Datensicherheit in autonomen Fahrzeugen

Technische und organisatorische Maßnahmen für Fahrzeughersteller

Julia Seufert, LL.M., ist als Wirtschaftsjuristin bei der Safetronics GmbH in Hofbieber tätig und befasst sich dort mit regulatorischen Anforderungen an Automotive Cyber Security und Datensicherheit.

■ Datensicherheit in Fahrzeugen ist bereits heute von zentraler Bedeutung und wird bei autonomen Fahrzeugen weiter zunehmen (I.). Um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau sicherzustellen, fordert die DS-GVO die Entwicklung und Implementierung von geeigneten technischen und organisatorischen Maßnahmen (II.1.). Im Anwendungsfall autonomer Fahrzeuge nimmt insbesondere der Fahrzeughersteller einen großen Einfluss auf die Datenverarbeitung und kann spezifische Maßnahmen implementieren (II.2.).

■ Data security in vehicles is already of central importance today and will become even more so with autonomous vehicles (I.). To ensure a level of protection appropriate to the risk of data processing, the GDPR requires the development and implementation of appropriate technical and organisational measures (II.1.). In the case of autonomous vehicles, the vehicle manufacturer has a great influence on data processing and can implement specific measures (II.2.).

Lesedauer: 21 Minuten

I. Einleitung

Autonome Fahrzeuge sind auf die Verarbeitung von Daten angewiesen, um den Fahrzeuginnenraum sowie das gesamte Umfeld des Fahrzeugs zu erfassen und sich selbstständig fortbewegen zu können.[1] In der Literatur sind hierzu umfassende Diskussionen um die Art der Daten entstanden, dh ob es sich um personenbezogene oder nicht-personenbezogene Daten handelt.[2] Denn diese Unterscheidung ist fundamental für die Anwendbarkeit des europäischen Datenschutzrechts.[3] Mehrheitlich wird die Meinung vertreten, iRv Big Data und dem Internet der Dinge sei in letzter Konsequenz immer ein Personenbezug möglich.[4] Daher könne auch bei Daten in autonomen Fahrzeugen im Zweifel stets von personenbezogenen Daten ausgegangen werden.[5] Nicht zuletzt der Verband der Automobilindustrie (VDA) und die Datenschutzaufsichtsbehörden sehen technische Fahrzeugdaten bereits dann vom Anwendungsbereich des Datenschutzrechts umfasst, wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer (FIN) oder dem KFZ-Kennzeichen möglich ist.[6] Vor diesem Hintergrund soll in diesem Beitrag auf eine erneute Darstellung des Anwendungsbereichs und die damit einhergehenden Vorschriften an den rechtlichen Datenschutz verzichtet werden.

Der Fokus liegt vielmehr auf dem technischen und organisatorischen Schutz von personenbezogenen Daten. Denn durch die umfassende Vernetzung, die neuen Schnittstellen und die zunehmende Datenverarbeitung steigt insbesondere die Anfälligkeit des Fahrzeugs für Cyberangriffe.[7] Da die Auswirkungen

möglicher Schäden durch einen Cyberangriff immens sein können, gewinnt die Datensicherheit in autonomen Fahrzeugen an signifikanter Bedeutung. Denn wird der Datenfluss gestört oder manipuliert, kann es zu rechtlichen Bedrohungen des Datenschutzes einerseits und zu technischen Bedrohungen der Fahrfunktion des Fahrzeugs und damit zur Gefährdung des Lebens der Insassen und der Menschen im Umfeld des Fahrzeugs andererseits kommen.[8]

II. Datensicherheit durch technische und organisatorische Maßnahmen

Datensicherheit stellt die Gesamtheit der technischen und organisatorischen Maßnahmen (TOMs) dar, durch welche die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten sichergestellt werden.[9] In Abgrenzung zum Datenschutz stellt Datensicherheit somit Anforderungen an das „wie" einer Datenverarbeitung, während Datenschutz auf das „ob" einer Datenverarbeitung abstellt.[10]

Auch die DS-GVO setzt neben dem rechtlichen Datenschutz (vgl. Art. 5 und 6 DS-GVO) auf einen technischen und organisatorischen Schutz iSv Datensicherheit.[11] Durch TOMs sollen die Anforderungen der DS-GVO wirksam umgesetzt und die Rechte der betroffenen Personen geschützt (Art. 25 Abs. 1 DS-GVO), datenschutzfreundliche Voreinstellungen vorgenommen (Art. 25 Abs. 2 DS-GVO) und eine sichere Datenverarbeitung gewährleistet werden (Art. 32 Abs. 1 DS-GVO). Der Gleichlauf der TOMs an unterschiedlicher Stelle der DS-GVO ist Ausdruck des risikobasierten Ansatzes des Datenschutzrechts.[12] Es bietet sich daher nicht nur an, die TOMs gemeinsam zu betrachten, sondern es ist zudem erforderlich, um ein sinnvolles Ergebnis und angemessenes Datenschutzniveau zu erreichen.[13]

1. Festlegung geeigneter Maßnahmen

Wie genau TOMs auszugestalten sind, konkretisiert die DS-GVO nicht.[14] Dies birgt zwar zunächst das Risiko der Rechtsunsicherheit bei dem Verantwortlichen.[15] Der europäische Gesetzgeber setzt jedoch auf technikneutrale Vorgaben und unbestimmte Rechtsbegriffe, um durch Dynamik und Anpassungsfähigkeit eine Vielzahl von Sachverhalten und zukünftige Entwicklungen zu erfassen.[16]

An die Maßnahmen stellt der Gesetzgeber insoweit Anforderungen, als die Maßnahmen geeignet sein müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.[17] Dabei können Maßnahmen bereits als geeignet gelten, welche das Ziel der sicheren Datenverarbeitung zumindest fördern.[18] Darüber hinaus misst sich die Geeignetheit von Maßnahmen am Risiko einer Verarbeitung.

a) Risikobegriff

Obwohl die DS-GVO einen risikobasierten Ansatz verfolgt, fehlt es an einer Definition des Risikobegriffs in der Verordnung.[19] Dies wäre iRd umfassenden Definitionskatalogs nach Art. 4 DS-GVO wünschenswert gewesen.[20] Ein Anhaltspunkt des Risikobegriffs ist in Erwägungsgrund 75 DS-GVO zu finden. Danach besteht ein Risiko für die Rechte und Freiheiten natürlicher Personen, wenn unter Berücksichtigung der Eintrittswahrscheinlichkeit und der Schwere ein physischer, materieller oder immaterieller Schaden aus einer Verarbeitung von personenbezogenen Daten hervorgehen kann. Aus Erwägungsgrund 75 DS-GVO und Art. 25 Abs. 1, 32 Abs. 1, 35 Abs. 3[21] DS-GVO lässt sich ein grobes Verständnis der DS-GVO von einem Risiko ableiten, nämlich das Verhältnis aus Eintrittswahrscheinlichkeit und Schadensausmaß.[22] Darüber hinaus obliegt es dem Anwender, das Risiko durch umfassende und individuelle Würdigung des Einzelfalls zu bestimmen.[23]

b) Abwägungskriterien

Bei der Festlegung der TOMs nach Art. 32 Abs. 1 und 25 Abs. 1 DS-GVO soll der Verantwortliche den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und den Zweck der Verarbeitung berücksichtigen. Mit diesen Abwägungskriterien verfolgt der Gesetzgeber die Intention, dass der Aufwand des Verantwortlichen zur Umsetzung einer Maßnahme in einem angemessenen Verhältnis zum Nutzen der Maßnahme steht.[24]

Bei dem Kriterium „Stand der Technik" handelt es sich um einen unbestimmten Rechtsbegriff, den die DS-GVO nicht weiter definiert.[25] Eine Begriffsdefinition auf europäischer Ebene verbietet den Rückgriff auf nationale Rechtsbegriffe[26] und fordert eine autonome Auslegung.[27] Hilfsweise kann auf andere europäische Regelungswerke zurückgegriffen werden. Das europäische Umweltrecht versteht unter „bester verfügbarer Technik" den „effizientesten und fortschrittlichsten Entwicklungsstand".[28] Danach wird einerseits auf einen hohen Sicherheitsstandard gesetzt und anderseits auf realistisch umsetzbare und verfügbare Verfahren.[29] In letzter Konsequenz wird sich der Stand der Technik stets an der Verfügbarkeit am Markt orientieren müssen.[30]

Neben dem Stand der Technik stehen die Maßnahmen unter der Berücksichtigung der Implementierungskosten. Die Implementierungskosten umfassen dabei alle Kosten, welche durch die Umsetzung der Maßnahmen entstehen. Dies sind insbesondere Anschaffungs- und Installationskosten. Streitig ist, ob auch Folgekosten wie Betriebs- und Wartungskosten umfasst sind.[31] Dies wird in der Literatur jedoch mehrheitlich verneint.[32] Bei der Berücksichtigung der Implementierungskosten wird zudem auf die Maßnahme selbst und nicht auf die finanziellen Mittel des Verantwortlichen abgestellt.[33] Das bedeutet, die Implementierungskosten müssen angemessen für die Maßnahmen und ihren Erfolg sein. Der Verantwortliche kann mangelnde Sicherheitsmaßnahmen nicht durch fehlende finanzielle oder personelle Mittel begründen.[34]

Bei der Festlegung der Maßnahmen sind die Art, der Umfang, die Umstände und der Zweck der Verarbeitung zu berücksichtigen. Bei der Art der Verarbeitung kann zB unterschieden werden, ob eine Verarbeitung lokal auf einem Computer oder dezentral in einer Cloud stattfindet,[35] oder ob Daten veröffentlicht werden.[36] Darüber hinaus könnte auch auf die Art der Daten abgestellt werden, zB ob es sich um sensible Daten nach Art. 9 DS-GVO handelt[37] oder Daten von Kindern verarbeitet werden.[38] Der Umfang der Verarbeitung bezieht sich auf die Menge der verarbeiteten Daten. Die massenhafte Datenverarbeitung, wie zB Profiling, kann ein erhöhtes Risiko für die betroffene Person darstellen, auch wenn die jeweiligen Daten einzeln betrachtet mit keinem hohen Risiko behaftet sind.[39] Die Umstände der Verarbeitung können einerseits auf die äußerlichen Rahmenbedingungen bezogen sein, zB auf globaler Ebene die aktuelle Cybersicherheitssituation oder auf Organisationsebene die Überarbeitung der Mitarbeiter.[40] Andererseits können die Umstände auch die Verarbeitung selbst betreffen, zB wenn sensible Daten verarbeitet oder besonders lange gespeichert werden.[41] Der Zweck der Verarbeitung ist im Hinblick auf die Rechtmäßigkeit iSv Art. 6 DS-GVO zu berücksichtigen. ZB muss bei sozialer Abhängigkeit oder Maßnahmen, die Grundrechte einschränken könnten, ein besonders enger Maßstab angesetzt werden.[42] Um die Art, den Umfang, die Umstände und den Zweck der Verarbeitung bei der Festlegung der Maßnahmen zu berücksichtigen, sollte auf das verpflichtende Verzeichnis von Verarbeitungstätigkeiten iSv Art. 30 DS-GVO zurückgegriffen werden.[43]

Die DS-GVO stellt auf die Berücksichtigung statt auf die verpflichtende Einhaltung der Kriterien ab.[44] In welchem Umfang Kriterien als berücksichtigt gelten, wird nicht weiter konkretisiert. Die Kriterien könnten als berücksichtigt gelten, wenn der Verantwortliche diese kennt, fachkundig bewertet und daraus möglichen Handlungsbedarf schlussfolgert.[45] Damit ist es dem Verantwortlichen erlaubt, den Stand der Technik planmäßig und begründet zu unterschreiten, da das Kriterium selbst keine Aussage über die Geeignetheit einer Maßnahme trifft.[46] Die Berücksichtigung der Kriterien, insbesondere des Stands der Technik und der Implementierungskosten, hat vielmehr eine begrenzende Funktion.[47] Die Berücksichtigung der Implementierungskosten erlaubt eine Wirtschaftlichkeitsbetrachtung, denn die Kosten einer Maßnahme und das Risiko einer Verarbeitung müssen in einem angemessenen Verhältnis

stehen.[48] Darüber hinaus kann vor dem Hintergrund der Berufsfreiheit iSd Art. 15 GRCh und der unternehmerischen Freiheit nach Art. 16 GRCh die Berücksichtigung der wirtschaftlichen Leistungsfähigkeit nicht gänzlich ausgeschlossen werden.[49]

c) Maßnahmen nach Art. 32 Abs. 1 Hs. 2 DS-GVO

In Art. 32 Abs. 1 Hs. 2 DS-GVO stellt der Gesetzgeber bereits einen Maßnahmenkatalog für die Sicherstellung eines angemessenen Schutzniveaus zur Verfügung.[50] Durch die enge Beziehung zu Art. 25 DS-GVO kann der Maßnahmenkatalog gleichermaßen zur Einhaltung dieser Vorschrift herangezogen werden.[51] Der Katalog beinhaltet Maßnahmen zur Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 Hs. 2 lit. a DS-GVO), zur dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 Hs. 2 lit. b DS-GVO), zur raschen Wiederherstellung der Verfügbarkeit von personenbezogenen Daten nach einem physischen oder technischen Zwischenfall (Art. 32 Abs. 1 Hs. 2 lit. c DS-GVO) und zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen (Art. 32 Abs. 1 Hs. 2 lit. d DS-GVO).

2. Technische und organisatorische Maßnahmen für autonome Fahrzeuge

Welche TOMs sich im Anwendungsfall von autonomen Fahrzeugen ergeben, ist abhängig von einer individuellen Risikoanalyse und Abwägungskriterien. Für den Fahrzeughersteller können andere Maßnahmen geeignet sein als für Verantwortliche

wie zB Werkstätten, Kommunikationsanbieter oder Versicherungsgesellschaften. Im Hinblick auf Datensicherheit spielt der Fahrzeughersteller eine zentrale Rolle, da er einerseits über Möglichkeiten verfügt, Datenschutz bereits im Entwicklungsstadium des Fahrzeugs zu berücksichtigen und er andererseits die tatsächliche Datenherrschaft über den größten Teil der Daten hat.[52] Daher werden nachfolgend Maßnahmen dargestellt, welche speziell aus der Perspektive des Fahrzeugherstellers geeignet sind. Die Festlegung der Maßnahmen orientiert sich zunächst an dem Maßnahmenkatalog nach Art. 32 Abs. 1 Hs. 2 DS-GVO. Sodann wird geprüft, ob darüberhinausgehende Maßnahmen geeignet sein können, um das Ziel eines angemessenen Schutzniveaus zu erreichen. Die Maßnahmen können dabei aus Technik, Organisation und der Kombination aus beiden bestehen.[53]

Das Schutzziel der Vertraulichkeit kann durch Pseudonymisierung und Verschlüsselung erreicht werden. Durch die Pseudonymisierung kann eine betroffene Person nicht mehr ohne das Hinzuziehen zusätzlicher Informationen identifiziert werden, Art. 4 Nr. 5 DS-GVO. Durch die Verschlüsselung sind Daten ohne einen entsprechenden Schlüssel zur „Entschlüsselung" nicht mehr lesbar und auf diese Weise vor einem unberechtigten Zugriff geschützt.[54] Um die Vertraulichkeit von Fahrzeugdaten sicherzustellen, sollten Signale innerhalb von Kommunikationskanälen verschlüsselt werden. Dies betrifft die Signale zwischen den Steuergeräten innerhalb des Fahrzeugs sowie die Signale vom Fahrzeug zur Außenwelt.[55] Verschlüsselungscodes sollten für jedes Fahrzeug – statt für Fahrzeugtypen – individuell gestaltet sein.[56] Außerdem sollte der Verschlüsselungscode regelmäßig erneuert werden. Zusätzlich sollten sich Datenempfangsgeräte authentifizieren müssen.[57]

Die Integrität der Daten kann durch Autorisierung und Zugriffsanforderungen geschützt werden.[58] Auch die Verschlüsselung dient neben dem Schutzziel der Vertraulichkeit der Integrität. Die Verschlüsselung kann einerseits vor dem unrechtmäßigen Löschen der Daten schützen und andererseits zum sicheren Löschen dienen, zB wenn der Zugangsschlüssel gelöscht wird.[59] Je

nach Datenkategorie ist die Kontrolle der Verarbeitung durch den Betroffenen notwendig, um die Richtigkeit der Daten zu prüfen. Dies kann zB durch Webportale, Apps oder das Infotainmentsystem ermöglicht werden. Jedoch ist auch hierbei die Vertraulichkeit zB durch Passwort-Authentifizierung oder Verschlüsselung der Daten sicherzustellen.60

Die Verfügbarkeit von Systemen, Diensten und Daten kann durch Backup-Systeme, regelmäßige Datensicherung, Redundanz und Notstromaggregate sichergestellt werden. Um im Falle eines Datenverlusts oder einer sonstigen Störung effizient zu handeln und eine Gefährdung abwenden zu können, sollte ein Notfallkonzept erstellt werden.61 Da autonome Fahrzeuge über Kommunikationskanäle und insbesondere eine Internetverbindung verfügen, sollten Denial-of-Service(DoS)-Angriffe auf das Fahrzeug als übliche Bedrohung berücksichtigt und das System entsprechend gehärtet werden.62

Der Belastbarkeit von Systemen kommt in autonomen Fahrzeugen eine besonderen Bedeutung zu.63 Um die Belastbarkeit des Datenverarbeitungssystems in autonomen Fahrzeugen zu erhöhen, sollten Fahrzeugfunktionen, welche durch lokale Datenverarbeitung möglich sind, von Funktionen getrennt werden, welche abhängig von der Telekommunikation sind, wie insbesondere das Infotainmentsystem.64 Das Entkoppeln der Steuergeräte vom Infotainmentsystem kann darüber hinaus auch der Vertraulichkeit, Integrität und Verfügbarkeit der Daten dienen, wenn auf diese Weise der Zugriff auf die Fahrzeugdaten nicht mehr über das Infotainmentsystem möglich ist.65 Bei Störungen oder Beeinträchtigungen muss das System in der Lage sein, einen risikominimalen Zustand zu erreichen.66 Dies könnte zB das Halten des Fahrzeugs auf dem Seitenstreifen sein.67 Der Fahrzeughersteller sollte kontinuierlich nach Sicherheitslücken forschen und die Möglichkeit haben, diese jederzeit zu schließen.68 Da die Belastbarkeit von Systemen auch zT der funktionalen Sicherheit zuzuordnen ist, sollte insbesondere der Standard ISO 26262 zur funktionalen Sicherheit in Fahrzeugen berücksichtigt werden.

Die Wirksamkeit der Maßnahmen muss regelmäßig überprüft, bewertet und evaluiert werden. Dies kann durch die Analyse neuer Angriffspfade erzielt werden, sowie durch Penetrationstests69 oder interne Audits.70 Neben solchen technischen Maßnahmen sollten zudem auch organisatorische Maßnahmen vorgesehen werden. Durch die Definition eines Überprüfungsprozesses und eine regelmäßige Versionsverwaltung der Fahrzeugsoftware können Systemverbesserungen identifiziert und umgesetzt werden. Auf diese Weise kann gleichzeitig Transparenz gegenüber dem Nutzer sichergestellt werden.71 Durch die regelmäßige Überprüfung der Maßnahmen können zudem Kosten ggf. gesenkt, zB durch die Vermeidung von Iterationen in der Implementierung, und Maßnahmen an den Stand der Technik angepasst werden.72

Da der Maßnahmenkatalog nach Art. 32 Abs. 1 DS-GVO als beispielhaft und nicht abschließend betrachtet werden muss, können weitere Maßnahmen geeignet sein, um ein angemessenes Schutzniveau sicherzustellen. Im Hinblick auf autonome Fahrzeuge empfehlen sich insbesondere die im Folgenden genannten Maßnahmen.

Es sollte stets eine lokale Datenverarbeitung gegenüber einer Verarbeitung in der Cloud oder einem Datentransfer bevorzugt werden.73 Dadurch bleiben Daten im Kontrollbereich des Betroffenen.74 In den Fällen, in denen keine lokale Datenverarbeitung möglich ist, sollte die Maßnahme der sog. „Datenaggregation" vorgenommen werden. Das bedeutet, auf lokaler Ebene werden Datensummen gebildet und lediglich Ergebnisse übermittelt. Durch die Datenaggregation können Daten zudem anonymisiert werden, wenn die Datensummen groß genug sind, dass kein Datum einer einzelnen Person zugeordnet werden kann.75 Durch die Datenaggregation lässt sich

auf lokaler Ebene die Menge kritischer Daten reduzieren, die das Fahrzeug und damit den Kontrollbereich des Betroffenen verlassen.[76] Insbesondere Standortdaten sollten lokal verarbeitet werden, um die Gefährdung des unrechtmäßigen Erstellens von Bewegungsprofilen zu minimieren. Auch wenn die lokale Datenverarbeitung als sicherer gegenüber einer Verarbeitung in der Cloud oder in einem Backend-Server des Fahrzeugherstellers gilt, sind Maßnahmen der Zugriffskontrolle und Verschlüsselung notwendig, da die physikalische Bedrohung der Daten latent gegeben ist.[77]

Da das autonome Fahrzeug eine große Datenmenge verarbeiten muss, wird es mit der Zeit an physische Grenzen stoßen, und Daten müssen hilfsweise in der Cloud oder im Backend des Fahrzeugherstellers verarbeitet werden.[78] Daher sind Maßnahmen zur Einhaltung des Grundsatzes der Datensparsamkeit besonders bei autonomen Fahrzeugen essenziell.[79] Die Datensparsamkeit kann dabei durch Datenanonymisierung und -aggregation sichergestellt werden. Die Datenanonymisierung ist für die betroffene Person wünschenswert, da sie nicht mehr identifiziert werden kann. Gleichzeitig ist die Anonymisierung auch für den Verantwortlichen vorteilhaft, da es sich bei anonymisierten Daten nicht mehr um personenbezogene Daten handelt und die strengen Vorschriften der DS-GVO nicht länger anwendbar sind.[80] Im Hinblick auf Standortdaten ist zu prüfen, zu welchem Zeitpunkt die Erhebung notwendig ist. ZB könnte ein Gyroskop verwendet werden, um Bewegungen eines Fahrzeugs zu erfassen.[81] Ist die Standorterfassung notwendig, sollte geprüft werden, ob die exakte Position erforderlich ist oder ob eine Abstraktion, zB durch die Erfassung der Position in Quadranten, ausreicht, um zu bestimmen, an welchem Ort sich das Fahrzeug aufhält.[82]

Weitere Maßnahmen, die der Datensparsamkeit dienen, sind eine begrenzte Speicherdauer und ein automatisiertes Löschkonzept. Es ist zu prüfen, wann die Speicherung und das Auslesen von personenbezogenen Daten notwendig ist. Sofern die Momentaufnahme von Daten ausreicht, zB zur Erkennung anderer Verkehrsteilnehmer über Bilderfassung, sollten die Daten unmittelbar nach der Auswertung wieder überschrieben werden.[83] Durch ein automatisiertes Löschkonzept[84] kann sichergestellt werden, dass Daten nur für einen begrenzten Zeitraum gespeichert werden.[85] ZB könnten Daten automatisch gelöscht werden, wenn ein bestimmter Sensor aktiviert wird, etwa das Öffnen der Fahrertür.[86] Darüber hinaus sollte der Nutzer die Möglichkeit haben, nicht erforderliche Daten dauerhaft zu löschen, insbesondere vor dem Verkauf des Fahrzeugs.[87] Diese Maßnahme dient ebenfalls dem Schutzziel der Vertraulichkeit von Daten.

Der Betroffene sollte jederzeit die Möglichkeit haben, die Datenverarbeitung zu überwachen.[88] Hierzu muss der Betroffene umfassend über Zweck und Umfang der Datenerhebung, die Speicherdauer sowie die Weitergabe der Daten informiert werden.[89] Transparenz[90] über die Datenverarbeitungen sollte in der Art umgesetzt werden, dass der Betroffene in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache informiert wird.[91] Hierfür sollte eine verständliche Borddokumentation, zB iRd Betriebsanleitung, zur Verfügung stehen, die Aufschluss über die erhobenen Daten und die Verarbeitungsvorgänge gibt.[92] Zusätzlich sollten Dialoge, Symbole und Pop-up-Fenster im Infotainmentsystem verwendet werden.[93] ZB sollte der Betroffene durch Symbole im Infotainmentsystem darüber informiert werden, wann die Funktion der Standorterfassung aktiviert ist.[94]

Die o.g. Maßnahmen orientieren sich einerseits an einer effizienten Umsetzung datenschutzrechtlicher Vorgaben durch den Fahrzeughersteller und andererseits an einem effektiven Grund-

rechtschutz des Nutzers autonomer Fahrzeuge. Dabei sollten die Maßnahmen nicht als abschließend, sondern als fundamental betrachtet werden, welche auf individuelle Einzelfälle angepasst und ergänzt werden sollten.

III. Zusammenfassung und Ausblick

Zentrales Instrument zur Umsetzung der Anforderungen an Datensicherheit sind TOMs. Dabei verfolgt die DS-GVO einen risikobasierten Ansatz. Es muss demnach kein absolutes Schutzniveau gewährleistet werden, sondern ein dem Risiko der Verarbeitung angemessenes Schutzniveau.

Für den Hersteller autonomer Fahrzeuge ergeben sich insbesondere technische Maßnahmen wie die Pseudonymisierung, Anonymisierung und Aggregation von personenbezogenen Daten. Außerdem sollten für die Fahrfunktion notwendige Steuergeräte von Kommunikationskanälen und -schnittstellen wie zB dem Infotainmentsystem entkoppelt sein. Auf diese Weise werden vom Fahrzeug generierte Daten, wie etwa Standortdaten, vor unbefugtem Zugriff über das Infotainmentsystem geschützt und die Fahrfunktion des Fahrzeugs gesichert. Darüber hinaus sollte stets eine lokale Verarbeitung einer Verarbeitung der Daten in der Cloud und einem Datentransfer vorgezogen werden. Bei jeder Verarbeitung kommt der Datensparsamkeit sowie der Transparenz der Verarbeitung gegenüber dem Nutzer des Fahrzeugs eine besondere Bedeutung zu.

Zukünftig wird das Gefährdungspotenzial von Cyberangriffen nicht nur durch fortschreitende Automatisierung, Vernetzung und Digitalisierung erhöht, sondern vor dem Hintergrund zunehmender Datenregulierung, wie insbesondere iRd Data Act, außerdem durch Datenzugangs- und -portabilitätsrechte verschärft. Denn die rechtliche und technische Ausgestaltung des Datenzugangs und der Datennutzung – zB über Schnittstellen am Fahrzeug selbst (sog. In-Vehicle-Zugriff) oder im Backend-Server des Fahrzeugherstellers – wird zentralen Einfluss auf das Risiko einer Datenverarbeitung und damit auf datensicherheitsrechtliche Anforderungen haben.

Schnell gelesen …

■ Datensicherheit erfordert technische und organisatorische Maßnahmen, die nach der DS-GVO einerseits von dem Risiko einer Verarbeitung und andererseits von Abwägungskriterien abhängig sind.

■ Für den Fahrzeughersteller sind insbesondere technische Maßnahmen wie die Pseudonymisierung, Anonymisierung und Aggregation von personenbezogenen Daten von besonderer Bedeutung sowie die Entkopplung der für die Fahrfunktion notwendigen Steuergeräte von Kommunikationskanälen und -schnittstellen.

■ Über die Datensicherheit hinaus kommt der Datensparsamkeit sowie der Transparenz der Verarbeitung von Fahrzeugdaten gegenüber dem Betroffenen eine grundsätzliche Bedeutung zu.

Julia Seufert, LL.M.,
ist als Wirtschaftsjuristin bei der Safetronics GmbH in Hofbieber tätig und befasst sich dort mit regulatorischen Anforderungen an Automotive Cyber Security und Datensicherheit.

---

1 Ebers/Heinze/Krügel/Steinrötter, KI und Robotik/Niederée/Nejdl, 2020, § 2 Rn. 139.

2 S. zB Weichert NZV 2017, 507; Klink-Straub/Straub NJW 2018, 3201; Steege MMR 2019, 509.

3 S. hierzu vertiefend Oppermann/Stender-Vorwachs, Autonomes Fahren/Forgó, 2. Aufl. 2020, Kap. 3.5 Rn. 12 ff.

4 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 6; Buchner DuD 2015, 372 (374); Ebers/Heinze/Krügel/Steinrötter, KI und Robotik/Krügel/Pfeiffenbring, 2020, § 11 Rn. 15; Chibanguza/Kuß/Steege, KI/Steege/Stender-Vorwachs, 2022, § 3 K. Rn. 9.

5 Steinrötter ZD 2021, 513; Metzger GRUR 2019, 129 (131); im Ergebnis ähnl. Chibanguza/Kuß/Steege, KI/Steege/Stender-Vorwachs, 2022, § 3 K. Rn. 11; Klink-Straub/Straub NJW 2018, 3201 (3203).

6 VDA, Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), abrufbar unter: https://www.vda.de/de/themen/digitalisierung/daten/datenschutz.

7 Teichmann/Falker CCZ 2020, 89 (90); Ensthaler/Gollrad, Rechtsgrundlagen des automatisierten Fahrens, 2019, S. 132; für Beispiele aus der Praxis s. Lüdemann ZD 2015, 247 (250) mwN; Hemker/Mischkovsky DuD 2017, 233 (235).

8 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 50.

9 Roßnagel, Das neue Datenschutzrecht/Husemann, 2018, § 5 IV Rn. 33; Sassenberg/Faber, Industrie 4.0 und IoT/Mantz/Spittka, 2. Aufl. 2020, § 6 Rn. 147.

10 Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 1b.

11 Gola/Heckmann, DS-GVO – BDSG/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 1, 2.

12 Kühling/Buchner, DS-GVO BDSG/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 19.

13 Kühling/Buchner, DS-GVO BDSG/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 19; Sydow, Europäische Datenschutzgrundverordnung/Mantz, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 6, 83; im Ergebnis ähnl. Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 25 Rn. 38.

14 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/Krätschmer, 2019, § 6 Rn. 14.

15 Bieker/Hansen DuD 2017, 285 mwN.

16 Hofmann, Dynamische Zertifizierung, 2019, S. 32; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hansen, 2019, DSGVO Art. 32 Rn. 20; Gola, DS-GVO/Piltz, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 3.

17 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/Krätschmer, 2019, § 6 Rn. 14.

18 Kühling/Buchner, DS-GVO BDSG/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 5; ähnl. Schläger/Thode, HdB Datenschutz und IT-Sicherheit/Schläger, 2018, S. 478 Rn. 9; Eisenberg InTeR 2021, 17 (20).

19 Ritter/Reibach/Lee ZD 2019, 531; Alt DS 2020, 169.

20 Beck/Kusche/Valerius, Digitalisierung, Automatisierung, KI und Recht/Vogel, 2020, S. 653.

21 Art. 35 Abs. 3 DS-GVO nennt beispielhaft Verarbeitungen, bei denen ein hohes Risiko vorliegt und daher eine Datenschutz-Folgenabschätzung erforderlich ist, Ritter/Reibach/Lee ZD 2019, 531.

22 Ritter/Reibach/Lee ZD 2019, 531.

23 In der Lit. haben sich hierzu mehrere Ansätze entwickelt, vgl. zB Ritter/Reibach/Lee ZD 2019, 531; Beck/Kusche/Valerius, Digitalisierung, Automatisierung, KI und Recht/Vogel, 2020, S. 654; Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 25 Rn. 50; Bieker/Bremert/Hansen DuD 2018, 492 (493 f.).

24 Gola, DS-GVO/Nolte/Werkmeister, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 22.

25 Johannes/Geminn InTeR 2021, 140 (142).

26 Auf nationaler Ebene ist der Stand der Technik zwischen den „allgemein anerkannten Regeln der Technik" als Mindestmaß und dem „Stand von Wissenschaft und Technik" als Höchstmaß einzuordnen, s. vertiefender Roßnagel, Das neue Datenschutzrecht/Husemann, 2018, § 5 Abs. 2 Rn. 50 mwN; Johannes/Geminn InTeR 2021, 140 (142).

27 Hofmann/Johannes ZD 2017, 221; Roßnagel, Das neue Datenschutzrecht/Husemann, 2018, § 5 Abs. 2 Rn. 48; Gola, DS-GVO/Piltz, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 15.

28 RL (EU) 2010/75 Art. 3 Nr. 10; Roßnagel, Das neue Datenschutzrecht/Husemann, 2018, § 5 Abs. 2 Rn. 49.

29 Gola, DS-GVO/Nolte/Werkmeister, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 23; Baumgartner/Gausling ZD 2017, 308 (310).

30 Gola, DS-GVO/Piltz, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 19; Roßnagel, Das neue Datenschutzrecht/Husemann, 2018, § 5 Abs. 2 Rn. 53; Bartels/Backer DuD 2018, 214 (216).

31 Bejahend Schläger/Thode, HdB Datenschutz und IT-Sicherheit/Schläger, 2018, S. 479 Rn. 15; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Petri, 2019, DSGVO Art. 24 Rn. 12; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hansen, 2019, DSGVO Art. 25 Rn. 26.

32 Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/Keber/Keppeler, 2. Aufl. 2020, DS-GVO Art. 25 Rn. 48; Sydow, Europäische Datenschutzgrundverordnung/Mantz, 2. Aufl. 2018, DSGVO Art. 25 Rn. 45; Johannes/Geminn InTeR 2021, 140 (144); im Ergebnis ähnl. Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 25 Rn. 59.

33 Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 42; Baumgartner/Gausling ZD 2017, 308 (310); Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 25 Rn. 60.

34 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hansen, 2019, DSGVO Art. 25 Rn. 26.

35 Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/Ritter, 2. Aufl. 2020, DS-GVO Art. 32 Rn. 86.

36 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Petri, 2019, DSGVO Art. 24 Rn. 12.

37 Kühling/Buchner, DS-GVO BDSG/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 12; Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/Mantz/Marosi, 2019, § 3 Rn. 158.

38 Johannes/Geminn InTeR 2021, 140 (142).

39 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Petri, 2019, DSGVO Art. 24 Rn. 12.

40 Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/Ritter, 2. Aufl. 2020, DS-GVO Art. 32 Rn. 88.

41 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Petri, 2019, DSGVO Art. 24 Rn. 12.

42 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Petri, 2019, DSGVO Art. 24 Rn. 12.

43 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Petri, 2019, DSGVO Art. 24 Rn. 11; Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht/Sattler, 2021, S. 216.

44 Gola, DS-GVO/Piltz, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 14.

45 Bartels/Backer DuD 2018, 214 (219).

46 Bartels/Backer DuD 2018, 214 (219); ähnl. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hansen, 2019, DSGVO Art. 32 Rn. 24; Johannes/Geminn InTeR 2021, 140 (143); Gola, DS-GVO/Piltz, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 14.

47 Kühling/Buchner, DS-GVO BDSG/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 10; Baumgartner/Gausling ZD 2017, 308 (310); ähnl. Schläger/Thode, HdB Datenschutz und IT-Sicherheit/Schläger, 2018, S. 481 Rn. 21.

48 Kühling/Buchner, DS-GVO BDSG/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 11; Johannes/Geminn InTeR 2021, 140 (144); Kipker/Barudi, Cybersecurity/Voßkamp, 2020, Kap. 5 Rn. 25.

49 Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 25 Rn. 60; Johannes/Geminn InTeR 2021, 140 (144).

50 Missverständlich ist, ob es sich bei dem Maßnahmenkatalog um ein verpflichtendes Mindestschutzniveau oder um beispielhafte Maßnahmen handelt. Als verpflichtendes Mindestschutzniveau sehen es Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 32; Voigt, IT-Sicherheitsrecht, 2018, S. 129; Bartels/Backer DuD 2018, 214 (216); als beispielshaften Maßnahmenkatalog sehen es Gola, DS-GVO/Piltz, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 24; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hansen, 2019, DSGVO Art. 32 Rn. 31; ähnl. Sydow, Europäische Datenschutzgrundverordnung/Mantz, 2. Aufl. 2018, DSGVO Art. 32 Rn 9; Kühling/Buchner, DS-GVO BDSG/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 14.

51 Kühling/Buchner, DS-GVO BDSG/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 15; Baumgartner/Gausling ZD 2017, 308 (310).

52 Weichert NZV 2017, 507 (512); Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 20; Reiter DAR 2022, 123 (124).

53 Eine trennscharfe Zuordnung der Maßnahmen in TOMs ist häufig nicht möglich und im Hinblick auf den Regelungszweck nicht nötig, da auch die DS-GVO lediglich auf die Eignung der Maßnahmen abstellt, Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, DSGVO Art. 25 Rn. 36.

54 Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 34.

55 Roßnagel/Hornung, Grundrechtsschutz im Smart Car/Krauß, 2019, S. 239.

56 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 28 Rn. 93.

57 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 28 Rn. 93.

58 Europäischer Datenschutzausschuss, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, v. 20.10.2020, abrufbar unter: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf, S. 13 Rn. 45.

59 Roßnagel/Hornung, Grundrechtsschutz im Smart Car/Krauß, 2019, S. 239.

60 Sörup/Marquardt ZD 2015, 310 (313).

61 Voigt, IT-Sicherheitsrecht, 2018, S. 128.

62 European Union Agency for Cybersecurity (ENISA), 13.1.2017, Cyber Security and Resilience of smart cars. Good practices and recommendations, abrufbar unter: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/@@download/fullReport, S. 54; zur Anfälligkeit für DoS-Angriffe auch Hornung/Schallbruch, IT-Sicherheitsrecht/Geminn/Müller, 2021, § 22 Rn. 50.

63 Ebers/Heinze/Krügel/Steinrötter, KI und Robotik/Niederée/Nejdl, 2020, § 2 Rn. 142.

64 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und

mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 23 Rn. 75; ähnl. Rieß/Greß DuD 2015, 391 (393).

65 Stender-Vorwachs/Steege MMR 2018, 212; Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 51.

66 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hansen, 2019, DSGVO Art. 32 Rn. 45: „Fail-Safe-Modus".

67 Buck-Heeb/Dieckmann NZV 2019, 113 (116); Hermann/Knauff, Autonomes Fahren/Knoepffler, 2021, S. 14.

68 Vgl. Erwägungsgrund 78 DS-GVO.

69 Gabel/Heinrich/Kiefner, Rechtshandbuch Cyber-Security/Gabel, 2019, Kap. 4 S. 97; Esser/Kramer/von Lewinski, DSGVO, BDSG/Kramer/Meints, 7. Aufl. 2020, DSGVO Art. 32 Rn. 35; Rieß/Greß DuD 2015, 391 (393); Poncza ZD 2023, 8.

70 Voigt, IT-Sicherheitsrecht, 2018, S. 129.

71 Vásquez DuD 2022, 98 (101).

72 Vásquez DuD 2022, 98 (101); Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht/Sattler, 2021, S. 237.

73 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 43.

74 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 22 Rn. 73.

75 Oppermann/Stender-Vorwachs, Autonomes Fahren/Forgó, 2. Aufl. 2020, Kap. 3.5 Rn. 19.

76 Roßnagel/Hornung, Grundrechtsschutz im Smart Car/Krauß, 2019, S. 239.

77 Roßnagel/Hornung, Grundrechtsschutz im Smart Car/Krauß, 2019, S. 239.

78 Lüdemann ZD 2015, 247 (249).

79 Zwar ist das Prinzip der Datensparsamkeit nicht der technischen und organisatorischen Datensicherheit zuzuordnen, soll jedoch dennoch als Maßnahme erläutert werden, da die Datensparsamkeit bereits durch die Gestaltung der technischen Systeme (sog. technischer Datenschutz) wirksam umgesetzt werden kann, vgl. Gola/Heckmann, DS-GVO – BDSG/Pötters, 3. Aufl. 2022, DS-GVO Art. 5 Rn. 24; Taeger/Gabel, DSGVO – BDSG – TTDSG/Voigt, 4. Aufl. 2022, DSGVO Art. 5 Rn. 29; ähnl. Ehmann/Selmayr, DS-GVO/Heberlein, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 23.

80 Vgl. Erwägungsgrund 26 DS-GVO.

81 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 19 Rn. 63.

82 Roßnagel/Hornung, Grundrechtsschutz im Smart Car/Krauß, 2019, S. 240.

83 Oppermann/Stender-Vorwachs, Autonomes Fahren/Forgó, 2. Aufl. 2020, Kap.3.5 Rn. 20; Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 43; Buchner DuD 2015, 372 (374).

84 Maurer/Gerdes/Lenz/Winner, Autonomes Fahren/Rannenberg, 2015, S. 534.

85 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/Mantz/Marosi, 2019, § 3 Rn. 161; ähnl. zum Speicherkonzept Buchner DuD 2015, 372 (374).

86 Rieß/Greß DuD 2015, 391 (394).

87 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 23 Rn. 23.

88 Vgl. Erwägungsgrund 78 DS-GVO.

89 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 25 Rn. 84.

90 Ähnl. zum Prinzip der Datensparsamkeit gilt das Prinzip der Transparenz nicht als Teil der Datensicherheit, kann jedoch durch Technikgestaltung bereits frühzeitig von dem Fahrzeughersteller implementiert werden, vgl. Gola/Heckmann, DS-GVO – BDSG/Pötters, 3. Aufl. 2022, DS-GVO Art. 5 Rn. 24; Taeger/Gabel, DSGVO – BDSG – TTDSG/Voigt, 4. Aufl. 2022, DSGVO Art. 5 Rn. 29; ähnl. Ehmann/Selmayr, DS-GVO/Heberlein, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 23.

91 Vgl. Art. 12 DS-GVO.

92 Specht-Riemenschneider/Mantz, Europäisches und deutsches Datenschutzrecht/von Bodungen, 2019, § 16 Rn. 48; Rieß/Greß DuD 2015, 391 (394).

93 Gola, DS-GVO/Nolte/Werkmeister, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 16.

94 Europäischer Datenschutzausschuss, 9.3.2021, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf, S. 19 Rn. 64.