Missbrauchs verringert. Die Pseudonymisierung ist im

[42] Siehe DSGVO Artikel 4 Nummer 1 und Erwägungsgrund 26.
[43] WP29 – Stellungnahme 05/2014 zu Anonymisierungstechniken; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf
[44] DSGVO Artikel 4 Nummer 5. Bericht der ENISA vom 3. Dezember 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

Gegensatz zur Anonymisierung reversibel, und pseudonymisierte Daten gelten als personenbezogene Daten, die der DSGVO unterliegen.

### 2.4.3 Datenschutz-Folgenabschätzungen

82. Angesichts des Umfangs und der Sensibilität der personenbezogenen Daten, die von vernetzten Fahrzeugen erzeugt werden können, ist es wahrscheinlich, dass die Verarbeitung – insbesondere in Situationen, in denen personenbezogene Daten außerhalb des Fahrzeugs verarbeitet werden – häufig zu einem hohen Risiko für die Rechte und Freiheiten einzelner Personen führt. In diesem Fall müssen die Teilnehmer der Branche eine Datenschutz-Folgenabschätzung durchführen, um die in den Artikeln 35 und 36 DSGVO beschriebenen Risiken zu ermitteln und zu mindern. Selbst in Fällen, in denen keine Datenschutz-Folgenabschätzung erforderlich ist, empfiehlt es sich, eine Datenschutz-Folgenabschätzung so früh wie möglich während der Systementwicklung durchzuführen. Auf diese Weise können die Teilnehmer der Branche die Ergebnisse dieser Analyse vor der Einführung neuer Technologien in ihre Gestaltungsentscheidungen einbeziehen.

## 2.5 Information

83. Vor der Verarbeitung personenbezogener Daten muss die betroffene Person über die Identität des Verantwortlichen (z. B. des Fahrzeug- und Ausrüstungsherstellers oder Dienstleisters), den Zweck der Verarbeitung, die Datenempfänger und den Zeitraum, für den die Daten gespeichert werden, sowie über die Rechte der betroffenen Person gemäß der DSGVO informiert werden.[45]

84. Darüber hinaus sollte der Fahrzeug- und Ausrüstungshersteller, Dienstleister oder sonstige Verantwortliche der betroffenen Person die folgenden Informationen in einer klaren, einfachen Sprache und in leicht zugänglicher Form zur Verfügung stellen:

- die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- die ausdrücklich genannten berechtigten Interessen, die vom Verantwortlichen oder von Dritten verfolgt werden, wenn diese berechtigten Interessen die Rechtsgrundlage für die Verarbeitung bilden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

[45] DSGVO Artikel 5 Absatz 1 Buchstabe a und Artikel 13. Siehe auch Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung (EU) 2016/679 (wp260rev.01) (vom EDSA gebilligt).

- das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird, wenn die Verarbeitung auf einer Einwilligung beruht;
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie die für die Übertragung angewandten Schutzvorkehrungen;
- Angaben darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten zur Verfügung zu stellen, und welche möglichen Folgen die Nichtbereitstellung hätte;
- das Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, die für die betroffene Person rechtliche Folgen nach sich zieht oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigt, sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person. Dies könnte insbesondere im Zusammenhang mit der Bereitstellung einer nutzungsabhängigen Versicherung für Einzelpersonen der Fall sein;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- Informationen über die Weiterverarbeitung;
- im Falle einer gemeinsamen Datenverantwortung klare und vollständige Informationen über die Zuständigkeiten der einzelnen Verantwortlichen.

85. In einigen Fällen werden personenbezogene Daten nicht direkt bei der betreffenden Person erhoben. Beispielsweise kann ein Fahrzeug- und Ausrüstungshersteller einen Händler ersuchen, Informationen über den Halter des Fahrzeugs zu erheben, um einen Pannenhilfsdienst anzubieten. Wenn die Daten nicht direkt erhoben wurden, muss der Fahrzeug- und Ausrüstungshersteller, Dienstleister oder sonstige Verantwortliche zusätzlich zu den vorstehend genannten Informationen auch angeben, um welche Arten personenbezogener Daten es sich handelt, aus welcher Quelle die personenbezogenen Daten stammen und ob diese Daten gegebenenfalls aus öffentlich zugänglichen Quellen stammen. Diese Informationen muss der Verantwortliche gemäß Artikel 14 Nummer 3 DSGVO innerhalb einer angemessenen Frist nach Erhalt der Daten zur Verfügung stellen, **spätestens jedoch am ersten der folgenden Zeitpunkte**: i) einen Monat nach Erhalt der Daten unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten, ii) zum Zeitpunkt der ersten Mitteilung an die betroffene Person oder iii) wenn diese Daten an Dritte weitergegeben werden, vor der Übermittlung der Daten.

86. Möglicherweise müssen der betroffenen Person auch neue Informationen zur Verfügung gestellt werden, wenn sie von einem neuen Verantwortlichen betreut wird. Ein Pannenhilfsdienst, der mit vernetzten Fahrzeugen interagiert, kann von verschiedenen Verantwortlichen erbracht werden, je nachdem, in welchem Land oder in welcher Region die Hilfe benötigt wird. Neue Verantwortliche sollten der betroffenen Person die erforderlichen Informationen zur Verfügung stellen, wenn die betroffenen Personen Grenzen überschreiten und Dienste, die mit vernetzten Fahrzeugen interagieren, von neuen Verantwortlichen erbracht werden.

87. Die an die betroffene Person gerichteten Informationen können schichtweise bereitgestellt werden[46], d. h. durch Trennung von zwei Informationsebenen: Zum einen Informationen der ersten Ebene, die für die betroffene Person am wichtigsten sind, und zum anderen Informationen, die vermutlich erst zu einem späteren Zeitpunkt von Interesse sind. Zu den wesentlichen Informationen der ersten Ebene gehören neben der Identität des Verantwortlichen, dem Zweck der Verarbeitung und einer Beschreibung der Rechte der betroffenen Person auch alle zusätzlichen Informationen über die Verarbeitung, die sich am stärksten auf die betroffene Person auswirkt, sowie die Verarbeitung, die sie überraschen könnte. Der EDSA empfiehlt, dass die betroffene Person im Zusammenhang mit vernetzten Fahrzeugen auf der ersten Informationsebene über alle Datenempfänger informiert werden sollte. Wie in den Leitlinien der Artikel-29-Datenschutzgruppe für Transparenz ausgeführt, sollten die Verantwortlichen Informationen über die Empfänger zur Verfügung stellen, die für die betroffenen Personen die größte Aussagekraft haben. In der Praxis sind dies in der Regel die namentlich genannten Empfänger, sodass die betroffenen Personen genau wissen, wer über ihre personenbezogenen Daten verfügt. Wenn der Verantwortliche die Namen der Empfänger nicht angeben kann, sollten die Informationen so spezifisch wie möglich sein, indem die Art des Empfängers (bezogen auf die von ihm ausgeübten Tätigkeiten), die Branche, der Sektor und der Teilsektor sowie der Standort der Empfänger angegeben werden.

88. Die betroffenen Personen können durch präzise und leicht verständliche Klauseln im Fahrzeugkaufvertrag, im Vertrag über die Erbringung von Dienstleistungen und/oder mithilfe eines beliebigen schriftlichen Mediums unter Verwendung gesonderter Dokumente (z. B. des Fahrzeug-Wartungsbuchs oder -Handbuchs) oder über den Bordcomputer informiert werden.

89. Zusätzlich zu den Informationen, die gemäß Artikel 13 und 14 DSGVO gefordert sind, könnten standardisierte Symbole verwendet werden, um die Transparenz zu erhöhen, indem die Notwendigkeit, einer betroffenen Person große Mengen an schriftlichen Informationen vorzulegen, möglicherweise reduziert wird. Sie sollten im Fahrzeug sichtbar sein, um in Bezug auf die beabsichtigte Verarbeitung einen guten Überblick zu bieten, sowie verständlich und klar lesbar sein. Der EDSA betont, wie wichtig es ist, diese Symbole zu standardisieren, damit der Nutzer unabhängig von der Marke oder dem Modell des Fahrzeugs dieselben Symbole vorfindet. Wenn beispielsweise bestimmte Arten von Daten wie der Standort erhoben werden, könnten die Fahrzeuge über ein eindeutiges bordseitiges Signal verfügen (z. B. eine Leuchte im Fahrzeuginneren), um Fahrer und Insassen über die Datenerhebung in Kenntnis zu setzen.

## 2.6 Rechte der betroffenen Person

90. Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstige Verantwortliche sollten der betroffenen Person die Kontrolle über ihre Daten während des gesamten Verarbeitungszeitraums erleichtern, indem sie spezifische Hilfsmittel anwenden, die eine wirksame Möglichkeit zur Ausübung der Rechte bieten, insbesondere ihres Rechts auf Zugang, Berichtigung und Löschung, ihres Rechts auf Einschränkung der Verarbeitung, und,

[46] Siehe Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung (EU) 2016/679 (wp260rev.01) (vom EDSA gebilligt).

je nach Rechtsgrundlage der Verarbeitung, ihres Rechts auf Datenübertragbarkeit sowie ihres Widerspruchsrechts.

91. Um Änderungen an den Einstellungen zu erleichtern, sollte ein Profilverwaltungssystem implementiert werden, um die Präferenzen bekannter Fahrer zu speichern und ihnen zu helfen, ihre Privatsphäre-Einstellungen jederzeit einfach zu ändern. Das Profilverwaltungssystem sollte jede Dateneinstellung für jede Datenverarbeitung zentralisieren, insbesondere um den Zugriff, die Löschung, die Entfernung und die Übertragbarkeit personenbezogener Daten aus Fahrzeugsystemen auf Wunsch der betroffenen Person zu erleichtern. Die Fahrer sollten in die Lage versetzt werden, die Erhebung bestimmter Arten von Daten jederzeit vorübergehend oder dauerhaft zu unterbinden, außer wenn der Verantwortliche sich auf einen bestimmten Rechtsgrund berufen kann, um die Erhebung bestimmter Daten fortzusetzen. Im Falle eines Vertrags, der ein personalisiertes Angebot auf der Grundlage des Fahrverhaltens bereitstellt, kann dies bedeuten, dass der Nutzer dann zu den Standardbedingungen dieses Vertrags zurückkehren sollte. Diese Funktionen sollten im Fahrzeug implementiert sein, wobei sie der betroffenen Person aber auch durch zusätzliche Mittel (z. B. eine spezielle Anwendung) zur Verfügung gestellt werden könnten. Darüber hinaus empfiehlt der EDSA den Herstellern, eine einfache Funktionalität (z. B. eine Löschtaste) bereitzustellen, damit die betroffenen Personen schnell und einfach personenbezogene Daten löschen können, die auf dem Armaturenbrett des Fahrzeugs gespeichert werden können (z. B. GPS-Navigationsverlauf, Internetaktivitäten usw.).

92. Der Verkauf eines vernetzten Fahrzeugs und der darauffolgende Halterwechsel sollten ebenfalls die Löschung aller personenbezogenen Daten auslösen, die für die zuvor angegebenen Zwecke nicht mehr benötigt werden, und die betroffene Person sollte in der Lage sein, ihr Recht auf Übertragbarkeit auszuüben.

## 2.7 Sicherheit

93. Fahrzeug- und Ausrüstungshersteller, Dienstleister und sonstige Verantwortliche sollten Maßnahmen ergreifen, die die Sicherheit und Vertraulichkeit der verarbeiteten Daten gewährleisten, und alle sinnvollen Vorkehrungen treffen, um zu verhindern, dass eine unbefugte Person die Kontrolle übernimmt. Insbesondere sollten die Teilnehmer der Branche erwägen, die folgenden Maßnahmen zu ergreifen:

- Verschlüsselung der Kommunikationskanäle mittels eines dem Stand der Technik entsprechenden Algorithmus;
- Einrichtung eines Systems zur Verwaltung der Verschlüsselungscodes, das für jedes Fahrzeug und nicht für jedes Modell einzigartig ist;
- bei Fernspeicherung Verschlüsselung der Daten mit einem dem Stand der Technik entsprechenden Algorithmus;
- regelmäßige Erneuerung der Verschlüsselungscodes;
- Schutz der Verschlüsselungscodes vor jeglicher Offenlegung;
- Authentifizierung von Datenempfangsgeräten;
- Sicherstellen der Datenintegrität (z. B. durch Hashing);

- zuverlässige Techniken zur Authentifizierung des Nutzers (Passwort, elektronisches Zertifikat usw.), von denen der Zugriff auf personenbezogene Daten abhängt.

94. Bezüglich der Fahrzeughersteller empfiehlt der EDSA die Umsetzung der folgenden Sicherheitsmaßnahmen:

- Trennung der wichtigsten Funktionen des Fahrzeugs von denen, die jederzeit auf Telekommunikationskapazitäten angewiesen sind (z. B. Infotainment-Dienste);
- Umsetzung technischer Maßnahmen, die es Fahrzeugherstellern ermöglichen, Sicherheitslücken während der gesamten Nutzungsdauer des Fahrzeugs rasch zu schließen;
- für die wichtigsten Funktionen des Fahrzeugs soweit möglich vorrangige Verwendung sicherer Kommunikationsmittel, die speziell für den Verkehr bestimmt sind;
- Einrichtung eines Alarmsystems für den Fall eines Angriffs auf die Fahrzeugsysteme mit der Möglichkeit, im „herabgestuften Modus“[47] zu arbeiten;
- Speicherung eines Protokolls aller Zugriffe auf das Informationssystem des Fahrzeugs, z. B. über einen Zeitraum von höchstens sechs Monaten, um den Ursprung eines etwaigen Angriffs nachvollziehen zu können, und regelmäßige Überprüfung der protokollierten Informationen, um mögliche Anomalien zu erkennen.

95. Diese allgemeinen Empfehlungen sollten durch spezifische Anforderungen ergänzt werden, die den Merkmalen und dem Zweck der jeweiligen Datenverarbeitung Rechnung tragen.

## 2.8 Übertragung personenbezogener Daten an Dritte

96. Grundsätzlich haben nur der Verantwortliche und die betroffene Person Zugriff auf die von einem vernetzten Fahrzeug erzeugten Daten. Der Verantwortliche kann jedoch personenbezogene Daten an einen Geschäftspartner (Empfänger) übermitteln, sofern sich diese Übermittlung rechtmäßig auf eine der in Artikel 6 DSGVO genannten Rechtsgrundlagen stützt.

97. In Anbetracht der möglichen Sensibilität der Fahrzeugnutzungsdaten (z. B. zurückgelegte Fahrten, Fahrstil) empfiehlt der EDSA, dass die Einwilligung der betroffenen Person systematisch eingeholt wird, bevor ihre Daten an einen Geschäftspartner übertragen werden, der als Verantwortlicher fungiert (z. B. durch Ankreuzen eines Kästchens, das nicht vorab angekreuzt ist, oder, sofern technisch möglich, durch Verwendung eines physischen oder logischen Geräts, auf das die Person vom Fahrzeug aus zugreifen kann). Der Geschäftspartner wiederum übernimmt die Verantwortung für die Daten, die er erhält, und unterliegt allen Bestimmungen der DSGVO.

98. Der Fahrzeughersteller, Dienstleister oder sonstige Verantwortliche kann personenbezogene Daten an einen Auftragsverarbeiter übermitteln, der ausgewählt wurde, um an der Erbringung der Dienstleistung für die betroffene Person mitzuwirken, sofern der Auftragsverarbeiter diese Daten nicht für eigene Zwecke verwendet. Die Verantwortlichen

[47] Der „herabgestufte Modus“ ist ein Betriebsmodus des Fahrzeugs, der sicherstellt, dass die für den sicheren Betrieb des Fahrzeugs wesentlichen Funktionen (d. h. die minimalen Sicherheitsanforderungen) gewährleistet sind, selbst wenn andere, weniger wichtige Funktionen deaktiviert sind (z. B. kann der Betrieb des Geo-Leitgeräts im Gegensatz zum Bremssystem als nicht wesentlich betrachtet werden).

und Auftragsverarbeiter müssen einen Vertrag oder ein anderes rechtliches Dokument aufsetzen, in dem die Pflichten jeder Partei und die Bestimmungen des Artikels 28 DSGVO dargelegt werden.

## 2.9 Übermittlung personenbezogener Daten außerhalb der EU/des EWR

99. Wenn personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums übertragen werden, sind besondere Vorkehrungen vorgesehen, um sicherzustellen, dass der Schutz weiterhin besteht.

100. Infolgedessen darf der Verantwortliche personenbezogene Daten nur dann an einen Empfänger übermitteln, wenn diese Übermittlung den in Kapitel V DSGVO festgelegten Anforderungen entspricht.

## 2.10 Verwendung bordeigener Wi-Fi-Technologie

101. Fortschritte in der Mobilfunktechnologie haben es möglich gemacht, das Internet unterwegs problemlos zu nutzen. Während es möglich ist, über einen Smartphone-Hotspot oder ein spezielles Gerät (OBD-II-Dongle, drahtloses Modem oder Router usw.) eine Wi-Fi-Anschlussmöglichkeit in einem Fahrzeug zur Verfügung zu stellen, bieten die meisten Hersteller heutzutage Modelle an, die eine eingebaute Mobilfunk-Datenverbindung enthalten und auch in der Lage sind, Wi-Fi-Netzwerke zu erzeugen. Je nach Fall sind verschiedene Aspekte zu berücksichtigen:

- Die Wi-Fi-Anschlussmöglichkeit wird als Dienstleistung von einem professionellen Verkehrsteilnehmer angeboten, beispielsweise von einem Taxifahrer für seine Kunden. In diesem Fall kann der professionelle Verkehrsteilnehmer oder sein Unternehmen als Internetdienstleister betrachtet werden, der somit besonderen Verpflichtungen und Beschränkungen hinsichtlich der Verarbeitung der personenbezogenen Daten seiner Kunden unterliegt.

- Die Wi-Fi-Anschlussmöglichkeit wird für die alleinige Nutzung durch den Fahrer (unter Ausschluss des Fahrers und der Fahrzeuginsassen) eingerichtet. In diesem Fall gilt die Verarbeitung personenbezogener Daten als ausschließlich persönliche oder familiäre Tätigkeit im Sinne des Artikels 2 Absatz 2 Buchstabe c und Erwägungsgrund 18 DSGVO.

102. Im Allgemeinen birgt die Verbreitung von Schnittstellen für Internetverbindungen über Wi-Fi größere Risiken für die Privatsphäre des Einzelnen. In der Tat werden die Nutzer durch ihre Fahrzeuge zu kontinuierlichen Sendern und können daher identifiziert und verfolgt werden. Um eine Rückverfolgung zu verhindern, sollten die Fahrzeug- und Gerätehersteller daher einfach zu bedienende Widerspruchsmöglichkeiten einrichten, die sicherstellen, dass der Service Set Identifier (SSID) des bordeigenen Wi-Fi-Netzwerks nicht erfasst wird.

# 3 FALLSTUDIEN

103. In diesem Abschnitt werden fünf spezifische Beispiele für die Verarbeitung im Zusammenhang mit vernetzten Fahrzeugen behandelt, die Szenarios entsprechen, mit denen die Interessengruppen in diesem Sektor wahrscheinlich konfrontiert sein werden. Die Beispiele umfassen Datenverarbeitung, die Rechenleistung erfordert, die nicht lokal im Fahrzeug erbracht werden kann, und/oder die Übermittlung personenbezogener Daten an Dritte erfordert, um weitere Analysen durchzuführen oder weitere Funktionen aus der Ferne zur Verfügung zu stellen. In den vorliegenden Leitlinien werden für jede Art der Verarbeitung die beabsichtigten Zwecke, die Arten der erhobenen Daten, die Speicherfrist für diese Daten, die Rechte der betroffenen Personen, die erforderlichen Sicherheitsmaßnahmen und die Empfänger der Informationen angegeben. Für den Fall, dass einige dieser Bereiche im Folgenden nicht beschrieben werden, gelten die im vorstehenden Teil beschriebenen allgemeinen Empfehlungen.

104. Die ausgewählten Beispiele erheben keinen Anspruch auf Vollständigkeit und sollen auf die Vielfalt der Verarbeitungsarten, der Rechtsgrundlagen, der Akteure usw. hinweisen, die im Zusammenhang mit vernetzten Fahrzeugen zum Einsatz kommen können.

## 3.1 Erbringung einer Dienstleistung durch eine dritte Partei

105. Betroffene Personen können einen Vertrag mit einem Dienstleister schließen, um Dienste mit Zusatznutzen für ihr Fahrzeug zu erhalten. Beispielsweise kann eine betroffene Person einen nutzungsabhängigen Versicherungsvertrag abschließen, der reduzierte Versicherungsprämien bei geringerer Fahrleistung (Abrechnung nach gefahrenen Kilometern, „Pay As You Drive“) oder vorbildlichem Fahrverhalten („Pay How You Drive“) bietet und eine Überwachung der Fahrgewohnheiten durch die Versicherungsgesellschaft erfordert. Eine betroffene Person könnte auch einen Vertrag mit einem Unternehmen schließen, das einen Pannenhilfsdienst anbietet, für den der Standort des Fahrzeugs an das Unternehmen oder an einen Dienstleister übermittelt wird, um Nachrichten oder Warnungen bezüglich der Funktionsweise des Fahrzeugs zu erhalten (z. B. eine Warnung über den Verschleißzustand der Bremsen oder eine Erinnerung an einen Inspektionstermin).

### 3.1.1 Nutzungsabhängige Versicherung

106. Die Abrechnung nach gefahrenen Kilometern ist eine Art von nutzungsabhängiger Versicherung, bei der die Kilometerleistung und/oder die Fahrgewohnheiten des Fahrers erfasst werden, um „sichere“ Fahrer durch niedrigere Prämien zu unterscheiden und zu belohnen. Die Versicherungsgesellschaft fordert vom Fahrer die Installation eines eingebauten Telematikdienstes oder einer mobilen Anwendung oder die Aktivierung eines vom Hersteller eingebauten Moduls, das die zurückgelegten Kilometer und/oder das Fahrverhalten (Bremsverhalten, schnelles Beschleunigen usw.) des Versicherungsnehmers verfolgt. Anhand der vom Telematikgerät erhobenen Informationen werden dem Fahrer Bewertungspunkte zugewiesen, um zu analysieren, welche Risiken sich daraus für die Versicherungsgesellschaft ergeben.

107. Da die nutzungsabhängige Versicherung eine Einwilligung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erfordert, weist der EDSA darauf hin, dass der Versicherungsnehmer die Wahl haben muss, einen nicht nutzungsabhängigen Versicherungsvertrag abzuschließen. Andernfalls würde die Einwilligung nicht als freiwillig erteilt betrachtet, da die Vertragserfüllung von der Einwilligung abhängig wäre. Ferner verlangt Artikel 7 Absatz 3 DSGVO, dass eine betroffene Person das Recht haben muss, ihre Einwilligung zu widerrufen.

#### *3.1.1.1 Rechtsgrundlage*

108. Wenn die Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst (z. B. über die im Telematikgerät enthaltene SIM-Karte) erhoben werden, ist gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation eine Einwilligung erforderlich, um Zugriff auf Informationen zu erhalten, die bereits im Fahrzeug gespeichert sind. Tatsächlich greift in diesem Zusammenhang keine der in diesen Bestimmungen vorgesehenen Ausnahmen: Die Verarbeitung erfolgt weder zum alleinigen Zweck der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz, noch bezieht sie sich auf einen vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienst der Informationsgesellschaft. Die Einwilligung könnte zum Zeitpunkt des Vertragsschlusses eingeholt werden.

109. Was die Verarbeitung personenbezogener Daten nach der Speicherung oder dem Zugriff auf das Endgerät des Nutzers betrifft, so kann sich die Versicherungsgesellschaft in diesem speziellen Kontext auf Artikel 6 Absatz 1 Buchstabe b DSGVO stützen, sofern sie nachweisen kann, dass die Verarbeitung im Rahmen eines gültigen Vertrags mit der betroffenen Person

erfolgt und dass die Verarbeitung erforderlich ist, damit der jeweilige Vertrag mit der betroffenen Person erfüllt werden kann. Sofern die Verarbeitung für die Erfüllung des Vertrags mit der betroffenen Person objektiv erforderlich ist, vertritt der EDSA die Ansicht, dass die Berufung auf Artikel 6 Absatz 1 Buchstabe b DSGVO nicht dazu führen würde, dass sich der durch Artikel 5 Absatz 3 der ePrivacy-RL gewährte zusätzliche Schutz in diesem speziellen Fall verringert. Diese Rechtsgrundlage kommt dadurch zustande, dass die betroffene Person einen Vertrag mit der Versicherungsgesellschaft schließt.

#### *3.1.1.2 Erhobene Daten*

110. Es sind zwei Arten von personenbezogenen Daten zu berücksichtigen:

- **Geschäfts- und Transaktionsdaten**: Daten zur Identifizierung der betroffenen Person, transaktionsbezogene Daten, Daten über Zahlungsmittel usw.;
- **Nutzungsdaten**: personenbezogene Daten, die durch das Fahrzeug erzeugt werden, Fahrgewohnheiten, Standort usw.

111. Der EDSA empfiehlt – soweit möglich und angesichts des Risikos, dass die von der Telematikbox erhobenen Daten zur Erstellung eines genauen Bewegungsprofils des Fahrers missbraucht werden könnten –, dass Rohdaten über das Fahrverhalten entweder:

- im Fahrzeug in der Telematikbox oder im Smartphone des Nutzers verarbeitet werden sollten, sodass die Versicherungsgesellschaft nur auf die Ergebnisdaten (z. B. die Bewertung der Fahrgewohnheiten) und nicht auf detaillierte Rohdaten zugreift (siehe Abschnitt 2.1);
- oder vom Telematikdienstleister im Auftrag des Verantwortlichen (der Versicherungsgesellschaft) verarbeitet werden sollten, um numerische Bewertungen zu erzeugen, die auf einer festgelegten Grundlage an die Versicherungsgesellschaft übermittelt werden. In diesem Fall müssen Rohdaten und Daten, die sich direkt auf die Identität des Fahrers beziehen, getrennt werden. Dies bedeutet, dass der Telematikdienstleister die Echtzeitdaten erhält, jedoch den Namen, das Kennzeichen usw. des Versicherungsnehmers nicht kennt. Auf der anderen Seite kennt die Versicherungsgesellschaft den Namen des Versicherungsnehmers, erhält jedoch nur die Bewertung und die Summe der gefahrenen Kilometer, aber nicht die Rohdaten, die zur Erstellung dieser Bewertung verwendet wurden.

112. Darüber hinaus ist zu beachten, dass Standortdaten nicht erhoben werden dürfen, wenn nur die Übermittlung des Kilometerstands für die Vertragserfüllung erforderlich ist.

#### *3.1.1.3 Speicherfrist*

113. Im Zusammenhang mit der Datenverarbeitung, die zur Erfüllung eines Vertrags (d. h. Erbringung einer Dienstleistung) stattfindet, ist es wichtig, zwischen zwei Arten von Daten zu unterscheiden, bevor ihre jeweiligen Speicherfristen festgelegt werden:

- **Geschäfts- und Transaktionsdaten:** Diese Daten können während der gesamten Vertragsdauer in einer aktiven Datenbank gespeichert werden. Bei Vertragsende können sie physisch (auf einem gesonderten Medium: DVD usw.) oder logisch (durch Berechtigungsverwaltung) für den Fall eines möglichen Rechtsstreits archiviert werden. Anschließend werden die Daten nach Ablauf der gesetzlichen Verjährungsfristen gelöscht oder anonymisiert;
- **Nutzungsdaten:** Nutzungsdaten lassen sich in Rohdaten und aggregierte Daten unterteilen. Wie vorstehend erwähnt, sollten Verantwortliche oder Auftragsverarbeiter nach Möglichkeit

keine Rohdaten verarbeiten. Wenn es notwendig ist, sollten Rohdaten nur so lange gespeichert werden, wie zur Ausarbeitung der aggregierten Daten und zur Überprüfung der Gültigkeit dieses Aggregationsverfahrens erforderlich. Aggregierte Daten sollten so lange gespeichert werden, wie für die Erbringung der Dienstleistung erforderlich oder anderweitig durch Unionsrecht oder das Recht der Mitgliedstaaten gefordert.

#### *3.1.1.4 Information und Rechte der betroffenen Personen*

114. Vor der Verarbeitung personenbezogener Daten ist die betroffene Person gemäß Artikel 13 DSGVO auf transparente und verständliche Weise zu informieren. Insbesondere muss sie über die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, über die Kriterien für die Festlegung dieser Dauer informiert werden. In letzterem Fall empfiehlt der EDSA einen pädagogischen Ansatz, um den Unterschied zwischen den Rohdaten und der auf dieser Grundlage erstellten Bewertung hervorzuheben und dabei zu betonen, dass die Versicherungsgesellschaft in diesem Fall gegebenenfalls nur das Ergebnis der Bewertung erfasst.

115. Werden die Daten nicht im Fahrzeug, sondern von einem Telematikanbieter im Auftrag des Verantwortlichen (der Versicherungsgesellschaft) verarbeitet, so könnte in den Informationen sinnvollerweise erwähnt werden, dass der Anbieter in diesem Fall keinen Zugriff auf Daten hat, die sich direkt auf die Identität des Fahrers beziehen (wie Namen, Kennzeichen usw.). Da die betroffenen Personen unbedingt über die Folgen der Verarbeitung ihrer personenbezogenen Daten informiert werden müssen und die betroffenen Personen von der Verarbeitung ihrer personenbezogenen Daten nicht überrascht werden sollten, empfiehlt der EDSA ferner, die betroffenen Personen darauf hinzuweisen, dass Profiling stattfindet und welche Folgen dies hat, auch wenn es sich nicht um eine automatisierte Entscheidung im Sinne des Artikels 22 DSGVO handelt.

116. In Bezug auf das Recht der betroffenen Personen sind sie ausdrücklich über die verfügbaren Mittel zur Ausübung ihres Rechts auf Auskunft, Berichtigung, Einschränkung und Löschung zu informieren. Da die in diesem Zusammenhang erhobenen Rohdaten von der betroffenen Person (durch bestimmte Formulare oder durch ihre Tätigkeit) zur Verfügung gestellt und auf der Grundlage des Artikels 6 Absatz 1 Buchstabe b DSGVO (Erfüllung eines Vertrags) verarbeitet werden, ist die betroffene Person berechtigt, von ihrem Recht auf Datenübertragbarkeit Gebrauch zu machen. Wie in den Leitlinien zum Recht auf Datenübertragbarkeit hervorgehoben, empfiehlt der EDSA nachdrücklich, „dass Verantwortliche klar und deutlich den Unterschied zwischen den verschiedenen Arten von Daten darlegen, die eine betroffene Person erhalten kann, wenn sie von ihrem Auskunftsrecht oder von ihrem Recht auf Datenübertragbarkeit Gebrauch macht“.[48]

117. Die Information kann bei Vertragsunterzeichnung zur Verfügung gestellt werden.

#### *3.1.1.5 Empfänger*

118. Der EDSA empfiehlt, die Nutzungsdaten des Fahrzeugs möglichst direkt in den Telematikboxen zu verarbeiten, damit die Versicherungsgesellschaft nur auf die

[48] Artikel-29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit gemäß Verordnung (EU) 2016/676, WP242 rev.01, (vom EDSA gebilligt), S. 15.

Ergebnisdaten (z. B. die erreichten Bewertungspunkte) und nicht auf detaillierte Rohdaten zugreift.

119. Erhebt ein Telematikdienstleister die Daten im Auftrag des Verantwortlichen (der Versicherungsgesellschaft), um numerische Bewertungen zu erzeugen, muss er nicht die Identität des Fahrers (wie Namen, Kennzeichen usw.) der Versicherungsnehmer kennen.

#### *3.1.1.6 Sicherheit*

120. Es gelten die allgemeinen Empfehlungen. Siehe Abschnitt 2.7.

### 3.1.2 Vermietung und Reservierung eines Parkplatzes

121. Es kann sein, dass der Eigentümer eines Parkplatzes diesen vermieten will. Dazu führt er den Platz in einer Webanwendung in einer Liste auf und legt einen Preis dafür fest. Sobald der Parkplatz auf der Liste ist, benachrichtigt die Anwendung den Eigentümer, wenn ein Fahrer ihn reservieren möchte. Der Fahrer kann ein Ziel auswählen und anhand mehrerer Kriterien nach verfügbaren Parkplätzen suchen. Nach der Einwilligung des Eigentümers wird das Geschäft bestätigt, und der Dienstleister wickelt den Zahlungsvorgang ab. Anschließend fährt der Fahrer mithilfe der Navigation zum angegebenen Ort.

#### *3.1.2.1 Rechtsgrundlage*

122. Wenn die Daten über eine öffentlich zugängliche elektronische Kommunikation erhoben werden, gilt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation.

123. Da es sich um einen Dienst der Informationsgesellschaft handelt, verlangt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation keine Einwilligung für den Zugriff auf bereits im Fahrzeug gespeicherte Informationen, wenn ein solcher Dienst vom Teilnehmer ausdrücklich angefordert wird.

124. Für die Verarbeitung personenbezogener Daten und nur für Daten, die für die Erfüllung des Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich sind, bildet Artikel 6 Absatz 1 Buchstabe b DSGVO die Rechtsgrundlage.

#### *3.1.2.2 Erhobene Daten*

125. Zu den verarbeiteten Daten gehören die Kontaktdaten des Fahrers (Name, E-Mail-Adresse, Telefonnummer), der Fahrzeugtyp (z. B. Pkw, Lkw, Motorrad), das Kennzeichen, die Parkdauer, die Zahlungsdaten (z. B. Kreditkarteninformationen) sowie Navigationsdaten.

#### *3.1.2.3 Speicherfrist*

126. Daten sollten nur so lange gespeichert werden, wie zur Erfüllung des Parkvertrags oder anderweitig durch Unionsrecht oder das Recht der Mitgliedstaaten erforderlich. Danach werden die Daten entweder anonymisiert oder gelöscht.

#### *3.1.2.4 Information und Rechte der betroffenen Personen*

127. Vor der Verarbeitung personenbezogener Daten sollte die betroffene Person gemäß Artikel 13 DSGVO auf transparente und verständliche Weise informiert werden.

128. Die betroffene Person sollte ausdrücklich über die verfügbaren Mittel zur Ausübung ihres Rechts auf Auskunft, Berichtigung, Einschränkung und Löschung informiert werden. Da die in diesem Zusammenhang erhobenen Daten von der betroffenen Person (durch bestimmte Formulare oder durch ihre Tätigkeit) zur Verfügung gestellt und auf der Grundlage von Artikel 6 Absatz 1 Buchstabe b DSGVO (Erfüllung eines Vertrags) verarbeitet werden, ist die betroffene Person berechtigt, von ihrem Recht auf Datenübertragbarkeit Gebrauch zu

machen. Wie in den Leitlinien zum Recht auf Datenübertragbarkeit hervorgehoben, empfiehlt der EDSA nachdrücklich, *„dass Verantwortliche klar und deutlich den Unterschied zwischen den verschiedenen Arten von Daten darlegen, die eine betroffene Person erhalten kann, wenn sie von ihrem Auskunftsrecht oder von ihrem Recht auf Datenübertragbarkeit Gebrauch macht“*.

#### *3.1.2.5* Empfänger

129. Grundsätzlich haben nur der Verantwortliche und der Auftragsverarbeiter Zugriff auf die Daten.

#### *3.1.2.6 Sicherheit*

130. Es gelten die allgemeinen Empfehlungen. Siehe Abschnitt 2.7.

## 3.2 eCall

131. Bei einem schweren Unfall in der Europäischen Union löst das Fahrzeug automatisch einen eCall an die EU-weite Notrufnummer 112 aus (weitere Einzelheiten dazu in Abschnitt 1.1), über die gemäß der Verordnung (EU) 2015/758 vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG (im Folgenden „Verordnung (EU) 2015/758“) umgehend ein Krankenwagen an den Unfallort geschickt werden kann.

132. Tatsächlich löst der im Fahrzeug installierte eCall-Generator, der die Übertragung über ein öffentliches Mobilfunknetz ermöglicht, einen Notruf aus, der nur im Falle eines Unfalls entweder automatisch von Fahrzeugsensoren oder manuell von den Fahrzeuginsassen ausgelöst wird. Neben der Herstellung einer Tonverbindung wird infolge eines Unfalls zudem ein Minimaler Datensatz (MSD) automatisch erzeugt und an die Notrufabfragestelle übermittelt.

### 3.2.1 Rechtsgrundlage

133. Bei der Anwendung der Datenschutzrichtlinie für elektronische Kommunikation sind zwei Bestimmungen zu beachten:

- Artikel 9 bezüglich anderer Standortdaten als Verkehrsdaten, der nur für elektronische Kommunikationsdienste gilt;
- Artikel 5 Absatz 3 für den Zugriff auf Informationen, die in dem im Fahrzeug installierten Generator gespeichert sind.

134. Obgleich diese Bestimmungen grundsätzlich die Einwilligung der betroffenen Person erfordern, stellt die Verordnung (EU) 2015/758 eine rechtliche Verpflichtung dar, der der Verantwortliche unterliegt (die betroffene Person hat keine echte oder freie Wahl und kann die Verarbeitung ihrer Daten nicht verweigern). Daher setzt die Verordnung (EU) 2015/758

das Erfordernis einer Einwilligung des Fahrers für die Verarbeitung der Standortdaten und des MSD außer Kraft.[49]

135. Die Rechtsgrundlage für die Verarbeitung dieser Daten ist die Einhaltung einer rechtlichen Verpflichtung gemäß Artikel 6 Absatz 1 Buchstabe c DSGVO (d. h. der Verordnung (EU) 2015/758).

### 3.2.2 Erhobene Daten

136. Die Verordnung (EU) 2015/578 sieht vor, dass die vom auf dem 112-Notruf basierenden bordeigenen eCall-System übermittelten Daten ausschließlich die Mindestinformationen gemäß der Norm EN 15722:2015 „Intelligente Transportsysteme – Elektronische Sicherheit – Minimaler Datensatz (MSD) für den elektronischen Notruf eCall“ enthalten. Dazu gehören:

- die Anzeige, ob das eCall-System manuell oder automatisch ausgelöst wurde;
- der Fahrzeugtyp;
- die Fahrzeug-Identifizierungsnummer;
- die Antriebsart des Fahrzeugs;
- der Zeitstempel der Erzeugung der ersten Datenmeldung innerhalb des aktuellen eCall-Ereignisses;
- die letzte bekannte Position des Fahrzeugs in geografischer Breite und Länge, die zum letztmöglichen Zeitpunkt vor der Erzeugung der Meldung bestimmt wurde;
- die letzte bekannte tatsächliche Fahrtrichtung des Fahrzeugs, die zum letztmöglichen Zeitpunkt vor der Erzeugung der Meldung ermittelt wurde (nur die letzten drei Standorte des Fahrzeugs).

### 3.2.3 Speicherfrist

137. Die Verordnung (EU) 2015/758 sieht vor, dass Daten nicht länger gespeichert werden dürfen, als es für die Handhabung von Notfallsituationen erforderlich ist. Diese Daten werden vollständig gelöscht, wenn sie für diesen Zweck nicht mehr benötigt werden. Darüber hinaus müssen die Daten im internen Speicher des eCall-Systems automatisch und kontinuierlich gelöscht werden. Es können nur die letzten drei Positionen des Fahrzeugs gespeichert werden, sofern dies unbedingt erforderlich ist, um die aktuelle Position des Fahrzeugs und die Fahrtrichtung zum Zeitpunkt des Ereignisses anzugeben.

### 3.2.4 Information und Rechte der betroffenen Personen

138. Gemäß Artikel 6 der Verordnung (EU) 2015/758 müssen die Hersteller klare und umfassende Informationen über die Verarbeitung von Daten durch das eCall-System zur Verfügung stellen. Diese Informationen müssen in der Betriebsanleitung für das auf dem

[49] Es ist anzumerken, dass Artikel 8 Absatz 1 Buchstabe f des Verhandlungsmandats des Rates für den Vorschlag für eine Datenschutzverordnung für elektronische Kommunikation insofern eine besondere Ausnahme für das eCall-System vorsieht, als eine Einwilligung nicht erforderlich ist, wenn es notwendig ist, *„Endeinrichtungen im Einklang mit Artikel 13 Absatz 3 zu orten, wenn ein Endnutzer einen Notruf tätigt, entweder über die einheitliche europäische Notrufnummer „112“ oder über eine nationale Notrufnummer.“*

112-Notruf basierende bordeigene eCall-System und alle von Drittanbietern unterstützten eCall-Systeme getrennt voneinander vor der Inbetriebnahme des Systems bereitgestellt werden. Dazu gehören:

- die Angabe der Rechtsgrundlage für die Datenverarbeitung;
- die Angabe, dass das auf dem 112-Notruf basierende bordeigene eCall-System standardmäßig automatisch aktiviert wird;
- die Ausgestaltung der vom auf dem 112-Notruf basierenden bordeigenen eCall-System durchgeführten Datenverarbeitung;
- der spezifische Zweck der eCall-Verarbeitung, der auf die in Artikel 5 Absatz 2 Unterabsatz 1 der Verordnung (EU) 2015/758 genannten Notfallsituationen beschränkt ist;
- die Art der erhobenen und verarbeiteten Daten sowie die Empfänger derselben;
- die Dauer der Speicherung der Daten im auf dem 112-Notruf basierenden bordeigenen eCall-System;
- die Angabe, dass keine dauerhafte Verfolgung des Fahrzeugs erfolgt;
- die Ausgestaltung der Wahrnehmung der Rechte der durch die Datenverarbeitung betroffenen Personen sowie die Kontaktstelle, die für die Bearbeitung von Zugriffsanträgen zuständig ist;
- jegliche sonstigen zusätzlichen Informationen hinsichtlich der Verfolgbarkeit, Verfolgung und Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung eines eCall-Systems und/oder anderer Dienste mit Zusatznutzen durch Drittanbieter, für die der Fahrzeughalter seine ausdrückliche Einwilligung erteilen muss und die mit der DSGVO im Einklang stehen müssen. Insbesondere ist zu berücksichtigen, dass es Unterschiede bei der Datenverarbeitung über das auf dem 112-Notruf basierende bordeigene eCall-System und über die bordeigenen TPS-eCall-Systeme oder andere Dienste mit Zusatznutzen geben kann.

139. Darüber hinaus hat der Dienstleister die betroffenen Personen gemäß Artikel 13 DSGVO auf transparente und verständliche Weise zu informieren. Insbesondere muss er sie über die Zwecke der Verarbeitung informieren, für die die personenbezogenen Daten bestimmt sind, sowie darüber, dass die Verarbeitung personenbezogener Daten auf einer rechtlichen Verpflichtung beruht, der der Verantwortliche unterliegt.

140. Darüber hinaus sollten, unter Berücksichtigung der Art der Verarbeitung, die Informationen über die Empfänger bzw. Kategorien von Empfängern der personenbezogenen Daten eindeutig sein, und die betroffenen Personen sollten darüber informiert werden, dass die Daten außerhalb des auf dem 112-Notruf basierenden bordeigenen eCall-Systems nicht für andere Einrichtungen verfügbar sind, bevor der eCall ausgelöst wird.

141. In Bezug auf die Rechte der betroffenen Person ist zu beachten, dass das Widerspruchsrecht und das Recht auf Übertragbarkeit nicht gelten, da die Verarbeitung auf einer rechtlichen Verpflichtung beruht.

### 3.2.5 Empfänger

142. Bevor der eCall ausgelöst wird, dürfen die Daten außerhalb des auf dem 112-Notruf basierenden bordeigenen eCall-Systems für keine Einrichtung zugänglich sein.

143. Wenn er ausgelöst wird (entweder manuell von den Fahrzeuginsassen oder automatisch, sobald ein bordeigener Sensor eine schwere Kollision erkennt), stellt das eCall-System eine Sprachverbindung mit der entsprechenden Notrufabfragestelle her, und der MSD wird an den Betreiber der Notrufabfragestelle übermittelt.

144. Darüber hinaus dürfen die über ein auf dem 112-Notruf basierendes bordeigenes eCall-System übermittelten und von den Notrufabfragestellen verarbeiteten Daten an die im Beschluss Nr. 585/2014/EU aufgeführten Notdienste und Dienstleistungspartner nur im Zusammenhang mit eCalls und unter den in jenem Beschluss festgelegten Bedingungen weitergegeben und ausschließlich für die Erreichung der mit jenem Beschluss verfolgten Ziele verwendet werden. Die von den Notrufabfragestellen über das auf dem 112-Notruf basierende bordeigene eCall-System verarbeiteten Daten werden nicht ohne die ausdrückliche vorherige Einwilligung der betroffenen Person an andere Dritte weitergegeben.

### 3.2.6 Sicherheit

145. In der Verordnung (EU) 2015/758 sind die Anforderungen festgelegt, in das eCall-System Technologien zu integrieren, die den Schutz der Privatsphäre verbessern, um den Nutzern ein angemessenes Maß an Schutz der Privatsphäre sowie die Garantien zu bieten, die zur Verhinderung von Überwachung und missbräuchlicher Verwendung erforderlich sind. Darüber hinaus sollten die Hersteller sicherstellen, dass das auf dem 112-Notruf basierende eCall-System sowie jedes andere System, das einen eCall bereitstellt, der von Drittanbietern oder einem Dienst mit Zusatznutzen bearbeitet wird, so gestaltet ist, dass ein Austausch personenbezogener Daten zwischen diesen Systemen unmöglich ist.

146. Hinsichtlich der Notrufabfragestellen sollten die Mitgliedstaaten sicherstellen, dass personenbezogene Daten vor Missbrauch wie unrechtmäßigem Zugriff, Veränderung oder Verlust geschützt sind und dass Bestimmungen für die Speicherung personenbezogener Daten, die Dauer der Speicherung, die Verarbeitung und den Schutz auf der angemessenen Ebene erlassen und ordnungsgemäß eingehalten werden.

## 3.3 Unfallforschungsstudien

147. Die betroffenen Personen können sich freiwillig bereiterklären, an Unfallforschungsstudien teilzunehmen, die dem besseren Verständnis der Ursachen von Verkehrsunfällen und allgemein wissenschaftlichen Zwecken dienen.

### 3.3.1 Rechtsgrundlage

148. Wenn die Daten über einen öffentlichen elektronischen Kommunikationsdienst erhoben werden, muss der Verantwortliche die Einwilligung der betroffenen Person einholen, um Zugriff auf Informationen zu erhalten, die bereits im Fahrzeug gespeichert sind, wie es gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erforderlich ist. Tatsächlich greift in diesem Zusammenhang keine der in diesen Bestimmungen vorgesehenen Ausnahmen: Die Verarbeitung erfolgt weder zum alleinigen Zweck der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz, noch bezieht sie sich auf einen vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienst der Informationsgesellschaft.

149. In Bezug auf die Verarbeitung personenbezogener Daten und unter Berücksichtigung der Vielfalt und der Menge der personenbezogenen Daten, die für Unfallforschungsstudien benötigt werden, empfiehlt der EDSA, dass die Verarbeitung auf der vorherigen Einwilligung

der betroffenen Person gemäß Artikel 6 DSGVO beruht. Diese vorherige Einwilligung muss durch ein bestimmtes Formular erteilt werden, mit dem sich die betroffene Person freiwillig zur Teilnahme an der Studie und zur Verarbeitung ihrer personenbezogenen Daten zu diesem Zweck bereit erklärt. Die Einwilligung muss eine freiwillig für den bestimmten Fall und in informierter Weise abgegebene Willensbekundung der Person sein, deren Daten verarbeitet werden (z. B. durch Ankreuzen eines Kästchens, das nicht vorab angekreuzt ist, oder durch die Konfiguration des Bordcomputers zur Aktivierung einer Funktion im Fahrzeug). Eine solche Einwilligung muss jeweils gesondert für bestimmte Zwecke erteilt werden und darf nicht mit dem Kauf- oder Leasingvertrag eines neuen Kraftfahrzeugs gebündelt werden; auch muss die Einwilligung genauso einfach zurückgezogen werden können, wie sie erteilt wird. Der Widerruf der Einwilligung führt zur Einstellung der Verarbeitung. Die Daten werden dann aus der aktiven Datenbank gelöscht oder anonymisiert.

150. Die Einwilligung, die nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erforderlich ist, und die Einwilligung, die als Rechtsgrundlage für die Verarbeitung von Daten erforderlich ist, können gleichzeitig eingeholt werden (z. B. durch Ankreuzen eines Kästchens, das eindeutig angibt, wozu die betroffene Person ihre Einwilligung erteilt).

151. Es ist zu beachten, dass je nach den Bedingungen der Verarbeitung (Art des Verantwortlichen usw.) eine andere Rechtsgrundlage rechtmäßig gewählt werden kann, solange sie den zusätzlichen Schutz gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation nicht mindert (siehe Randnummer 15). Beruht die Verarbeitung auf einer anderen Rechtsgrundlage, beispielsweise auf der Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt (Artikel 6 Absatz 1 Buchstabe e DSGVO), so empfiehlt der EDSA, die betroffenen Personen auf freiwilliger Basis in die Studie einzubeziehen.

### 3.3.2 Erhobene Daten

152. Der Verantwortliche darf nur personenbezogene Daten erheben, die für die Verarbeitung unbedingt erforderlich sind.

153. Es sind zwei Arten von Daten zu berücksichtigen:

- **Daten über Teilnehmer und Fahrzeuge**;
- **technische Daten von Fahrzeugen** (aktuelle Geschwindigkeit usw.).

154. Wissenschaftliche Forschung im Zusammenhang mit Unfallforschung rechtfertigt die Erhebung der aktuellen Geschwindigkeit, auch durch juristische Personen, die keine öffentliche Dienstleistung im engeren Sinne erbringen.

155. Wie vorstehend erwähnt, vertritt der EDSA die Ansicht, dass die im Rahmen einer Unfallforschungsstudie erhobene aktuelle Geschwindigkeit dem Zweck nach nicht zu den strafrechtlich relevanten Daten gehört (d. h. sie wird nicht zum Zweck der Untersuchung oder Verfolgung einer Straftat erhoben), was ihre Erhebung durch juristische Personen rechtfertigt, die keine öffentliche Dienstleistung im engeren Sinne erbringen.

### 3.3.3 Speicherfrist

156. Es ist wichtig, zwischen zwei Arten von Daten zu unterscheiden. Erstens können die Daten, die sich auf Teilnehmer und Fahrzeuge beziehen, für die Dauer der Studie gespeichert

werden. Zweitens sollten zu diesem Zweck die technischen Daten von Fahrzeugen so kurz wie möglich gespeichert werden. In dieser Hinsicht dürften fünf Jahre ab dem Enddatum der Studie ein angemessener Zeitraum sein. Am Ende dieses Zeitraums werden die Daten gelöscht oder anonymisiert.

### 3.3.4 Information und Rechte der betroffenen Personen

157. Vor der Verarbeitung personenbezogener Daten ist die betroffene Person gemäß Artikel 13 DSGVO auf transparente und verständliche Weise zu informieren. Insbesondere bei der Erhebung der aktuellen Geschwindigkeit sollten die betroffenen Personen ausdrücklich über die Datenerhebung informiert werden. Da die Datenverarbeitung auf einer Einwilligung beruht, muss die betroffene Person ausdrücklich über sein Recht informiert werden, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Darüber hinaus ist die betroffene Person berechtigt, von ihrem Recht auf Datenübertragbarkeit Gebrauch zu machen, da die in diesem Zusammenhang erhobenen Daten von der betroffenen Person (durch bestimmte Formulare oder durch ihre Tätigkeit) zur Verfügung gestellt und auf der Grundlage des Artikels 6 Absatz 1 Buchstabe a DSGVO (Einwilligung) verarbeitet werden. Wie in den Leitlinien zum Recht auf Datenübertragbarkeit hervorgehoben, empfiehlt der EDSA nachdrücklich, „dass Verantwortliche klar und deutlich den Unterschied zwischen den verschiedenen Arten von Daten darlegen, die eine betroffene Person erhalten kann, wenn sie von ihrem Auskunftsrecht oder von ihrem Recht auf Datenübertragbarkeit Gebrauch macht“. Folglich sollte der Verantwortliche eine einfache Möglichkeit zur Verfügung stellen, die Einwilligung jederzeit und freiwillig zu widerrufen, und Instrumente entwickeln, um Anfragen zur Übertragbarkeit der Daten beantworten zu können.

158. Diese Informationen können bei der Unterzeichnung des Formulars zur Einwilligung in die Teilnahme an der Unfallforschungsstudie bereitgestellt werden.

### 3.3.5 Empfänger

159. Grundsätzlich haben nur der Verantwortliche und der Auftragsverarbeiter Zugriff auf die Daten.

### 3.3.6 Sicherheit

160. Wie vorstehend erwähnt, müssen die getroffenen Sicherheitsmaßnahmen an die Sensibilität der Daten angepasst werden. Wenn beispielsweise im Rahmen einer Unfallforschungsstudie die aktuelle Geschwindigkeit (oder andere Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten) erhoben wird, empfiehlt der EDSA dringend, strenge Sicherheitsmaßnahmen zu ergreifen, wie beispielsweise:

- Umsetzung von Maßnahmen zur Pseudonymisierung (z. B. Hashing von Daten mit geheimem Schlüssel wie dem Nachnamen/Vornamen der betroffenen Person und der Seriennummer);
- Speicherung von Daten zur aktuellen Geschwindigkeit und zum Standort in getrennten Datenbanken (z. B. unter Verwendung eines dem Stand der Technik entsprechenden Verschlüsselungsmechanismus mit unterschiedlichen Schlüsseln und Freigabeverfahren);
- und/oder Löschung von Standortdaten, sobald das Referenzereignis oder die Referenzsequenz näher bestimmt wurde (z. B. Art der Straße, Tag/Nacht), und Speicherung von direkt identifizierenden Daten in einer getrennten Datenbank, auf die nur eine kleine Anzahl von Personen zugreifen kann.

## 3.4 Vorgehen bei Autodiebstahl

161. Es kann sein, dass betroffene Personen im Falle eines Diebstahls versuchen möchten, ihr Fahrzeug anhand des Standorts zu finden. Die Verwendung von Standortdaten ist strikt auf die Ermittlungserfordernisse und auf die Fallbewertung durch die zuständigen Justizbehörden beschränkt.

### 3.4.1 Rechtsgrundlage

162. Wenn die Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst erhoben werden, gilt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation.

163. Da es sich um einen Dienst der Informationsgesellschaft handelt, verlangt Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation keine Einwilligung für den Zugriff auf bereits im Fahrzeug gespeicherte Informationen, wenn ein solcher Dienst vom Teilnehmer ausdrücklich angefordert wird.

164. In Bezug auf die Verarbeitung personenbezogener Daten ist die Rechtsgrundlage für die Verarbeitung der Standortdaten die Einwilligung des Fahrzeughalters oder gegebenenfalls die Erfüllung eines Vertrags (nur für Daten, die für die Erfüllung des Vertrags, dessen Vertragspartei der Fahrzeughalter ist, erforderlich sind).

165. Die Einwilligung muss eine freiwillig für den bestimmten Fall und in informierter Weise abgegebene Willensbekundung der Person sein, deren Daten verarbeitet werden (z. B. durch Ankreuzen eines Kästchens, das nicht vorab angekreuzt ist, oder durch die Konfiguration des Bordcomputers zur Aktivierung einer Funktion im Fahrzeug). Die Freiheit zur Erteilung einer Einwilligung beinhaltet die Möglichkeit, die Einwilligung jederzeit zu widerrufen, worüber die betroffene Person ausdrücklich informiert werden sollte. Der Widerruf der Einwilligung führt zur Einstellung der Verarbeitung. Die Daten sollten dann aus der aktiven Datenbank gelöscht, anonymisiert oder archiviert werden.

### 3.4.2 Erhobene Daten

166. Standortdaten können nur ab dem Zeitpunkt der Diebstahlmeldung übermittelt und in der restlichen Zeit nicht kontinuierlich erhoben werden.

### 3.4.3 Speicherfrist

167. Standortdaten können nur für den Zeitraum gespeichert werden, während dessen der Fall von den zuständigen Justizbehörden geprüft wird, oder bis zum Ende eines Verfahrens zur Ausräumung von Zweifeln, das nicht mit der Bestätigung des Diebstahls des Fahrzeugs endet.

### 3.4.4 Information der betroffenen Personen

168. Vor der Verarbeitung personenbezogener Daten sollte die betroffene Person gemäß Artikel 13 DSGVO auf transparente und verständliche Weise informiert werden. Insbesondere empfiehlt der EDSA, dass der Verantwortliche darauf hinweist, dass keine ständige Verfolgung des Fahrzeugs erfolgt und dass Standortdaten erst ab dem Zeitpunkt der Diebstahlmeldung erhoben und übermittelt werden können. Darüber hinaus muss der Verantwortliche die betroffene Person darüber informieren, dass nur zugelassene Mitarbeiter der Fernüberwachungsplattform und gesetzlich zugelassene Behörden Zugriff auf die Daten haben.

169. Im Hinblick auf die Rechte der betroffenen Personen sollten sie, sofern die Datenverarbeitung auf einer Einwilligung beruht, ausdrücklich über ihr Recht informiert werden, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Zudem ist die betroffene Person berechtigt, von ihrem Recht auf Datenübertragbarkeit Gebrauch zu machen, wenn die in diesem Zusammenhang erhobenen Daten von der betroffenen Person (durch bestimmte Formulare oder durch ihre Tätigkeit) zur Verfügung gestellt und auf der Grundlage des Artikels 6 Absatz 1 Buchstabe a (Einwilligung) oder Artikel 6 Absatz 1 Buchstabe b DSGVO (Erfüllung eines Vertrags) verarbeitet werden. Wie in den Leitlinien zum Recht auf Datenübertragbarkeit hervorgehoben, empfiehlt der EDSA nachdrücklich, „dass Verantwortliche klar und deutlich den Unterschied zwischen den verschiedenen Arten von Daten darlegen, die eine betroffene Person erhalten kann, wenn sie von ihrem Auskunftsrecht oder von ihrem Recht auf Datenübertragbarkeit Gebrauch macht“.

170. Folglich sollte der Verantwortliche eine einfache Möglichkeit zur Verfügung stellen, die Einwilligung jederzeit und freiwillig zu widerrufen (nur wenn die Einwilligung die Rechtsgrundlage ist), und Instrumente entwickeln, um Anfragen zur Übertragbarkeit der Daten beantworten zu können.

171. Die Information kann bei Vertragsunterzeichnung zur Verfügung gestellt werden.

### 3.4.5 Empfänger

172. Im Falle einer Diebstahlmeldung können die Standortdaten i) an zugelassene Mitarbeiter der Fernüberwachungsplattform und ii) an die gesetzlich zugelassenen Behörden weitergegeben werden.

### 3.4.6 Sicherheit

173. Es gelten die allgemeinen Empfehlungen. Siehe Abschnitt 2.7