Anhang

Entwicklung eines Konzepts und Lastenheftes für eine Szenariendatenbank zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen

Berichte der Bundesanstalt
für Straßenwesen
Fahrzeugtechnik Heft F 156

bast
Bundesanstalt für
Straßenwesen

Anhang:

A1: Praktische Hürden und Handlungsempfehlungen aus rechtlicher Sicht

A2: Analyse der rechtlichen Rahmenbedingungen und Ableitung praktischer Handlungsempfehlungen

A3: Rollenmodell und Betriebsarchitektur einer AD/ADAS Szenariendatenbank

A4: Lastenheft für die kooperative Szenariendatenbank

A1: Praktische Hürden und Handlungsempfehlungen aus rechtlicher Sicht

Im Rahmen des Projekts „Entwicklung eines Konzepts und Lastenhefts für eine Szenariendatenbank zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen“ forscht das IKEM im Auftrag der Bundesanstalt für Straßenwesen zum rechtlichen Rahmen der Konzeptionierung einer solchen Szenariendatenbank, ermittelte rechtliche Hürden und leitete praktische Handlungsvorgaben ab. Die ausführliche wissenschaftliche Begutachtung und Erörterung der Empfehlungen findet sich in dem in diesem Zusammenhang erstellten Rechtsgutachten.

Rechtliche Hürden

Wesentliche rechtliche Hindernisse und Erschwernisse bei der Umsetzung einer zentralen Fusionierung einer großen Datenmenge ergeben sich aus dem Datenschutzrecht.

Das durch die unzureichende Harmonisierung bedingte, komplexe Zusammenspiel verschiedener Datenschutzregelungen auf europäischer und nationaler Ebene (in Form des Bundesdatenschutzgesetzes und der Datenschutzgesetze der Länder) sowie gegebenenfalls bereichsspezifische Vorschriften schaffen allgemeine Rechts- und damit Planungsunsicherheit für alle Beteiligten an innovativen Datenkonzepten. Dies wird verstärkt durch den zuweilen hohen Abstraktionsgrad der Regelungen, insbesondere der Datenschutzgrundverordnung (DSGVO), widersprüchlichen Vorgaben der verschiedenen Regelungsmaxime sowie fehlenden Hilfestellungen für die Konkretisierung und Ausfüllung datenschutzrechtlicher Vorgaben (welche Kriterien sind für die Privilegierung von Forschungsdaten erforderlich? Wann liegt echte Anonymisierung vor?) Rechtsprechung existiert, auch aufgrund der Neuartigkeit der DSGVO, nur punktuell für Einzelfälle und kann schwer übertragen und antizipiert werden. Gerade im Bereich der Forschung bestehen mit Blick auf innovative Datenkonzepte viele Unklarheiten. Darüber hinaus besteht aufgrund der Rechenschafts-, Auskunfts- und Nachweispflichten der Verantwortlichen ein enormer Dokumentationsaufwand, gerade mit Blick auf die in der Forschungspraxis besonders relevanten Interessenabwägungen und die Darlegung der Erfüllung der Forschungsdatenprivilegien (Forschungskonzept, wissenschaftliche Methodik, Ergebnispublikation usw.). Demgegenüber drohen bei DSGVO-Verstößen beträchtliche Schadensersatzforderungen und die Verhängung hoher Bußgelder.

Daneben erschweren fehlende konkrete Vorgaben mit Blick auf IT-Sicherheit und eine fehlende Rechtsform, speziell für Forschungskooperationen die Umsetzung einer Forschungsdatenbank.

Handlungsempfehlungen

Praktische Handlungsvorgaben ohne regulatorische Anpassungen

1. Die Gewährleistung von Authentizität, Vertraulichkeit, Qualität und Integrität der verwendeten Datensätze (und Prozesse) ist von Anfang an mitzudenken, um straf- und haftungsrechtlichen Risiken einzudämmen. Gesetzliche Vorgaben und Standards, welche als Orientierung herangezogen werden könnten, fehlen - maßgebend ist daher der aktuelle Stand der Wissenschaft und Forschung.

2. In die Datenbank sollten so wenig personenbezogene Daten wie möglich übertragen werden, was vertraglich mit den verschiedenen Datenlieferanten sichergestellt werden sollte. Dies kann einerseits durch die bevorzugte Anforderung von nicht-personenbezogenen Daten von den Datenlieferanten erfolgen, soweit diese einen ausreichenden Informationsgehalt für den Verarbeitungszweck aufweisen. Daneben können die Datenlieferanten zur Aufhebung des Personenbezugs mittels Aggregierung bzw. Synthetisierung der Rohdaten oder zur Anonymisierung im Wege der Löschung sämtlicher potenzieller Identifikatoren durch *Blurring* o.Ä. verpflichtet werden. Auch an dieser Stelle gilt es zu beachten, dass die Anonymisierung unter Umständen den Informationsgehalt mit Blick auf den Verarbeitungszeck mindert.

3. Hilfsweise (falls dennoch personenbezogene Daten in Datenbank einfließen) sollten die Datenverarbeitungsprozesse DSGVO-konform ausgestaltet werden. Praktisch relevante Rechtfertigungstatbestände mit Blick auf die in die Datenbank eingespeisten Forschungsdaten sind:

   a. Freiwillige informierte und bestimmte Einwilligung

   Sinnvoll wäre es, bei sämtlichen vertraglich vorgesehenen Verarbeitungen personenbezogener Daten, welche für die Datenbank relevant sind in dem jeweiligen Rechtsverhältnis neben der vertragsspezifischen Einwilligung auch eine Einwilligung zur nachträglichen Nutzung zu Forschungszwecken einzuholen. Aufgrund der Widerrufbarkeit der Einwilligung sollte die Verarbeitung sicherheitshalber auch auf Grundlage einer weiteren Rechtfertigungsgrundlage erfolgen. Zu beachten ist in dem Zusammenhang, dass eine (widerrufene) Einwilligung unter Umständen den Rückgriff auf eine gesetzliche Rechtfertigungsgrundlage verbauen kann, wenn in der betroffenen Person das (schutzwürdige) Vertrauen geweckt wurde, dass die Datenverarbeitung nur im Rahmen der Einwilligung erfolgt. Aus diesem Grund ist ein Hinweis sinnvoll, dass die Daten auch nach Wegfallen der Einwilligung auf anderer Grundlage verarbeitet werden können.

   b. Erforderlichkeit zur Vertragserfüllung

   Mit Blick auf neuartige Geschäftsmodelle, gerichtet auf den Fahrzeugerwerb oder fahrzeugbezogene Leistungen kann die Verarbeitung personenbezogener Daten in bestimmten Fällen auch zur Vertragserfüllung

erforderlich und somit gerechtfertigt sein, etwa wenn die Datenverarbeitung als solche erst die Fahrfunktion ermöglicht.

c. Interessenabwägung

Auf die Rechtfertigung auf Grundlage einer Interessenabwägung kann durch die Ergreifung verschiedener Maßnahmen zugunsten des Datenverarbeitenden eingewirkt werden, mit der Folge, dass die Datenverarbeitung gerechtfertigt ist. Denkbar sind beispielsweise die effiziente Durchsetzung der Datensparsamkeit, das Pseudonymisieren der Daten, das Einbeziehen zusätzlicher Kontrollmaßnahmen (unabhängige Überwachungsinstanzen),die Einbindung von Datentreuhändern sowie das Vorsehen einer besonders engen Zweckbindung und einer besonders kurzen Verarbeitungsdauer.

4. Sämtliche Verarbeitungs-/ Informations-/ und Abwägungsprozesse sind zudem umfassend zu dokumentieren um Betroffenenrechten und Nachweispflichten (beispielsweise zwecks Exkulpation gemäß Art 82 DSGVO)nachkommen zu können. Daneben empfiehlt sich, wenn nicht ohnehin die Verpflichtung greift, die freiwillige Bestellung eines Datenschutzbeauftragten gemäß Art. 37 Abs. 4 S. 1 DSGVO.

5. Bei der Delegierung datenschutzrechtlicher Pflichten an Auftragsverarbeitende ist die Dokumentation der Einhaltung verbleibender Organisations- und Aufsichtspflichten sicherzustellen, um den Nachweis des fehlenden Verschuldens erbringen zu können.

6. Der Verantwortliche sollte durch ein entsprechendes Schutzkonzept die eigenverantwortliche Einhaltung der Löschpflicht gemäß Art 17 DSGVO (insbesondere bei widerrufener Einwilligung, Zweckfortfall und unrechtmäßiger Datenverarbeitung) sicherstellen.

7. Daneben sollte die datenschutzrechtliche Privilegierung von Forschungsdaten (mit Blick auf Zweckbindung und Speicherbegrenzung) genutzt werden. Daneben sollte die datenschutzrechtliche Privilegierung von Forschungsdaten (mit Blick auf Zweckbindung und Speicherbegrenzung) genutzt werden. Das Konzept des Forschungsvorhabens (insbesondere Fragestellung, Verantwortlichkeiten, herangezogene Datenarten, ggf. Abwägungsgründe, Methodik, Gemeinschaftsnutzen und die Veröffentlichung der wesentlichen Ergebnisse)und das Ergreifen geeigneter Garantien gemäß Art 89 Abs. 1 und Abs. 2 DSGVO sollte transparent dargestellt werden. Wenn die Datenbank privat betrieben wird, ist darauf zu achten, dass die rein kommerzieller Nutzung und der Bereich der Forschung und Entwicklung voneinander getrennt sind, sodass sich das Aufziehen einer ausgelagerten Forschungsdatenbank empfiehlt. Bei privater Finanzierung und/oder der Verfolgung privater Eigeninteressen oder politischer Interessen ist ein Konzept zu entwickeln, welches eine direkte Einflussnahme auf den Erkenntnisprozess (z.B. durch Weisungen) ausschließt. Daneben ist darzulegen, dass private (z.B. wirtschaftliche) Interesse das Forschungsinteresse nicht dominieren.

8. Insgesamt ist es lohnenswert, im kooperativen Austausch mit der verantwortlichen Datenschutzbehörde zu stehen und so für Transparenz zu sorgen. In der DSGVO gibt es gemäß Art. 40 DSGVO beispielsweise die Möglichkeit für Vereinigungen und Verbände, eigenständig, im Wege der Selbstregulierung datenschutzrechtliche Verhaltensregeln zu entwerfen und der Behörde zur Genehmigung vorzulegen. Vorlageberechtigt sind neben klassischen Vereinen und Verbänden sämtliche freiwilligen Zusammenschlüsse, soweit diese eine bestimmte homogene Gruppe vertreten, nicht jedoch einzelne Unternehmen. Genehmigte Verhaltensvorgaben generieren eine gewisse Rechtssicherheit dahingehend, dass die abstrakten Vorschriften der DSGVO eine branchenspezifische Präzisierung und Konkretisierung erfahren. Die Einhaltung genehmigter Verhaltensregeln und Zertifizierungsverfahren wirkt sich zudem, im Falle eines unvermeidbaren Verstoßes gegen Vorschriften der DSGVO, positiv auf die Bußgeldhöhe aus, vgl. Art. 82 Abs. 2 S 2 lit j DSGVO. Daneben besteht die Möglichkeit der Zertifizierung von Datenverarbeitungsvorgängen, vgl. Art. 42 DSGVO. Darüber hinaus kann auch über die gesetzlich vorgesehenen Kooperationen mit der Aufsichtsbehörde ein informeller Austausch angestrebt werden.

9. Der Betrieb der Datenbank durch eine Forschungskooperation ist ungeeignet. Eine solche Kooperation generiert aufgrund fehlender rechtlicher Vorschriften Rechtsunsicherheit und ist mit großem vertraglichen Aufwand verbunden, sodass von Anfang an eine passende Rechtsform gefunden werden sollte. In Betracht kommt aus Haftungsgründen entweder die Ausgestaltung als GmbH oder als eingetragener Verein, wobei der GmbH wohl langfristig der Vorzug einzuräumen ist. Die Anerkennung als gemeinnützige GmbH hat zahlreiche Vorteile, ist aber nur dann denkbar, wenn das Gewinnausschüttungsverbot durch ein passendes Finanzierungsmodell und einer nicht-kommerziell-orientierten Akteursstruktur im Kernbetrieb aufgefangen wird. Vor der Gründung eines Vereins oder einer GmbH, welche die Privilegien des § 51 AO aufgrund ihrer Gemeinnützigkeit erhalten soll, ist es ratsam, bereits vorab mit den zuständigen Finanzbehörden Kontakt aufzunehmen, um so sicherzustellen, dass die Anforderungen des Gemeinnützigkeitsrechts erfüllt sind.

10. In der Regel ist davon auszugehen, dass die Forschungskooperation vom Kartellverbot durch eine EU-Gruppenfreistellungsverordnung freigestellt wird. Allerdings gilt es zu beachten, dass die an der Kooperation beteiligten Unternehmen das Risiko der Freistellung, insbesondere die Beweislast mit Blick auf die Freistellungsvoraussetzungen, tragen. Daher empfiehlt sich eine regelmäßige Überprüfung der Freistellungsvoraussetzungen.

Regulierungspotenzial mit Blick auf den nationalen Rechtsrahmen

Neben der Anpassung des gesamten europäischen Datenschutzrechts (insbesondere der DSGVO), was realistisch allenfalls eine mittel- bis langfristige Option darstellt, besteht die kurz- bis mittelfristig realisierbare Möglichkeit innerhalb der den Mitgliedstaaten verbleibenden Regelungsspielräume punktuell nationale Vorgaben zu treffen.

IKEM

Oktober 2021

A2: Analyse der rechtlichen Rahmenbedingungen und Ableitung praktischer Handlungsempfehlungen

Entwicklung eines Konzepts und Lastenhefts für eine Szenariendatenbank zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen (FE 82.0719/2018)

ERSTELLT VON

Mathilde Krampitz
Anne Freiberger
Tarek Neuparth
Wiebke Jafra

IM AUFTRAG DER

Bundesanstalt für Straßenwesen

Inhaltsverzeichnis

Einleitung 6

Haftungsausschluss 7

Nutzen der Datenbank aus rechtlicher Sicht 8

Rolle der Szenariendatenbank mit Blick auf das Zulassungsrecht 8

Zulassung von automatisierten Fahrfunktionen zum Straßenverkehr 8
Datenspeicherungs- und Übermittlungspflichten im StVG 9
Gesetz zum autonomen Fahren 2021 9

Absicherung im Rahmen der Typprüfung 10

Zulässige Erhebung von Halterdaten 10

Mögliche Datenquellen und Datenkategorien 12

Rechtsrahmen der Datenverarbeitung 15

Verarbeitung personenbezogener Daten 15

Sonderfall: Sensible Daten 18
Verarbeitung personenbezogener Daten 19
Anonymisierung von personenbezogenen Daten 19
Begriff der Anonymisierung 19
Praktische Sicherstellung der Anonymisierung 20
Blurring 20

Synthetisierung von Daten 20

Aggregation von Daten 21

Abgrenzung der Anonymisierung von der Pseudonymisierung 21

Datenschutzrechtliche Erfordernisse 22

Rechtfertigung automatisierter Datenverarbeitung 22
Einwilligung 22

Erforderlichkeit der Verarbeitung für die Erfüllung eines Vertrags mit der betroffenen Person 24

Erforderlichkeit der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen 24

Erforderlichkeit der Verarbeitung zum Schutz lebenswichtiger Interessen einer natürlichen Person 25

Erforderlichkeit der Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt durch den Verantwortlichen 25

Interessenabwägung 26

Relevante Rechtfertigungstatbestände mit Blick auf die in die Datenbank eingespeisten Forschungsdaten 26

Verantwortlichkeit 26

Allgemeine Datenschutzrechtliche Anforderungen und Pflichten der Verantwortlichen 27
Datenschutzbeauftragte 27
Informationspflichten 27
Rechenschaftspflichten 28
Zweckbindung 28
Datenschutzfolgenabschätzung 28
Löschpflichten 28
Sonderstellung von Forschungsdaten 29
Definition Forschungsdaten 29
Garantien für die Rechte und Freiheiten der Betroffenen 30
Einzelne Privilegierungen 30
Besonderheiten bei der Einwilligung in Datenverarbeitungen zu Forschungszwecken 31
Privilegierung der Zweckbindung 31
Eingeschränktes Widerspruchsrecht bei Datenverarbeitungen auf Grundlage von 31
Öffnungsklauseln für die Mitgliedstaaten mit Blick auf die Verarbeitung von Forschungsdaten 31
Haftung für Datenschutzverstöße 32
Was folgt aus der DSGVO für die Betreiberrolle (Öffentlich, Privat insb. Industriekooperation) 33
Zusammenfassung der datenschutzrechtlichen Hürden 34
Nicht-personenbezogene Daten 34
Gemischte Datensätze 35

Rechtsrahmen Datenzugang und Datenweiterverwendung 36

Europäische Gesetzgebung zum Datenzugang 37
Zugang zu Geodatensätzen - INSPIRE 38
Zugang zu Umweltinformationen – Umweltinformationsrichtlinie 38
Nationale Gesetzgebung zum Datenzugang 39
Zugang privater Akteure zu Informationen von öffentlichen Stellen 39
Zugang privater Akteure zu Informationen anderer privater Akteure 41
Zugang öffentlicher Stellen zu Informationen privater Akteure 41
Datenweiterverwendung 42
Europäische Gesetzgebung zur Datenweiterverwendung 42
Nationaler Rechtsrahmen Datenweiterverwendungsrechte 43
Keine Dateneigentumsrechte als Zuordnungskriterium 44
Zusammenfassung der rechtlichen Hürden aus dem Recht der Datenzugänge und Datenweiterverwertung 45

Ausblick: Europäische und nationale Datenstrategien 47

Europäische Datenstrategie **47**
Gemeinsame europäische Datenräume 47
Rechtsakt über Daten 48
Datenstrategie des Bundes **48**
Datenintermediäre und -treuhänder 48
Mobilitätsdatenräume und Gaia-X 49
Forschungsdatenzentren 50

IT-Sicherheit 51

Rechtsform der Datenbank 53

Nachteile einer bloßen Forschungskooperation **53**

Überblick über Kapital- und Personengesellschaften **53**

Eingetragener Verein **55**
Nichtwirtschaftlicher Verein 55
Haftung der Vereinsmitglieder und des Vorstands 56
Vereinsmitglieder 56

Vergleich zwischen GmbH und eingetragenem Verein **56**

Gemeinnützigkeit des Vereins oder der GmbH (ggf. UG) **57**

Fazit 59

Kartell- und Wettbewerbsrecht 60

Praktische Handlungsvorgaben ohne regulatorische Anpassungen 62

Regulierungspotenzial mit Blick auf den nationalen Rechtsrahmen 67

Nationale Formulierung von rechtlichen Verpflichtungen **67**

Literaturverzeichnis 68

Einleitung

Im Rahmen des Projekts „Entwicklung eines Konzepts und Lastenhefts für eine Szenariendatenbank zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen“ durch die Bundesanstalt für Straßenwesen (BASt) forscht das IKEM zum rechtlichen Rahmen der Konzeptionierung einer solchen Datenbank und leitet praktische Handlungsvorgaben ab. Im Folgenden werden der rechtlich relevante Nutzen der Szenariendatenbank umrissen, relevante rechtliche Vorgaben für die Szenariendatenbank überblickartig dargestellt, die eruierten Hürden herausgearbeitet und anschließend praktische Handlungsvorgaben vorgestellt.

Haftungsausschluss

Es wird darauf hingewiesen, dass es sich lediglich um eine interne projektbegleitende rechtliche Prüfung handelt, welche vornehmlich darauf abzielt, die Ziele des Projekts gemeinsam zu erreichen. Das IKEM übernimmt keine Gewähr für die Richtigkeit der summarischen Prüfung. Unternehmerische Entscheidungen können auf die Ergebnisse nicht gestützt werden, bevor sie nicht durch die Rechtsabteilung des beratenen Unternehmens oder eine externe anwaltliche Beratung geprüft wurden.

Nutzen der Datenbank aus rechtlicher Sicht

Neben der wesentlichen Funktion der Datenbank, als Informationsgrundlage mit Blick auf anstehende gesellschaftliche und politische Debatten und regulatorischer Feinsteuerung bietet die Szenariendatenbank sekundäre rechtliche Vorteile etwa mit Blick auf Fahrzeugentwicklung (angesichts der Bedeutsamkeit im Rahmen des Fahrzeugzulassungsrechts), sowie die Einhaltung von Complianceanforderungen (angesichts von Haftungsrisiken, Produktsicherheit etc.) usw. und zuletzt dem Vorantreiben von Formen der deregulierten Selbstregulierung wie bspw. der Entwicklung von bereichsspezifischen Standards.

Rolle der Szenariendatenbank mit Blick auf das Zulassungsrecht

Zwischen dem Fahrzeugzulassungsrecht und der Szenariendatenbank besteht eine gewisse Wechselwirkung. Zum einen kann die Szenariendatenbank zur Absicherung und Validierung des Fahrzeugs im Rahmen des Zulassungsverfahrens dienen. Andererseits können aus der Datenbank Informationen bezüglich der Fähigkeiten und Besonderheiten automatisierter Systeme gewonnen werden und auf dieser Grundlage entsprechend regulatorisch reagiert und auf das Zulassungsrecht eingewirkt werden. Schließlich weisen zulassungsrechtliche Regelungen vermehrt Datenspeicher- und Übermittlungspflichten auf, welche gegebenenfalls für die Einspeisung fahrzeugseitig erhobener Informationen in die Szenariendatenbank relevant sein könnten.

Zulassung von automatisierten Fahrfunktionen zum Straßenverkehr

Automatisiertes Fahren wird vom gegenwärtigen Rechtsrahmen nur zum Teil erfasst. Automatisierte Fahrfunktionen der Level 1 (z.B. Spurhalteassistent oder Abstandsregeltempomat) und Level 2 (Spurhalteassistent und Abstandsregeltempomat), zeichnen sich durch die fahrzeugführerseitige Beherrschung des Fahrzeugs aus, unterfallen damit den herkömmlichen zulassungsrechtlichen Vorgaben und sind bereits heute in zahlreichen Neufahrzeugen anzutreffen. 2017 sind mit §§ 1a und 1b StVG erstmals Regelungen für hochautomatisierte Fahrfunktionen[1] (z.B. Autobahnpiloten) normiert worden.[2] Die Vorschriften erlauben die systemseitige Übernahme der Fahrzeugsteuerung in bestimmten Situationen bei fortdauernder Wahrnehmungsbereitschaft des Fahrzeugführers. Die von den Vorschriften erfassten Fahrzeugfunktionen sind allerdings gemäß § 1a Abs. 3 StVG nur solche, die entweder in internationalen Vorschriften beschrieben sind und diesen entsprechen, oder für welche eine Typgenehmigung gem. Art. 20 der Rahmenrichtlinie vorliegt. 2020 wurden in diesem Zusammenhang erstmalig auf ECE-Ebene Anforderungen an automatisierte Spurhaltesysteme (*automated lane keeping systems*) mit Blick auf SAE-Level 3 normiert.[3] Die Zulässigkeit automatisierter Fahrfunktionen wird in § 1 a StVG in Relation zu einer spezifischen *operational design domain* (ODD) gestellt. Grundvoraussetzung der Zulässigkeit automatisierter Fahrfunktionen ist die selbstständige „Bewältigung der Fahraufgabe – einschließlich Längs- und Quersteuerung“ und die Umsetzung der an die Fahrzeugführung gerichteten Verkehrsvorschriften, vgl. § 1 a Abs. 2 StVG. Die konkreten zu bewältigenden Szenarien ergeben sich dabei aus der ODD. Die Szenariendatenbank könnte in dem Zusammenhang als Sicherheitsnachweis im Rahmen der Zulassung bedeutsam werden und den Absicherungsprozess erheblich

[1] Missverständlich in § 1 a und 1b StVG als hoch- und vollautomatisierte Fahrfunktion bezeichnet.
[2] Änderung des Straßenverkehrsgesetzes vom 16.6.2017, BGBl. 2017 I 1648.
[3] UNECE, UN Regulation on Automated Lane Keeping Systems is milestone for safe introduction of automated vehicles in traffic, veröffentlicht unter https://unece.org/transport/press/un-regulation-automated-lane-keeping-systems-milestone-safe-introduction-automated, zuletzt aufgerufen am 30.03.2021.

vereinfachen und erleichtern. Der automatisierungsbedingte Verantwortungswechsel von Mensch auf das Fahrzeug generiert enorme Anforderungen an die fahrzeugseitige funktionale Sicherheit. Aufgrund der automatisierungsbedingten zunehmenden Übernahme der Aufgaben der Fahrzeugsteuerung muss vorab eine enorme Anzahl von Szenarien getestet werden, welche innerhalb der Operational Design Domain potenziell auftreten könnten.

Datenspeicherungs- und Übermittlungspflichten im StVG

Daneben könnten durch die neuen Regelungen die zulässige Erhebung von Fahrzeugdaten ermöglicht werden, welche als zusätzliche Quelle der Datenbank in Betracht kommen.
Im Straßenverkehrsgesetz (StVG) konkret in § 63 a StVG, wird die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion bereits geregelt. In der Vorschrift ist die situative Datenspeicherung von Positions- und Zeitangaben, bei dem Verantwortungswechsel zwischen Fahrzeugsystem und Fahrzeugführers und bei systemseitigen Aufforderungen zur Übernahme der Fahrzeugsteuerung oder technischen Störungen des Systems geregelt, vgl. § 63 a Abs. 1 StVG. Hintergrund der Regelung ist die erleichterte Beweisführung.[4] Nicht geregelt, sondern an den Verordnungsgeber delegiert, vgl. § 63 b S. 1 Nr. 1 StVG wurden Ort[5] und Art der Speicherung. Die entsprechende Rechtsverordnung wurde aufgrund erforderlicher ausstehender Einigungen auf internationaler Ebene bis heute nicht erlassen.[6] Aufgrund der grenzüberschreitenden Harmonisierung der technischen Vorschriften für Kraftfahrzeuge müssen die entsprechenden Regelungen, einschließlich der in dem Zusammenhang geregelten datenschutz- und datensicherheitsrechtlichen Anforderungen, Berücksichtigung finden, um Handelshemmnisse aufgrund nationaler Alleingänge zu vermeiden.[7] Der 56. Verkehrsgerichtstag fordert mit Blick auf den Speicherort (auch) eine treuhändische Datenverwaltung.[8] Eine solche Datenübertragung an eine dritte Stelle bedarf aber aufgrund des damit verbundenen Grundrechtseingriffs einer gesetzlichen Rechtfertigung, welche hohen Verhältnismäßigkeitsanforderungen genügen muss.[9] Hierbei ist insbesondere das mit einer solchen Datensammlung verbundene Missbrauchspotential und der hohe Schutzbedarf der in Rede stehenden Fahrzeugdaten, vor dem Hintergrund der drohenden Erstellung von Verhaltens- und Bewegungsprofilen, zu berücksichtigen.[10]

Gesetz zum autonomen Fahren 2021

Am 28. Juli 2021 ist das Gesetz zum autonomen Fahren[11] in Kraft getreten. Der Szenariendatenbank könnte eine zentrale Rolle im Rahmen des neu kreierten Regelzulassungsverfahrens zukommen. Daneben könnten aufgrund der neuen Regelungen die zulässige Erhebung von Herstellerdaten und damit die zulässige Fusion wichtiger sicherheitsrelevanter Informationen ermöglicht werden.

---

[4]

[5] Stender-Vorwachs/ Steege, „Grundrechtliche Implikationen autonomen Fahrens“, 2020, RN. 197.

[6] Brockmeyer „Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge“, ZD 2018, 258 (259).

[7] BT-Drs. 18/11300 S.15.

[8] 56. Verkehrsgerichtstag 2018, Arbeitskreis II, Empfehlung Nr. 5, https://www.deutscher-verkehrsgerichtstag.de/vgt/themen-empfehlungen/82-50-deutscher-verkehrsgerichtstag-2067.

[9] Gagzow/ Körffer „Fahrzeugdaten als Beweismittel im Straf- und Bußgeldverfahren“ Roßnagel, Alexander/ Hornung, Gerrit Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 171.

[10] Roßnagel/ Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 171.

[11] Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, BGBl. 2021 I 3108.

Absicherung im Rahmen der Typprüfung

Der Szenariendatenbank könnte eine zentrale Rolle im Rahmen der Typprüfung auf Grundlage des neu kreierten Regelzulassungsverfahrens zukommen.
Die Datenbank könnte etwas als Informationsgrundlage zur Erstellung des erforderlichen Sicherheitskonzepts herangezogen werden. Ausweislich eines Entwurfs der Durchführungsverordnung zum neuen Gesetz hat der Hersteller, ausgehend von den systematisch ermittelten und anschließend bewerteten relevanten risikoträchtigen Szenarien innerhalb der ODD ein Sicherheitskonzept erstellen.[12] Eine zentrale Szenariendatenbank könnte hierfür, durch die Analyse und Aufbereitung einer großen Datenmenge eine wertvolle Informationsgrundlage für die Hersteller im Zulassungsverfahren schaffen. Die ausreichende Vollständigkeit der ODD-spezifischen Szenarien könnten die Hersteller leichter mit einer fusionierten Datenbereitstellung gewährleisten. Indirekt hätte die Datenbank dann auch Auswirkung auf die auf Grundlage des Sicherheitskonzepts herstellerseitig durchzuführende Gefährdungsanalyse[13] und den Testumfang. So sind abhängig von der jeweiligen ODD auf Basis eines herstellerseitig erstellten, mit einem Technischen Dienst abgestimmten, Szenarienkatalogs Testszenarien zu selektieren.[14]

Zulässige Erhebung von Halterdaten

Daneben wird in § 1 g StVG die zulässige Erhebung von Halterdaten, welche als zusätzliche Quelle der Datenbank in Betracht kommen, ermöglicht. Die Vorschrift sieht halterseitige Datenspeicherungs- und Übermittlungspflichten in beträchtlichem Umfang vor. Bei Betrieb ist der Halter in bestimmten Situationen[15] verpflichtet die Fahrzeugidentifikationsnummer, die Positionsdaten, Umwelt- und Wetterbedingungen, den Status der lichttechnischen Einrichtungen, die Fahrzeuggeschwindigkeit, Anzahl und Zeiten der Nutzung sowie der Aktivierung und der Deaktivierung der autonomen Fahrfunktion, Anzahl und Zeiten der Freigabe von alternativen Fahrmanövern, Systemüberwachungsdaten einschließlich Daten zum Softwarestand, Vernetzungsparameter wie beispielsweise Übertragungslatenz und verfügbare Bandbreite, Name der aktivierten und deaktivierten passiven und aktiven Sicherheitssysteme, Daten zum Zustand dieser Sicherheitssysteme sowie die Instanz, die das Sicherheitssystem ausgelöst hat, Daten betreffen die Fahrzeugbeschleunigung in Längs- und Querrichtung, Spannungsversorgung des Kraftfahrzeugs mit autonomer Fahrfunktion und von extern an das Kraftfahrzeug gesendete Befehle und Informationen zu speichern, vgl. § 1 g Abs. 1 S. 1 StVG. Der Halter wird zudem gemäß § 1 g Abs. 1 S. 2 StVG gesetzlich verpflichtet, dem Kraftfahrt-Bundesamt (KBA) und der nach Bundes- oder Landesrecht zuständigen Behörde oder auf Bundesfernstraßen, soweit dem Bund die Verwaltung zusteht, der Gesellschaft privaten Rechts im Sinne des Infrastrukturgesellschaftserrichtungsgesetzes auf Verlangen die gesammelten Daten zu übermitteln, soweit dies für die behördliche Aufgabenerfüllung gemäß § 1 g Abs. 4, 5 und 6 StVG erforderlich ist.
Mit Blick auf das KBA ist die „Überwachung des sicheren Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion" gemäß § 1 g Abs. 4 S. 1 StVG eine, die Datenverarbeitung rechtfertigende, Aufgabe.
Daneben kann das KBA gemäß § 1 g Abs. 5 S. 1 StVG nicht-personenbezogene Daten „für verkehrsbezogene Gemeinwohlzwecke, insbesondere zum Zweck der wissenschaftlichen Forschung im Bereich der Digitalisierung, Automatisierung und Vernetzung sowie zum Zweck der Unfallforschung im Straßenverkehr" weiteren Stellen, nämlich „1. Hochschulen und Universitäten, 2. außeruniversitäre Forschungseinrichtungen, 3. Bundes-, Landes- und Kommunalbehörden mit Forschungs-, Entwicklungs-, Verkehrsplanungs- oder Stadtplanungsaufgaben" zugänglich machen und durch jene zu vorbenannten Zwecken verwendet werden, vgl. § 1

[12] Anl. 1, Anh. 1 AFGBV (neu), Stand Februar 2021, 7.2.
[13] Anl. 1, Anh. 1 AFGBV (neu), Stand Februar 2021, 7.2. 1.
[14] Anl.1 Anh. 2 AFGBV (neu), Stand Februar 2021, 1.3.
[15] Bei Eingriffen durch die Technische Aufsicht, bei Konfliktszenarien, insbesondere bei Unfällen und Fast-Unfall-Szenarien, bei nicht planmäßigem Spurwechsel oder Ausweichen und bei Störungen im Betriebsablauf, vgl. § 1 g Abs. 2 StVG.

g Abs. 5 S. 1 StVG. Insoweit besteht bereits ein Anspruch von Forschungseinrichtungen auf ermessensfehlerfreie Entscheidung[16] gegen die öffentlichen Stellen mit dem Ziel der Zugänglichmachung und Verwendung anlassbezogen erhobener Halterdaten. Aufgrund der Beschränkung auf nicht personenbezogene Daten handelt es sich nicht um einen datenschutzrechtlichen Erlaubnistatbestand im Sinne von Art. 6 DSGVO.

[16] Specht-Riemenschneider, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung, 2021, S. 51.

Mögliche Datenquellen und Datenkategorien

Für die Errichtung der Szenariendatenbank kommen unterschiedliche Datenquellen bzw. -lieferanten in Betracht. Mögliche Akteure, welche die für die Szenarienbildung notwendigen Daten bereitstellen können, stammen sowohl aus dem privaten als auch aus dem öffentlichen Sektor.
Im privaten Sektor sind vor allem OEMs (Automobilhersteller) als mögliche Datenlieferanten für die Szenarienbildung relevant. Durch die Sensoren, die auf den Fahrzeugen mit automatisierten Fahrfunktionen angebracht sind, können Datensätze betreffend Außentemperatur, Wetterlage, Gewichtsverteilung, Reifenstellung, Geschwindigkeit zum Zeitpunkt von Unfall- oder beinahe Unfallgeschehen übermittelt werden.
Mögliche Datenlieferanten aus dem öffentlichen Sektor sind beispielsweise der Deutsche Wetterdienst (DWD) oder die Bundesanstalt für Straßenwesen (BASt). Durch Datenübermittlung, oder den Serverzugriff auf gespeicherten Date zu bspw. Wetterlage (Schnee, Regen etc.), oder Verkehrsdichte, können diese Datenkategorien durch den Betreiber der Szenariendatenbank zur Szenarienbildung verwendet werden.
Die folgende Tabelle stellt eine Übersicht über die abstrakte Datenkategorie und Beispiele für konkrete Datensätze dar, die zur Szenarienbildung notwendig sind. Daneben zeigt die Tabelle weiterhin auf, welche Datenlieferanten für die jeweiligen Datenkategorien aus dem öffentlichen und privaten Sektor in Betracht kommen.

Abbildung 1 Übersicht Datenkategorien, -lieferanten und -sätze

Datenkategorien	Datenlieferant	Datensatz
Temperatur in C	OEMs (lokaler Sensor)	Außentemperatur, Innentemperatur
Bereifung	OEMs (lokaler Sensor)	Allwetterreifen
Wetterlage	DWD (Serverzugriff) OEMs (lokaler Server)	Nebel, Regen, Schnee, Sonnenschein
Standort	OEMs (lokaler Sensor)	GPS-Koordinaten
Momentangeschwindigkeit / GPS-Koordinaten-Standort-Ableitung nach Zeit (t)	OEMs (lokaler Sensor und softwareinterne Berechnung)	GPS-Koordinaten

Masse (kg)	OEMs (lokaler Sensor)	Leergewicht / aktuelles Gewicht
Massenverteilung (kg/m^2)	OEMs (lokaler Sensor)	Gewichtsverteilung der Ladung / Beladungszustand
Aktorenzustände	OEMs (lokale Sensoren)	Reifenstellung, Reifenrotationsrichtung, Reifendruck etc. …
Allgemeine Verkehrsdichte (KfZ/24 h)	BASt	GPS-Koordinaten, Straßenname, Fahrbahnrichtung (Bsp. 19.645 KfZ/ 24 h auf A14 – AS Wanzleben in Richtung Magdeburg)
Konkrete Verkehrsdichte	OEMs (lokaler Sensor)	Videokameras, Lidar
Baustellenverteilung	BASt	Baustellenart, -länge, -dauer, Straßenname, Fahrrichtung
Car-to-X Daten	OEMs (lokaler Sensor)	Warnsignal – Bsp. „Einsatzfahrzeug von hinten“
Situativ zu speichernde Halterdaten gemäß § 1 g Abs. 1 S. 1 StVG	KBA, nach Bundes- oder Landesrecht zuständige Behörde u.a.	Fahrzeugidentifikationsnummer, die Positionsdaten, Umwelt- und Wetterbedingungen, den Status der lichttechnischen Einrichtungen, die Fahrzeuggeschwindigkeit, Anzahl und Zeiten der Nutzung sowie der Aktivierung und der Deaktivierung der autonomen Fahrfunktion, Anzahl und Zeiten der Freigabe von alternativen Fahrmanövern, Systemüberwachungsdaten einschließlich Daten zum Softwarestand, Vernetzungsparameter wie beispielsweise Übertragungslatenz und verfügbare Bandbreite, Name der aktivierten und

		deaktivierten passiven und aktiven Sicherheitssysteme, Daten zum Zustand dieser Sicherheitssysteme sowie die Instanz, die das Sicherheitssystem ausgelöst hat, Daten betreffen die Fahrzeugbeschleunigung in Längs- und Querrichtung, Spannungsversorgung des Kraftfahrzeugs mit autonomer Fahrfunktion und von extern an das Kraftfahrzeug gesendete Befehle und Informationen

Rechtsrahmen der Datenverarbeitung

Der einschlägige Rechtsrahmen für die Datenverarbeitung unterscheidet sich im Wesentlichen danach, ob personenbezogene oder nicht-personenbezogene Daten durch den Prozess zusammengetragen und gespeichert werden. Weitere Unterschiede können sich aus verschiedenen, für die Datenergebung verantwortlichen. Akteure ergeben. Rechtlich relevante Unterscheidungen der Akteure sind solche in juristische Personen des Privatrechts, sowie des öffentlichen Rechts, wie beispielsweise öffentliche Institutionen (Behörden) und öffentlich – rechtliche Unternehmen (Anstalten, GmbH etc.).

Verarbeitung personenbezogener Daten

Der Rechtsrahmen, der Datenerhebung und -verarbeitung regelt, wird maßgeblich durch europäische Gesetzesakte, sowie die EMRK bestimmt. Gemäß Art. 8 Abs. 1 EMRK hat jede Person das Recht auf Achtung ihres Privatlebens. Nach Verabschiedung eines Zustimmungsgesetzes gilt die EMRK als völkerrechtlicher Vertrag als einfaches Bundesgesetz (Art. 59 Abs. 2 S.1 GG).[2]

Auf europarechtlicher Ebene prägt die DSGVO die Voraussetzungen der Datenverarbeitung personenbezogener Daten. Die DSGVO gilt als Verordnung unmittelbar in allen europäischen Mitgliedstaaten.[3]

Neben der DSGVO existieren zum Teil bundes- und landesrechtliche Vorgaben sowie bereichsspezifische Gesetze, welche je nach Datenbankbetreiber und konkreter Ausgestaltung der Datenbank beachtet werden müssen, um den im Einzelfall bestehenden rechtlichen Rahmen zu ermitteln.[17]

Während das BDSG für öffentliche Stellen des Bundes und nicht öffentliche Stellen gilt, vgl. § 1 Abs. 1 BDSG, gelten die Landesdatenschutzgesetze für öffentliche Stellen der Länder.[18]

Personenbezogene Daten werden gem. Art. 4 Abs. 1 DSGVO als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ definiert. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind” definiert.

Die weit gefasste Definition hat zur Folge, dass mehrere Datenkategorien, die durch die Szenariendatenbank erfasst werden würden, Personenbezug aufweisen können. Zur näheren Analyse ist das bereits oben dargestellte Schaubild zur Übersicht über Datenkategorien, in der folgenden Abbildung, um die Möglichkeit des Personenbezugs erweitert. Die Möglichkeit des Personenbezugs besteht bei allen durch die OEMS

[17] Rücker/ Dienst/ Brandt für das Bundesministerium für Wirtschaft und Energie „Umsetzung der BMWi-Stategie „Reallabore als Testräume für Innovation und Regulierung“: Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen (Projekt Nr. 113/19-FL1-2/03), 2021 S. 27.
[18] Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen“ Version 1.1, 2020, S. 89.

durch lokale Sensoren auf oder in den Fahrzeugen gespeicherten Daten. Durch die Verbindung der Datensätze mit der Fahrzeugidentifikationsnummer (FIN) können die technischen Daten dem Halter des Fahrzeuges zugeordnet werden.[19]

Daneben besteht der mögliche Personenbezug auch bei den Videoaufnahmen, die durch Fahrzeuge von ihrer Umgebung aufgenommen werden. Sobald auf dem Videomaterial natürliche Personen identifizierbar sind, handelt es sich bei dem Videomaterial um personenbezogene Daten.

Abbildung 2 Übersicht Datenkategorien und möglicher Personenbezug

Datenkategorien	Datenlieferant	Datensatz	Möglichkeit des Personenbezugs
Temperatur in C	OEMs (lokaler Sensor)	Außentemperatur, Innentemperatur	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter / die Halterin oder das KFZ-Kennzeichen
Bereifung (allgemein: Betriebszustand)	OEMs (lokaler Sensor)	Allwetterreifen	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter / die Halterin oder das KFZ-Kennzeichen
Wetterlage	DWD (Serverzugriff) OEMs (lokaler Server)	Nebel, Regen, Schnee, Sonnenschein	Nein
Standort	OEMs (lokaler Sensor)	GPS-Koordinaten	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter /

[19] BMVI, Eigentumsordnung für Mobilitätsdaten – Eine Studie aus technischer, rechtlicher und ökonomischer Perspektive, 2018, S. 48.

			die Halterin oder das KFZ-Kennzeichen Bewegungsprofil
Momentangeschwindigkeit / GPS-Koordinaten-Standort-Ableitung nach Zeit (t)	OEMs (lokaler Sensor und softwareinterne Berechnung)	GPS-Koordinaten	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter / die Halterin oder das KFZ-Kennzeichen Bewegungsprofil
Masse (kg)	OEMs (lokaler Sensor)	Leergewicht / aktuelles Gewicht	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter / die Halterin oder das KFZ-Kennzeichen
Massenverteilung (kg/m^2)	OEMs (lokaler Sensor)	Gewichtsverteilung der Ladung / Beladungszustand	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter / die Halterin oder das KFZ-Kennzeichen
Aktorenzustände	OEMs (lokale Sensoren)	Reifenstellung, Reifenrotationsrichtung, Reifendruck etc. …	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter /

			die Halterin oder das KFZ-Kennzeichen
Allgemeine Verkehrsdichte (KfZ/24 h)	BASt	GPS-Koordinaten, Straßenname, Fahrbahnrichtung (Bsp. 19.645 KfZ/ 24 h auf A14 – AS Wanzleben in Richtung Magdeburg)	Nein
Konkrete Verkehrsdichte	OEMs (lokaler Sensor)	Videokameras, Lidar	Gesichter von gefilmten Personen, KfZ-Kenzeichen von gefilmten KfZ Bewegungsprofile
Baustellenverteilung	BASt	Baustellenart, -länge, -dauer, Straßenname, Fahrrichtung	Nein
Car-to-X Daten	OEMs (lokaler Sensor)	Warnsignal – Bsp. „Einsatzfahrzeug von hinten“	Über die Fahrzeugidentifikationsnummer (FIN) i.V.m. Seite 2 Nr. 4 der Zulassungsbescheinigung Teil I den Halter / die Halterin oder das KFZ-Kennzeichen

Sonderfall: Sensible Daten

Einen Sonderfall personenbezogener Daten stellen sensible Daten dar. Für sensible Daten bestehen verschärfte Schutzanforderungen, mit der Folge, dass die **Verarbeitungsmöglichkeiten (noch) restriktiver** ausgestaltet sind. Sensible Daten sind solche Daten, aus denen Informationen über Eigenschaften oder Zu-

schreibungen des Nutzers hervorgehen, die besonders oft Gegenstand von Diskriminierung sind[20] und deswegen besonderen Schutz erfordern. Dies können z.B. Daten über politische Anschauungen, religiöse Überzeugungen, die ethnische Herkunft, die sexuelle Identität oder Gesundheitsdaten sein.[21] Bei den personenbezogenen Daten, die zur Szenarienbildung gespeichert werden könnten (siehe Tabelle), handelt es sich nicht um sog. „sensible Daten". Daher wird im Rahmen der weiteren Prüfung auf die notwendige unterschiedliche Handhabung nicht weiter eingegangen.

Verarbeitung personenbezogener Daten

Die DSGVO greift, wenn eine Verarbeitung personenbezogener Daten vorliegt. Die Verarbeitung wird in Art. 4 Abs. 2 DSGVO definiert, als „jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung." Diese weite Definition hat zur Folge, dass sowohl die die Erhebung von personenbezogenen Daten und die anschließende Speicherung von sortierten Datensätzen in der Szenariendatenbank als "Verarbeitung" i.S.d. Art. 4 Abs. 2 DSGVO anzusehen sind.

Anonymisierung von personenbezogenen Daten

Die Anwendbarkeit der DSGVO entfällt, wenn der Personenbezug aufgrund der Anonymisierung von Daten entfällt.[22] Anonymisierte Daten können durch den Datenbankbetreiber ohne Beachtung der DSGVO verwendet und gespeichert bleiben.

Begriff der Anonymisierung

Die DSGVO definiert den Begriff der Anonymisierung selbst nicht.[23] Eine Anonymisierung setzt voraus, dass personenbezogene Daten derart verändert werden, dass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht bzw. nicht mehr identifiziert werden kann.[24] Dies wird je nach Verantwortlichem unterschiedlich beantwortet, entscheidend ist das „mobilisierte Zusatzwissen" der einzelnen Verantwortlichen.[25] Bei der Bewertung sind die, während der Speicherdauer erwartbaren, technischen Möglichkeiten zu berücksichtigen.[26] Solange die Person reidentifiziert werden kann, liegt lediglich Pseudonymisierung vor,[27] die DSGVO bleibt anwendbar. Die Anonymisierung stellt insoweit ein Mehr zur Pseudonymisierung dar.[28] **Echte Anonymisierung** ist, auf Grund des Anstiegs von Rechenleistung und Speicherkapazitäten, welche die Verknüpfung von Daten vereinfachen, in der Praxis kaum noch zu bewerkstelligen.[29] Die in dem Zusammenhang häufig generierte bloße „**faktische Anonymität**"

[20] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 9 DSGVO Rn. 10
[21] Ernst in Paal/Pauly, DS-GVO BDSG, Art.4 DSGVO, 3. Auflage, 2021, Rn. 19.
[22] Ernst in Paal/Pauly, DS-GVO BDSG, Art.4 DSGVO, 3. Auflage, 2021, Rn. 49.
[23] Ernst in Paal/Pauly, DS-GVO BDSG, 3. Auflage, 2021, Rn. 48.
[24] Ernst in Paal/Pauly, DS-GVO BDSG, 3. Auflage, 2021, Rn. 48.
[25] Roßnagel "Datenschutz in der Forschung - Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen", ZD 2019, 157 (159)
[26] Roßnagel "Datenschutz in der Forschung - Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen", ZD 2019, 157 (159)
[27] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO, 3. Auflage, 2021, Rn. 49.
[28] Ernst in Paal/Pauly, DS-GVO BDSG, Art. 4 DSGVO, 3. Auflage, 2021, Rn. 48.
[29] Kotter „Datenschutz beim vernetzten und autonomen Fahren. Welche Rahmenbedingungen können sensible Daten schützen?" 2019, S. 34

führt dazu, dass die DSGVO anwendbar bleibt, [30] die Schutzwürdigkeit der Daten indes auf das Niveau pseudonymisierter Daten abgesenkt wird. Im Ergebnis ist die faktische Anonymisierung damit so zu behandeln wie die Pseudonymisierung.

Praktische Sicherstellung der Anonymisierung

Praktische Möglichkeiten der Anonymisierung sind etwa das **dauerhafte Unkenntlichmachen (sog. *Blurring*)** von Gesichtern, Kennzeichen und sonstigen personenbezogenen Informationen[31] oder die **Aggregierung (Unterfall der Generalisierung) und Synthetisierung (Unterfall der Randomisierung) von Daten**.

Die Wahl einer geeigneten bzw. Kombination verschiedener Anonymisierungsmethoden muss sich an den Einzelfallumständen orientieren. [32] Stärken und Schwächen möglicher Techniken hat die Art.29-Datenschutzarbeitsgemeinschaft in einer Stellungnahme zusammengefasst.[33]

Fallstudien und Forschungsarbeiten haben aufgezeigt, wie schwer es praktisch ist, zum einen, einen tatsächlich anonymen Datenbestand zu generieren und zum anderen dabei sämtliche Informationen zu erhalten, welche für die zu bewältigende Aufgabe erforderlich sind.[34] Praktisch verbleibt aufgrund der einzelfallabhängigen Anforderungen immer ein gewisses Restrisiko.[35]

Blurring

Die dauerhafte visuelle Unkenntlichmachung von Identifikatoren (insbesondere Fahrzeugkennzeichen und Gesichter) ist beispielsweise mit Blick auf visuelle Umfeldaufnahmen von Fahrzeugen relevant, die als Datensätze für die Szenarienbildung verwendet werden. Technisch sind die Möglichkeiten des sog. Blurrings bereits fortgeschritten und könnten vor Einspeisung der Datenkategorien in die Szenariendatenbank herangezogen werden, um eine Anonymisierung der ansonsten personenbezogenen Daten zu erreichen. Wichtig ist, dass die durch Blurring bearbeiteten Bilddateien nicht mehr wiederherstellbar sein dürfen, um den Personenbezug zu unterbinden.[36] Zu beachten ist, dass neben den klassischen Identifikatoren in Gestalt von Gesichtern und Fahrzeugkennzeichen auch sonstige Identifikatoren wie beispielsweise auffällige, einzigartige Frisuren, Tattoos und eine unverwechselbare Fahrzeuggestaltung einen Personenbezug herstellen können, der von der einschlägige Software nicht erkannt und daher auch nicht aufgehoben wird.

Synthetisierung von Daten

Bei der Daten-Synthetisierung handelt es sich um eine Methode, mit der eine „künstliche“ Repräsentation eines Originaldatensatzes erstellt werden kann. Hierzu wird ein Modell entwickelt, das die Originaldaten so gut wie möglich erklärt. Aus diesem Modell werden neue Daten generiert, die wichtige statistische Eigenschaften des Originaldatensatzes erhalten. Der synthetische Datensatz besteht nicht aus Daten natürlicher Personen, sondern aus Daten synthetischer Einheiten. Je nach Anwendung kann die Daten-Synthetisierung mit mathematischen Garantien der Privatheit kombiniert werden. Diese Methode ist bereits bei Behörden und Instituten mehrerer Länder im Einsatz und wird dazu benutzt, Mikrodatensätze, also Datensätze mit Daten, die auf Individualebene beobachtet werden, zu anonymisieren.

[30] Härting „DSGVO: Gibt es Regelungen für anonyme Daten?“ 2016, https://www.cr-online.de/blog/2016/05/03/dsgvo-gibt-es-regelungen-fuer-anonyme-daten/ (25.04.2020).
[31] Steege in „Ist die DS-GVO zeitgemäß für das autonome Fahren?“, MMR 2019, 509 (512).
[32] ARTIKEL-29-DATENSCHUTZGRUPPE „Stellungnahme 5/2014 zu Anonymisierungstechniken“ S. 29.
[33] ARTIKEL-29-DATENSCHUTZGRUPPE „Stellungnahme 5/2014 zu Anonymisierungstechniken“ S. 29.
[34] ARTIKEL-29-DATENSCHUTZGRUPPE „Stellungnahme 5/2014 zu Anonymisierungstechniken“ S. 3.
[35] ARTIKEL-29-DATENSCHUTZGRUPPE „Stellungnahme 5/2014 zu Anonymisierungstechniken“ S. 7.
[36] Steege in „Ist die DS-GVO zeitgemäß für das autonome Fahren?“, MMR 2019, 509 (512).

Aggregation von Daten

Die Aggregation von Daten gilt als sicherstes Tool zur Anonymisierung. Mehrere personenbezogene Daten werden zu einem Gruppendatensatz zusammengeführt, mit der Folge, dass nicht mehr festgestellt werden kann, welche Einzeldaten, wem innerhalb des Datenkollektivs, zuzuordnen waren.[37]

Konkrete Angaben werden auf diese Weise durch allgemein gehaltene Ersatzangaben ersetzt.[38] Allerdings führt die Datenaggregation nicht in jedem Fall zur Aufhebung des Personenbezugs und damit zum Vorliegen anonymisierter Daten.[39]

Abgrenzung der Anonymisierung von der Pseudonymisierung

Anonymisierte Daten sind abzugrenzen von pseudonymisierten Daten, welche sich durch gelockerten Personenbezug und infolgedessen ein erhöhtes Sicherheitsniveau auszeichnen[40]. Die DSGVO bleibt folglich anwendbar[41], die Daten sind aufgrund der bereits ergriffenen Sicherheitsmaßnahmen aber in geringerem Maße schutzwürdig.
In Art. 4 Nr. 5 DSGVO wird Pseudonymisierung definiert als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.
Welche konkreten Anforderungen an die getrennte Aufbewahrung der Informationen zu stellen sind wird in der DSGVO nicht normiert.[42] Der, der DSGVO immanente risikobasierte Ansatz spricht für eine wertungsbedürftige, von der jeweiligen Schutzbedürftigkeit der Daten abhängige, Bestimmung der Aufwands an die getrennte Aufbewahrung.[43] Technische Maßnahmen zur Gewährleistung der Nichtzuordnung bestimmen sind beispielsweise die Verwendung von Referenzlisten und der Einsatz kryptografischer Verfahren.[44]
Die Pseudonymisierung schützt Betroffene davor, dass ganze Datencluster, welche ihnen persönlich zugeordnet werden können, von Unbefugten unmittelbar eingesehen werden können und entlastet den Verantwortlichen dadurch bei der Einhaltung (weiterer) datenschutzrechtlicher Pflichten.[45] Weil der technisch-organisatorische Schutzbedarf bei pseudonymisierten Daten geringer ist, fällt eine Interessenabwägung zwischen dem berechtigten Interesse an der Datenverarbeitung und dem Interesse an dem Schutz personenbezogener Daten regelmäßig zugunsten des Verantwortlichen aus.[46]

[37] Ernst in Paal/Pauly, DS-GVO BDSG, 3. Auflage, 2021, Rn. 49.
[38] Roßnagel “Datenlöschung und Anonymisierung-Verhältnis der beiden Datenschutzinstrumente nach DS-GVO”, ZD 2021, 188 (189).
[39] Forgó, „Datenschutzrechtliche Fragestellungen des autonomen Fahrens“, erschienen in Oppermann/Stender-Vorwachs „Autonomes Fahren- Technische Grundlagen, Rechtsprobleme, Rechtsfolgen“ 2. Auflage 2020 Rn. 19.
[40] Art. 32 Abs. 1 lit. a DSGVO.
[41] Erwägungsgrund 26 S. 2 zur DSGVO.
[42] Bischoff „Pseudonymisierung und Anonymisierung von personenbezogenen Forschungsdaten im Rahmen klinischer Prüfungen von Arzneimitteln (Teil I) – Gesetzliche Anforderungen“, erschienen in PharmR 2020, 309 (312).
[43] Bischoff „Pseudonymisierung und Anonymisierung von personenbezogenen Forschungsdaten im Rahmen klinischer Prüfungen von Arzneimitteln (Teil I) – Gesetzliche Anforderungen“, erschienen in PharmR 2020, 309 (312).
[44] Bischoff „Pseudonymisierung und Anonymisierung von personenbezogenen Forschungsdaten im Rahmen klinischer Prüfungen von Arzneimitteln (Teil I) – Gesetzliche Anforderungen“, erschienen in PharmR 2020, 309 (312).
[45] Erwägungsgrund 28 S.1 zur DSGVO.
[46] Kotter „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?“ 2019, S. 36.

Datenschutzrechtliche Erfordernisse

Rechtfertigung automatisierter Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist regelmäßig unzulässig und nur ausnahmsweise dann rechtmäßig, wenn einer der in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbestände greift.

Einwilligung

Die Einwilligung gemäß Art. 6 Abs. 1, S. 1, lit. a DSGVO in die Datenverarbeitung bildet den zentralen Erlaubnistatbestand bei der Verarbeitung personenbezogener Daten. An die wirksame Einwilligung werden hohe Anforderungen gestellt. So muss die Einwilligung zum einen ausdrücklich im Wege einer eindeutig bestätigenden Handlung erteilt werden.[47] Die Einwilligung ist formfrei und kann daher auch in elektronischer Form erfolgen.[48] Wegen der Nachweispflicht des Verwenders gem. Art. 7 Abs. 1 DSGVO ist allerdings die Speicherung der Einwilligung zweckmäßig.
Vor diesem Hintergrund scheidet (auch) das bloße Geschehenlasssen, des Gefilmtwerdens, mit Blick auf die gegebenenfalls mittels Symbolisierung auf Fahrzeug bzw. Schildern kenntlich gemachten Kameraaufzeichnungen der Fahrumgebung als Einwilligung aus.
Darüber hinaus muss die Einwilligung freiwillig erteilt werden.[49] Freiwilligkeit erfordert insbesondere, dass den Betroffenen eine informierte Entscheidung ermöglicht wird, also ihnen ausreichend Informationen darüber vorliegen, welche konkreten Daten erfasst und durch wen und für welche Zwecke diese anschließend verwendet werden. Entscheidend ist, dass die Betroffenen die Tragweite ihrer Einwilligungserklärung erfassen können.[50] In der Praxis kann es fraglich sein, ob Betroffene das Ausmaß ihrer Einwilligung angesichts der Komplexität möglicher Datenverarbeitungsszenarien tatsächlich abschätzen können. Aus diesem Grund verbleibt häufig ein Restrisiko, dass die Einwilligungserklärung später angreifbar ist.[51]
In dem Zusammenhang ist das Kopplungsverbot aus Art. 7 Abs. 4 DSGVO zu beachten, welches Freiwilligkeit ausschließt, wenn die Vertragserfüllung von der Einwilligung in die Verarbeitung von personenbezogenen Daten, welche für die Erfüllung des Vertrags nicht erforderlich sind, abhängig gemacht wird.
Die Einwilligung ist zudem mit Wirkung für die Zukunft jederzeit frei widerruflich, worüber der Betroffene in einfacher und verständlicher Sprache vorab aufzuklären ist, vgl. Art. 7 Abs. 3 DSGVO. Die hohen Anforderungen an die Wirksamkeit der Einwilligung und die jederzeitige Widerrufsmöglichkeit machen die Einwilligung zu einem unsicheren Rechtfertigungstatbestand. Die Einwilligungsmöglichkeit wird auch nur in solchen Fällen relevant, in denen eine Form von Kontakt zwischen Verwender und Betroffenem besteht, sodass die Einwilligung im Vorfeld nicht denkbar ist. Passanten und andere Verkehrsteilnehmer sind unbekannte Dritte und nicht Parteien eines Vertragsverhältnisses[52] mit dem Verwender, sodass eine Rechtfertigung gemäß Art. 6 Abs. 1 S. 1 lit. b DSGVO ausscheidet.

Mit Blick auf neue Mobilitätskonzepte, welche sich dadurch auszeichnen, dass der „Fahrzeugerwerb“ sukzessive zu einer Mobilitätslösung inklusive Kommunikation und Unterhaltung wird und sich in komplexe,

[47] BeckOK DatenschutzR/Albers/Veit, 31. Ed 1.11.2019, Art. 6 DSGVO Rn. 24.
[48] Kotter „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?“ 2019, S. 33.
[49] Metzger, GRUR 2019, 129 (131).
[50] Kotter, Philip „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?“ 2019, S. 33.
[51] Lüdemann, ZD 2015, 247 (253).
[52] Steege, MMR 2019, 509 (511).

vielgestaltige Mobilitätsverträge zwischen einer Vielzahl von Vertragsparteien auffächert, ist eine unterschiedliche datenschutzrechtliche Beurteilung erforderlich.[53]
Neue Geschäftsmodelle (z.B. zusätzliche Serviceangebote für Navigation und Parken und „All-Inclusive-Lösungen) bedingen entsprechende neue Vertragsleistungen (z.B. separate Serviceverträge zwischen Fahrern und Herstellern[54], teilweise aber auch integriert in den Kaufvertrag[55]) und Vertragspartner (z.B. Drittanbieter), welche neben die klassischen Vertragsschwerpunkte (Kauf, Miete Leasing etc.) und Vertragspartner (Hersteller, Händler, Käufer bzw. Leasingnehmer, Mieter usw.) treten. [56]
Je nach Vertragsausgestaltung und beteiligten Vertragspartnern können verschiedene Datenverarbeitungen anfallen und unterschiedliche Personen betreffen, sodass sich mit Blick auf die Einwilligung eine schematische Einordnung verbietet.
Dies gilt insbesondere, wenn die vertragliche Leistung auch von vertragsunbeteiligten Dritten (z.B. Eheleute, Kinder, Gebrauchtwagenkäufer etc.) genutzt wird.[57]
Der ursprünglich, beispielsweise zwischen Käufer und Hersteller, abgeschlossene Vertrag vermag nur die Vertragsparteien zu binden und nicht zu Lasten Dritter die Verarbeitung personenbezogener Daten regeln.[58] Zwar kann die Einwilligung stellvertretend erteilt werden, dies setzt aber die Kenntnis des Vertretenen voraus, was mit Blick auf sämtliche zukünftige Nutzer nicht durchführbar ist.[59]
Insgesamt gilt es daher, für jeden Fall gesondert zu prüfen, welche Personen, in welchen Rollen beteiligt sind und welche Datenflüsse anfallen.

Denkbar erscheint es, die Einwilligung für den in Anspruch genommenen Service vor jedem Fahrtantritt durch den jeweiligen Nutzer einzuholen,[60] oder für die verschiedenen Fahrzeugnutzer (die anders als der Fahrzeugerwerber nicht vertraglich einwilligen können) Fahrprofile im Fahrzeug anzulegen, deren persönliche En Einstellungen jederzeit durch die Nutzer geändert werden können[61].
Sinnvoll wäre es, bei sämtlichen vertraglich vorgesehenen Verarbeitungen personenbezogener Daten, welche für die Datenbank relevant sind in dem jeweiligen Rechtsverhältnis neben der vertragsspezifischen Einwilligung auch eine Einwilligung zur nachträglichen Nutzung zu Forschungszwecken einzuholen.

Zu beachten ist in dem Zusammenhang, dass eine (widerrufene) Einwilligung unter Umständen den Rückgriff auf eine gesetzliche Rechtfertigungsrundlage verbauen kann, wenn in der betroffenen Person das

[53] Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 60 f.
[54] „Mercedes-Me“ (Mercedes Benz) und „On-Star“ (Opel), vgl. Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62.
[55] z.B. „BMW-Connected-Drive-Vertrag“, vgl. Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62 f.
[56] Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 60 ff.
[57] Brink/ Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 83.
[58] Brink/ Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 84.
[59] Brink/ Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 84.
[60] Brink/ Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 85.
[61] Brink/ Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 86.

(schutzwürdige) Vertrauen geweckt wurde, dass die Datenverarbeitung nur im Rahmen der Einwilligung erfolgt.[62] Aus diesem Grund ist ein Hinweis sinnvoll, dass die Daten auch nach Wegfallen der Einwilligung auf anderer Grundlage verarbeitet werden können.[63]

Erforderlichkeit der Verarbeitung für die Erfüllung eines Vertrags mit der betroffenen Person

Die Datenverarbeitung ist daneben rechtmäßig, wenn sie für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist, vgl. Art. 6 Abs. 1 S. 1 lit. b DSGVO. Der bloße Bezug zu dem Vertragsverhältnis, reine Zweckdienlichkeit und ein wirtschaftlicher Nutzen genügt nicht, entscheidend ist, ob der Vertrag nur durch die Datenverarbeitung durchgeführt und erfüllt werden kann.[64] Welche Datenverarbeitungen als erforderlich anzusehen sind, ist im konkreten Fall im Rahmen einer umfassenden Interessenabwägung zu ermitteln.[65]Mit Blick auf neuartige Geschäftsmodelle, gerichtet auf den Fahrzeugerwerb oder fahrzeugbezogene Leistungen kann die Verarbeitung personenbezogener Daten in bestimmten Fällen auch zur Vertragserfüllung erforderlich und somit gerechtfertigt sein.[66] Dies ist etwa der Fall, wenn die Datenverarbeitung als solche erst die Fahrfunktion ermöglicht.[67] Anders verhält es sich mit Blick auf Datenverarbeitungen, welche zusätzliche personenbezogene Daten zwecks Personalisierung von Leistungen generieren wollen.[68] Handelt es sich um sensible Daten, so ist eine Rechtfertigung der Verarbeitung gemäß Art. 6 Abs. 1 lit. b DSGVO ausgeschlossen.[69] Als Option bleibt in diesen Fällen nur die Einwilligung, welche dann ausdrücklich und zu einem festgelegten Zweck erfolgen muss, Art. 9 Abs. 2 lit. a DSGVO.

Erforderlichkeit der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen

Eine Datenverarbeitung ist auch rechtmäßig, wenn sie erforderlich für die Erfüllung einer rechtlichen Verpflichtung ist, vgl. Art. 6 Abs. 1 S. 1 lit. c DSGVO. Eine solche gesetzliche Verpflichtung zur Erhebung der in Rede stehenden Daten existiert mit Blick auf den konkret in Rede stehenden Sachverhalt (Szenariendatenbank zur Bewertung der Sicherheitswirkung automatisierter Fahrfunktionen) bislang nicht. Die europäischen Mitgliedstaaten haben aber in diesem Zusammenhang selbst die Möglichkeit Datenverarbeitungen zu rechtfertigen, in dem sie entsprechende rechtliche Verpflichtungen schaffen.[70] Für das Vorliegen einer Rechtsgrundlage kommt es maßgeblich auf die Einordnung als „Rechtsnorm mit unmittelbarer Außenwirkung“ an.[71] Die mitgliedstaatliche Ausgestaltung kann daher durch formelles Gesetz von Bund- und Ländern durch Rechtsverordnung und Satzung juristischer Personen des öffentlichen Rechts erfolgen.[72] Nicht in Betracht kommen daneben Verwaltungsvorschriften, da ihnen die Außenwirkung fehlt.[73] Vorausgesetzt wird,

[62] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
[63] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
[64] Brink/ Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 77.
[65] BeckOK DatenschutzR/Albers/Veit, 31. Ed 1.11.2019, Art. 6 DSGVO Rn. 32.
[66] Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62 f.
[67] Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 64.
[68] Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 73.
[69] Art. 9 Nr. 1 DSGVO.
[70] Ebenda Rn. 55.
[71] Frenzel in Paal/Pauly, DS-GVO BDSG, Art.6, 3. Auflage, 2021, Rn. 35.
[72] Albers/ Veit in BeckOK DatenschutzR, Stand: 1.5.2020 Art. 6 DSGVO, Rn. 58.
[73] Frenzel in Paal/Pauly, DS-GVO BDSG, Art.6, 3. Auflage, 2021, Rn. 36.

dass der Zweck der Datenverarbeitung in der Rechtsgrundlage entweder festgelegt wird und zur Erfüllung einer Aufgabe erforderlich ist, oder sich aus dem Kontext der Aufgabe zur deren Erfüllung er erforderlich ist, ergibt.[74]

Rechtliche Verpflichtungen zur situativen Datenspeicherung bestehen etwa mit Blick auf die Klärung von Beweisschwierigkeiten beim Einsatz automatisierter Fahrzeuge, vgl. § 63 a StVG.

Entsprechende rechtliche Verpflichtungen sind auch in dem im Juli 2021 verabschiedeten Gesetz zum autonomen Fahren[75] enthalten.

Erforderlichkeit der Verarbeitung zum Schutz lebenswichtiger Interessen einer natürlichen Person

Die Datenverarbeitung ist auch rechtmäßig, wenn die Verarbeitung erforderlich ist, „um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“, vgl. Art. 6 Abs. 1 S. 1 lit. d DSGVO.

Erforderlichkeit der Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt durch den Verantwortlichen

Gemäß Art. 6 Abs. 1 S. 1 lit. e DSGVO ist die Datenverarbeitung weiterhin rechtmäßig, wenn sie erforderlich für die Wahrnehmung einer Aufgabe ist, „die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.“ In diesem Zusammenhang wird den einzelnen Mitgliedsstaaten ermöglicht, durch die Regulierung entsprechender Aufgaben im öffentlichen Interesse etc. den dafür erforderlichen Datenverarbeitungen den Rechtsboden zu bereiten.[76]

Gemäß Art. 21 Abs. 1 S. 1 DSGVO hat die betroffene Person das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Absatz 1 lit. e oder f DSGVO erfolgt, Widerspruch einzulegen.

Folge des Widerspruchs ist aber, anders als bei dem Widerruf der Einwilligung zunächst lediglich eine Prüf- und Abwägungspflicht seitens des Verantwortlichen. Gemäß Art. 21 Abs. 1 S. 1 DSGVO erarbeitet der Verantwortliche die personenbezogenen Daten nicht mehr, „es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“.

Die betroffene Person hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen, das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist, vgl. Art. 18 Abs. 1 lit. d DSGVO.

Gemäß Art. 21 Abs. 6 DSGVO gilt das Widerspruchsrecht mit Blick auf Forschungsdaten nur mit Einschränkungen. Eine Datenverarbeitung zu wissenschaftlichen Zwecken kann trotz Widerspruchs fortgesetzt werden, wenn die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich

[74] Art. 6 Abs. 3 UAbS. 2 S.1 DSGVO.
[75] Vgl. Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, BGBl. 2021 I 3108, § 1 g StVG.
[76] BeckOK DatenschutzR/Albers/Veit, 31. Ed 1.11.2019, Art. 6 DSGVO Rn. 55.

ist. Das Widerspruchsrecht wird also eingeschränkt, wenn dadurch der Forschungszweck unmöglich gemacht oder ernsthaft beeinträchtigt würde, vgl. Art. 27 Abs. 2 S. 1 BDSG, wobei die Abwägungen zu dokumentieren sind[77].

Interessenabwägung

Die Datenverarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO schließlich dann rechtmäßig, wenn die Datenverarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Für die vor diesem Hintergrund vorzunehmende Interessenabwägung obliegt dem Betroffenen die Darlegungslast, sodass bei einem Gleichgewicht der Interessen dem Verarbeitungsinteresse der Vorzug gegeben wird.[78]

Denkbare berechtigte Interessen sind zum einen die gemeinschaftsnützliche Erhöhung der Verkehrssicherheit[79] und zum anderen die Forschung.

Der Nutzer ist gem. Art. 13 Abs. 1 lit. c DSGVO über die verfolgten berechtigten Interessen, welche rechtlicher, wirtschaftlicher und ideeller Natur sein können, zu informieren.[80] Wie bei einer Verarbeitung gemäß Art. 6 Abs. 1 S. 1 lit. e DSGVO ist die betroffene Person auch bei einer Datenverarbeitung gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO berechtigt, der Datenverarbeitung gemäß Art. 21 Abs. 1 S. 1 DSGVO zu widersprechen.

Relevante Rechtfertigungstatbestände mit Blick auf die in die Datenbank eingespeisten Forschungsdaten

- Freiwillige informierte und bestimmte Einwilligung der Fahrzeugeigentümer im Vertrag zwischen Eigentümer und Hersteller, die sich auf die Datenweitergabe zu dem konkreten Forschungszweck (Szenariendatenbank zur Überprüfung der Sicherheitswirkung hochautomatisierter Fahrfunktionen) erstreckt. Zu beachten ist in dem Zusammenhang, dass eine (widerrufene) Einwilligung unter Umständen den Rückgriff auf eine gesetzliche Rechtfertigungsrundlage verbauen kann, wenn in der betroffenen Person das (schutzwürdige) Vertrauen geweckt wurde, dass die Datenverarbeitung nur im Rahmen der Einwilligung erfolgt.[81] Aus diesem Grund ist ein Hinweis sinnvoll, dass die Daten auch nach Wegfallen der Einwilligung auf anderer Grundlage verarbeitet werden können.[82]

- Erforderlichkeit zur Vertrasgerfüllung

- Gesetzlicher Rechtfertigungsgrund in Form der Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO (für private Datenverarbeitende)

Verantwortlichkeit

Adressat datenschutzrechtlicher Anforderungen ist der Verantwortliche und damit „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die

[77] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 25.
[78] Albers/Veit, BeckOK, Datenschutzrecht, Art. 6 DSGVO Rn. 52.
[79] Robrahn/Brehmert, „Interessenskonflikte im Datenschutzrecht - Rechtfertigung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO“ ZD 2018, 291 (292).
[80] Spindler in: Schuster/Spindler/Dalby, Recht der elektronischen Medien, 4. Auflage 2019, Art. 6 DSGVO Rn. 13.
[81] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
[82] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.

Zwecke und Mittel der Verarbeitung“ entscheidet, vgl. Art 4 Abs. 7 DSGVO. Die Verantwortlichkeit folgt aus dem Speicherort und richtet sich folglich danach, ob die Daten lokal im Shuttle oder beim Hersteller in einer zentralen Cloud gespeichert werden usw. Denkbare Verantwortliche, der in Rede stehenden erhobenen (Fahrzeug-)Daten sind zunächst der Hersteller, Verkäufer, Halter und Fahrer,[83] und bei Einspeisung in die Datenbank (sofern der Personenbezug nicht aufgehoben ist) der Datenbankbetreiber.

Allgemeine Datenschutzrechtliche Anforderungen und Pflichten der Verantwortlichen

Datenschutz ist bereits mittels entsprechender Hard- und Software technisch, organisatorisch und durch eine entsprechende Programmierung („privacy by design“ und „privacy by default“[84], vgl. Art. 25 DSGVO) sicherzustellen. Dies gilt insbesondere für das **datenschutzrechtliche Widerspruchsrecht aus Art. 21 DSGVO, das Recht auf Vergessenwerden vgl. Art 17 DSGVO** und das **Transparenzgebot** aus Art. 12 Abs. 1 DSGVO.[85]

Relevant sind außerdem die Grundätze der **Datenminimierung und Datenvermeidung**, vgl. Art 5 DSGVO. Um dem Grundsatz der Datenminimierung Genüge zu leisten, sollte im Rahmen des Möglichen bereits durch die verwendete Soft- und Hardware festgelegt werden, welche Daten zu welchem Zweck verarbeitet werden. Dies erfordert eine Vorabentscheidung darüber, welche Daten als notwendig anzusehen sind und zur Erfüllung des vorbestimmten Zwecks zwingend erhoben werden müssen.[86] Schließlich sind gemäß Art. 32 Abs. 1 DSGVO Datenverarbeitungsvorgänge unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen technisch und organisatorisch abzusichern.

Datenschutzbeauftragte

Öffentliche Stellen sowie nicht-öffentlicher Stellen, welche regelmäßig mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, oder „besonders riskante“[87] Datenverarbeitungen durchführen, sind verpflichtet einen Datenschutzbeauftragten zu bestellen, vgl. Art 37 Abs. 1 DSGVO, § 38 Abs. 1 S. 1 BDSG. Daneben besteht gemäß Art. 37 Abs. 4 S. 1 DSGVO auch die Möglichkeit eine freiwillige Benennung eines Datenschutzbeauftragten vorzunehmen.

Informationspflichten

Besonders relevant ist die in Art. 13 und Art. 14 DSGVO normierte, das Transparenzgebot konkretisierende Pflicht des Verantwortlichen,[88] eine Datenschutzerklärung abzugeben. Gemäß Art 13 DSGVO muss der Verantwortliche Betroffene darüber informieren, welche Daten zu welchen Zwecken auf Grundlage welcher Rechtsnorm (ggf. zur Verfolgung welcher berechtigten Interessen) verarbeitet und wie lange die Daten gespeichert werden.

[83] Forgó, in Oppermann/ Stender-Vorwachs „Autonomes Fahren“, S. 360.
[84] „Privacy by Default“ meint die Quantität, das Ausmaß der Verarbeitung, die Speicherdauer und den Datenzugang, Gierschmann, ZD 2016, 51 (53).
[85] Art. 25 Abs. 1 DSGVO; Paal/Hennemann, NJW 2017, 1697 (1700).
[86] Wiesche, Sauer et al, Management digitaler Plattformen, S. 185.
[87] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 26.
[88] Dix in Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Auflage 2019, Art. 13 DSGVO Rn. 1.

Mit Blick auf Videoaufzeichnungen von der Verkehrsumgebung ist in dem Zusammenhang auf die Möglichkeit gemäß Art. 12 Abs. 7 S. 1 DSGVO, die **Informationen in Kombination mit standardisierten Bildsymbolen bereitzustellen**, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln, hinzuweisen.

Rechenschaftspflichten

In Art. 5 Abs. 2 und Art. 24 DSGVO ist die Rechenschaftspflicht verankert. Maßgebend ist, dass die Betroffenen in die Lage versetzt werden, den konkreten Umfang der Datenverarbeitung nachvollziehen zu können.[89]

Zweckbindung

Schließlich ist das Gebot der Zweckbindung gemäß Art. 5 Abs. 1 lit. b DSGVO zu beachten. Danach dürfen die Daten nur für weitere Zwecke als die ursprünglich verfolgten (z.B. Marketing) verwendet werden, wenn dies von der Rechtsgrundlage für den ursprünglich verfolgten Zweck erfasst ist. Soll die Datenverarbeitung zu einem anderen als dem ursprünglichen erfolgen, muss der betroffene Nutzer erneut gem. Art. 13 DSGVO informiert werden.[90]

Datenschutzfolgenabschätzung

Bestimmte Verarbeitungsformen erfordern zudem eine Datenschutzfolgeabschätzung für den Schutz der betroffenen Personen. Dies ist der Fall, wenn „insbesondere bei Verwendung neuer Technologien, auf Grund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ besteht, vgl. Art. 35 Abs 1 DSGVO (sog. „Schwellwertanalyse“[91]). Eine Datenschutzfolgeabschätzung ist beispielsweise erforderlich, wenn eine umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen vorliegt oder Daten aus verschiedenen Quellen zusammenführt und verarbeitet werden. [92]

Löschpflichten

Art. 17 DSGVO garantiert das „Recht auf Vergessenwerden“ und ist Ausdruck des Grundsatzes der Datenminimierung.[93] Die Löschpflicht ist antragsunabhängig konzipiert, der **Verantwortliche ist verpflichtet, den Löschpflichten eigenverantwortlich nachzukommen**. [94]
Gemäß Art 17 Abs. 1 DSGVO ist der Verarbeitende verpflichtet personenbezogene Daten zu löschen, wenn diese **für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind** und wenn die betroffene Person ihre **Einwilligung widerruft und es an einer weiteren Rechtsgrundlage für die Verarbeitung fehlt**. Zur Löschung verpflichtet ist der Verantwortliche auch, wenn die betroffene Person gemäß Artikel 21 Abs. 1 DSGVO **Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung, beispielweise die Erforderlichkeit der Verarbeitung zu Forschungszwecken vgl. Art 21 Abs. 6 DSGVO**, vorliegen. Auch bei einer **unrechtmäßigen Verarbeitung von personenbezogenen Daten**

[89] Berning „Erfüllung der Nachweispflichten und Beweislast im Unternehmen“, ZD 2018, 348 (351).
[90] Art. 13 Abs. 3 DSGVO.
[91] DSK, „Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf, zuletzt aufgerufen am 21.04.2021.
[92] BfDI, „Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes“, Nr. 4, 5 und 10., https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_Verarbeitungsvorgaenge-DSK.html;jsessionid=40110D8C0A21E4FBD83A71A9B3F4BC8A.1_cid507?nn=9937868, zuletzt aufgerufen a 21.05.2021.
[93] Paal in Paal/Pauly, 3. Aufl. 2021, DSGVO Art. 17 Rn. 7.
[94] Paal in Paal/Pauly, 3. Aufl. 2021, DSGVO Art. 17 Rn. 7.

oder der **Erforderlichkeit aufgrund rechtlicher Verpflichtungen des Unionsrechts oder des nationalen Rechts** besteht eine Löschpflicht.

Sonderstellung von Forschungsdaten

Datenschutzrechtliche Vorgaben mit Blick auf Datenverarbeitungen zu Forschungszwecken sind vorrangig in der **DSGVO** normiert. Diese sieht für den Bereich verschiedene Öffnungsklauseln vor, welche **bundes- und landesrechtliche Regelungen** in gewissen Grenzen erlauben. Vor diesem Hintergrund kommt dem nationalen Recht mit Blick auf Forschungsdaten(schutz) eine wichtige Rolle zu und die Rechtslage kann nur durch das konkrete Zusammenspiel der einschlägigen Vorgaben erfasst werden.[95] Schließlich bestehen auch **bereichsspezifische Vorgaben für Forschungsdaten**, die den allgemeinen Regeln unter Umständen als speziellere Regeln vorgehen,[96] mit Blick auf automatisierte Fahrfunktionen etwa in dem im Juli 2021 in Kraft getretenen Gesetz zum autonomen Fahren im StVG.

Das Verhältnis zwischen Datenschutz und Forschung wird in der DSGVO in Art. 5 Abs. 1 lit. b, Art. 9 Abs. 2 lit. j und Art. 89 DSGVO normiert.[97] Die Verarbeitung personenbezogener Forschungsdaten wird, angesichts des Konflikts von Forschungsfreiheit gemäß Art. 13 GRCh und informationeller Selbstbestimmung gemäß Art. 7 und 8 GRCh, in der DSGVO an verschiedenen Stellen der DSGVO gegenüber zu sonstigen Zwecken verarbeiteten personenbezogenen Daten privilegiert, ausgleichend werden dafür Garantien für die Grundrechte und Freiheiten der, von der Datenverarbeitung betroffenen, Personen gefordert, vgl. Art. 89 Abs. 1, S. 1 DSGVO.[98] Diese Garantien sollen gewährleisten, dass technische und organisatorische Maßnahmen (z.B. die Pseudonymisierung[99] oder Anonymisierung[100]) bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird, vgl. Art. 89 Abs. 1, S. 2 DSGVO.

Definition Forschungsdaten

Mangels einer eigenständigen rechtsverbindlichen Definition des Forschungsbegriffs auf Ebene des europäischen Rechts muss zur Auslegung von Art. 13 GRCh, welcher vom deutschen Artikel 5 Abs. 3 GG inspiriert ist, auf die diesbezügliche Rechtsprechung des Bundesverfassungsgerichts, welche Forschung als „geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen“[101] versteht, zurückgegriffen werden.[102]
Aus Telos und Systematik der datenschutzrechtlichen Privilegierung von Verarbeitungen zu Forschungszwecken folgen weitere Einschränkungen. Insgesamt wird gefordert, dass es sich um Forschung handelt, welche dem Einzelnen als Teil der Gemeinschaft wenigstens indirekt und abstrakt zugutekommt, sodass seine eigenen privaten Interessen bei der gesetzlichen Interessenabwägungen weniger ins Gewicht fallen.

[95] Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen“ Version 1.1 2020 S. 89.
[96] Ebenda.
[97] Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen“ Version 1.1 2020 S. 89.
[98] Rossnagel, “Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (159).
[99] Vgl. Art 89 Abs. 1, S. 3 DSGVO.
[100] Vgl. Art 89 Abs. 1, S. 4 DSGVO.
[101] BVerfGE 35, 79.
[102] Roßnagel, “Datenschutz in der Forschung - Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (158).

Die datenschutzrechtliche Besserstellung gegenüber zu sonstigen Zwecken erhobenen Daten greift daher nur, wenn die Forschung, der **gemeinschaftsnützlichen** zweckgebunden Suche nach der Wahrheit dient.[103] Datenschutzrechtliche Privilegierungen greifen zudem nur für **unabhängige Forschung**,[104] da nur dann der **Erkenntnisgewinn zum Wohle der Allgemeinheit im Zentrum steht** und entsprechende Beschränkungen zu rechtfertigen vermag.[105] Private Finanzierung oder private Eigeninteressen an der Forschung stehen der Unabhängigkeit nicht entgegen, wenn eine **direkte Einflussnahme auf den freien wissenschaftlichen Erkenntnisprozess (z.B. externe Weisungen) oder die Unterordnung unter private (wirtschaftliche) Interessen ausgeschlossen** ist.[106] Auch die Verfolgung politischer Interessen darf den freien wissenschaftlichen Erkenntnisprozess zu Gemeinwohlzwecken, nicht dominieren.
Weiterhin schließt die fehlende **wissenschaftliche Methodik** die Privilegierung aus.[107] Wichtig ist zudem, dass die durch die Forschung erlangten Erkenntnisse **auf Publikation und Kommunikation angelegt** sind, also veröffentlicht werden, denn nur dann kann diese von der wissenschaftlichen Gemeinschaft überprüft werden und zum weiteren Erkenntnisgewinn beitragen.[108]

Garantien für die Rechte und Freiheiten der Betroffenen

Im Gegenzug zu den datenschutzrechtlichen Privilegien für Forschungsdaten wird das Ergreifen geeigneter Maßnahmen für die Rechte und Freiheiten der betroffenen Person gefordert, vgl. Art. 89 Abs. 1 S. 1 DSGVO, deren Gebotenheit vom konkreten Einzelfall abhängt, insbesondere davon, welche personenbezogenen Daten verarbeitet werden und wer an dem Prozess beteiligt ist.[109]
Denkbare Maßnahmen, welche als gesetzliche Gebote Niederschlag gefunden haben,[110] sind die Anonymisierung und Pseudonymisierung der Daten, vgl. Art 89 Abs. 1 S. 3 und S. 4 DSGVO, wenn dies die Zweckerfüllung nicht vereitelt. Denkbar sind in diesem Zusammenhang die Verschlüsselung von Daten bei Übermittlung, Geheimhaltungsvereinbarungen, die Auswahl und konkrete Ausgestaltung des Datenzugangs (Gastwissenschaftsarbeitsplatz, Download oder Remote Access).[111]

Einzelne Privilegierungen

Einschränkungen bzw. Ausnahmen von Betroffenenrechten bestehen etwa mit Blick auf die Zweckbindung für die Weiterverarbeitung für Forschungszwecke, [112] für die Speicherbegrenzung[113], den Bestimmtheitsgrundsatz für die Einwilligung,[114] das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten,[115], die Informations-[116] und Löschpflicht[117].[118]

[103] Weichert, Thilo „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20.).
[104] Krohm in Gola/Heckmann, 13. Aufl. 2019, § 27 BDSG Rn. 14.
[105] Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (19).
[106] Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (19 f.).
[107] Weichert, „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20.).
[108] Weichert, „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20.).
[109] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 23.
[110] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 19.
[111] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 23.
[112] Vgl. Art. 5 Abs. 1, lit. b DSGVO.
[113] Vgl. Art. 5 Abs. 1, lit. e DSGVO.
[114] Erwägungsgrund 33 DSGVO.
[115] Art. 9 Abs. 2, lit. j DSGVO.
[116] Art. 14 Abs. 5, lit. b DSGVO.
[117] Art. 17 Abs. 3, lit. d DSGVO.
[118] Roßnagel “Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (159).

Besonderheiten bei der Einwilligung in Datenverarbeitungen zu Forschungszwecken

Mit Blick auf Forschungszwecke besteht die Besonderheit, dass abweichend von dem Grundsatz, dass die Einwilligung für einen bestimmten Fall erteilt werden muss, unter Umständen ausnahmsweise eine Einwilligung mit einer weiten Zweckfestlegung („*broad consent*“) für bestimmte Bereiche erteilt werden kann, soweit ethische Standards eingehalten werden,[119] da sich Forschungsfragen- und -ziele nicht immer konkret im Vorhinein erfassen lassen.[120] Dies gilt allerdings nur für die Fälle, in denen das Forschungsvorhaben aufgrund seiner konkreten Konzeption bis zum Zeitpunkt der Datenerhebung tatsächlich keine abschließende Zweckbestimmung ermöglicht.[121]

Privilegierung der Zweckbindung

Der Grundsatz der Zweckbindung zielt darauf ab, die Menge der zulässigerweise erhobenen Daten (nur soweit zur Zweckerfüllung erforderlich) und die Speicherdauer (nur solange für Zweck erforderlich) zu begrenzen.[122] Die Datenerhebung darf grundsätzlich nur zu festgelegten Zwecken erfolgen, die Weiterverarbeitung darf nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise erfolgen, vgl. Art. 5 Abs. 1 lit. b DSGVO.
Werden die erhobenen Daten anschließend der wissenschaftlichen Forschung zugeführt, sieht Art. 5 Abs. 1 lit. b DSGVO eine Fiktion der Zweckidentität dahingehend vor, dass eine Unvereinbarkeit mit dem Erhebungszweck nicht anzunehmen ist, wenn wissenschaftliche Forschungszwecke gem. Art. 89 Abs. 1 DSGVO verfolgt werden. Die Privilegierung ermöglicht aber nicht, dass sich der Verantwortliche für die Forschungsnutzung auf die Rechtsgrundlage des Primärzwecks berufen könnte,[123] vielmehr ist eine eigenständige Rechtfertigung der Sekundärverarbeitung zu Forschungszwecken erforderlich.

Eingeschränktes Widerspruchsrecht bei Datenverarbeitungen auf Grundlage von

Das Widerspruchsrecht gegen die Verarbeitung sie personenbezogener Daten, die aufgrund von Art. 6 Absatz 1 lit. e oder f DSGVO erfolgt, gilt mit Blick auf Forschungsdaten nur eingeschränkt, vgl. Art. 21 Abs. 6 DSGVO (vgl. Erforderlichkeit der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen)

Öffnungsklauseln für die Mitgliedstaaten mit Blick auf die Verarbeitung von Forschungsdaten

Neben den allgemeinen Öffnungsklauseln gemäß Art. 6 Abs. 2 und 3 DSGVO und Art. 9 Abs. 2 DSGVO,[124] erlaubt Art. 89 Abs. 2 DSGVO den Mitgliedstaaten, vorbehaltlich der Bedingungen und Garantien gemäß Art. 89 Abs. 1 DSGVO, Ausnahmen von den Rechten der Betroffenen gemäß Art. 15, 16, 18 und 21 DSGVO zu normieren, insoweit jene Rechte voraussichtlich die Verwirklichung der Forschungszwecke vereiteln oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung der Forschungszwecke erforderlich sind[125]. Davon hat der nationale Gesetzgeber in § 27 Abs. 2 S. 1 BDSG Gebrauch gemacht.[126]

---

[119] Erwägungsgrund 33 S. 1 DSGVO.
[120] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 21.
[121] Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO 3. April 2019.
[122]
[123] Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (21).
[124] Roßnagel „Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (159).
[125] Vgl. Art 89 Abs. 2 DSGVO.
[126] Krohm in Gola/Heckmann, 13. Aufl. 2019, BDSG § 27 Rn. 6.

Haftung für Datenschutzverstöße

Die haftungsrechtliche Verantwortlichkeit weist der DSGVO-Compliance einen besonderen Stellenwert zu. Die Haftung für Datenschutzverstöße folgt neben allgemeinem Vertrags- und Deliktsrecht aus Art 82 Abs. 1 DSGVO. Demgemäß hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Schadensersatzpflichtig sind sowohl Verantwortliche als auch Auftragsverarbeitende. Gehaftet wird für Vorsatz und alle Formen der Fahrlässigkeit, inklusive leichter Fahrlässigkeit.[127]
Ein Auftragsverarbeiter haftet gemäß Art 82 Abs. 2 S. 2 DSGVO „für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat“.
Der Auftragsverarbeiter haftet als, anders als der Verantwortliche, nur für bestimmte Pflichtverletzungen. Verantwortliche und Auftragsverarbeitende können sich durch den Nachweis fehlenden Verschuldens gemäß Art. 82 Abs. 3 DSGVO exkulpieren, wobei sie beweispflichtig sind, anderenfalls wird das Verschulden vermutet[128]. Die Exkulpationsmöglichkeit gem. Art. 82 Abs. 3 gilt nicht beim Handeln eigener Mitarbeiter.[129] **Auch eine ordnungsgemäße Überwachung seiner Mitarbeiter vermag den Verantwortlichen nicht zu befreien, eine Exkulpationsmöglichkeit, welche der Regelung in § 831 BGB entspricht, fehlt**.[130] Ein vertraglicher Haftungsausschluss des Art. 82 DSGVO kommt selbst bei leichter Fahrlässigkeit nicht in Betracht.[131] Selbst die Einhaltung zertifizierter und genehmigte Verhaltensregeln vermögen die Haftung nicht auszuschließen,[132] wohl aber zu reduzieren.
Das Einschalten eines Auftragsverarbeiters gemäß Art. 28 DSGVO als „verlängerter Arm des Verantwortlichen“[133] verlagert eine etwaige Schadensersatzpflicht gesamtschuldnerisch[134], entsprechend dem Verantwortungsanteil,[135] auf mehrere Pflichtige. Die Delegierung von datenschutzrechtlichen Pflichten vermag allerdings keine Enthaftung herbeizuführen. Vielmehr bleiben neben der Begründung neuer Pflichten bei dem Übernehmer[136] gewisse Überwachungspflichten bestehen,[137] deren Verletzung haftungsbegründend wirkt (bspw. Auswahl geeigneter Mitarbeiter, Organisation und Aufsicht z.B. des Auftragsverarbeitenden,[138] sowie Schulung und Kontrolle).

[127] Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1.Auflage 2019, Art. 82 DSGVO Rn. 22.
[128] Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 82 Rn. 23.
[129] Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 82 Rn. 23.
[130] Wybitul/Haß/Albrecht „Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung“, erschienen in NJW 2018, 113 (116).
[131] Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1.Auflage 2019, Art. 82 DSGVO Rn. 25.
[132] Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1.Auflage 2019, Art. 82 DSGVO Rn. 21.
[133] Martini in Paal/Pauly/Martini, DSGVO, BDSG, 3. Aufl. 2021, Art. 28 DSGVO Rn. 2.
[134] Vgl. Art. 82 Abs. 4 DSGVO.
[135] Vgl. Art. 82 Abs. 5 DSGVO.
[136] So jedenfalls die ständige Rechtsprechung mit Blick auf die Delegation öffentlich-rechtlicher Streupflichten vgl. auszugsweise: BGH, Urteil vom 03-10-1989 - VI ZR 310/88, erschienen in NJW 1990, 111 (112).
[137] So jedenfalls die ständige Rechtsprechung mit Blick auf die Delegation öffentlich-rechtlicher Streupflichten vgl. auszugsweise: BGH, Urteil vom 15. 10. 1951 - III ZR 119/50, erschienen in NJW 1952, 61 (61).
[138] Paal „Schadensersatzansprüche bei Datenschutzverstößen - Voraussetzungen und Probleme des Art. 82 DSGVO“, MMR 2020, 14 (17)

Was folgt aus der DSGVO für die Betreiberrolle (Öffentlich, Privat insb. Industriekooperation)

Der Betrieb der Szenariendatenbank ist in unterschiedlichen Konstellationen denkbar. So können neben öffentlichen Stellen, auch juristische Personen des Privatrechts. Eine weitere Option ist, dass nicht nur eine Person des Privatrechts die Betreiberrolle übernimmt, sondern sich mehrere Private, beispielsweise Unternehmen, zur sog. Industriekooperationen zusammenschließen.
Das Datenschutzrecht der DSGVO gilt grundsätzlich sowohl für öffentliche als auch für nicht öffentliche Stellen. Dennoch ergeben sich teils abweichende Bestimmungen, welche mit Blick auf den Datenbankbetreiber relevant sein könnten.
Der zentrale Rechtfertigungstatbestand der Interessensabwägung für Datenverarbeitungsvorgänge gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gilt nur für Konstellationen in den private Akteure als datenverarbeitende Stelle auftreten und dadurch ein „Gleichordnungsverhältnis“ vorliegt.[139] Für die Fälle in denen öffentliche Stellen personenbezogene Daten bearbeiten kann nicht auf die Interessensabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO als Rechtfertigungstatbestand zurückgegriffen werden, da es hierfür einer gesetzgeberischen Regelungsbefugnis in Gestalt einer speziellen Rechtsgrundlage bedarf.[140] Mit Hinblick auf das innovative Konzept der Szenariendatenbank fehlt eine solche Rechtsgrundlage bisher. Demgegenüber besteht mit Blick auf öffentliche Stellen die Möglichkeit, gemäß Art. 6 Abs. 3 DSGVO datenschutzrechtliche Rechtfertigungstatbestände zur Aufgabenerfüllung (mittel- bis langfristig) auf europäischer und nationaler Ebene neu zu schaffen. Diese sind für die Rechtfertigungsgründe nach Art. 6 Abs.1 UAbs. 1 lit. c und e DSGVO maßgeblich, die die Erfüllung einer rechtlichen Verpflichtung oder der Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, dienen. Die hierfür notwendigen Regulierungsvorhaben sind jedoch häufig langwierig und angreifbar. Unter den Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO kann die Schaffung neuer Rechtsgrundlagen zur Datenverarbeitung auch für private Stellen relevant werden, soweit diesen die Wahrnehmung der öffentlichen Aufgabe übertragen wurde.

Neben dem Betrieb durch öffentliche Stellen und juristischen Personen des Privatrechts sind auch sog. Öffentlich-private Partnerschaften (ÖPP)als Betreiber vorstellbar. Die öffentlich-private Partnerschaft wird der sog. „funktionalen Privatisierung“ zugeordnet.[141] Sie zeichnet sich dadurch aus, dass zwar die Aufgabenerfüllung durch Private erfolgt, die Aufgabenverantwortung jedoch dem öffentlichen Träger obliegt.[142] Grundsätzlich können ÖPP sowohl unter den Anwendungsbereich von privatem, als auch von öffentlichem Recht fallen.[143] Für die Zuordnung kommt es maßgeblich auf den Vertragsgegenstand an, der der Partnerschaft zugrunde liegt.[144] Hierbei wird darauf abgestellt, ob die Leistung der Behörde, die dem Vertrag zu Grunde liegt, oder deren Erfüllung hierdurch vereinbart wird selbst dem Öffentlichen Recht zugeordnet wird und die zu erfüllende Leistung der Privaten nicht getrennt betrachtet werden kann.[145]
Durch den Betrieb der Szenariendatenbank werden sowohl private Interessen, wie das Interesse der OEMs an der Weiterentwicklung der automatisierten Fahrzeugfunktionen ihrer Produkte, als auch öffentliche Interessen, wie die Gewährleistung der Sicherheit im Straßenverkehr berührt. Da jedoch nach derzeitiger Rechtslage der Betrieb einer Szenariendatenbank für öffentliche Stellen nicht verpflichtend festgelegt wird,

[139] Frenzel in Paal/Pauly, DS-GVO BDSG, Art.6, 3. Auflage, 2021, Rn. 26.
[140] Frenzel in Paal/Pauly, DS-GVO BDSG, Art.6, 3. Auflage, 2021, Rn. 26.
[141] Ziekow, Öffentliches Wirtschaftsrecht, 4. Aufl. 2016, § 8 Rn. 6. / Bonk/Neumann/Siegel in: Stelkens/Bonk/Sachs, 9. Aufl. 2018, VwVfG § 54 Rn. 75.
[142] Ziekow, Öffentliches Wirtschaftsrecht, 4. Aufl. 2016, § 8 Rn. 6. / Bonk/Neumann/Siegel in: Stelkens/Bonk/Sachs, 9. Aufl. 2018, VwVfG § 54 Rn. 75.
[143] Bonk/Neumann/Siegel in: Stelkens/Bonk/Sachs, 9. Aufl. 2018, VwVfG § 54, Rn. 80.
[144] Bonk/Neumann/Siegel in: Stelkens/Bonk/Sachs. 9. Aufl. 2018, VwVfG § 54, Rn. 54.
[145] Bonk/Neumann/Siegel in: Stelkens/Bonk/Sachs, 9. Aufl. 2018, VwVfG § 54, Rn. 57.

würde die erfüllende Leistung des Betriebs voraussichtlich nicht dem öffentlichen Recht zugeordnet werden. Nach dieser Betrachtung wäre folglich auch eine öffentlich-private Partnerschaft zum Betrieb der Szenariendatenbank nach Privatrecht zu behandeln.

Daneben hat die Ausgestaltung der Szenariendatenbank durch Industriekooperationen den Vorteil, dass die einzelnen Unternehmen durch den Zusammenschluss weniger durch einseitige Interessen geprägt ist.

Zusammenfassung der datenschutzrechtlichen Hürden

1. Rechtsunsicherheit aufgrund fehlender Hilfestellungen für Konkretisierung und Ausfüllung der abstrakten datenschutzrechtlichen Regeln der DSGVO (Was ist Forschung, insbesondere bei der Beteiligung Privater? Wann liegt Anonymisierung vor? usw.)
2. Überkomplexität des deutschen Datenschutzrecht[146]
3. Regelungschaos aufgrund fehlender Harmonisierung von bundes- und landesrechtlichen sowie bereichsspezifischen Vorschriften insbesondere in der Forschungslandschaft[147]
4. Enormer Dokumentationsaufwand (insb. Interessenabwägung, Datenschutzfolgeabschätzung usw.)
5. Drohende eklatante Bußgelder und erleichterte Schadensersatzforderungen bei Zuwiderhandlungen gegen die DSGVO

Nicht-personenbezogene Daten

Nicht-personenbezogene Daten behandelt die Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (im Folgenden: Free-flow-of-non-personal-Data-Verordnung). Nicht-personenbezogene Daten werden definiert als „Daten, die sich ursprünglich nicht auf eine identifizierte oder identifizierbare natürliche Person bezogen"[148]. Nicht-personenbezogene Daten sind aber auch ordnungsgemäß anonymisierte Daten, da diese selbst durch die Verwendung zusätzlicher Daten einer Person nicht zugeordnet werden können.[149]

[146] Weichert „Die Forschungsprivilegierung in der DSGVO", ZD 2020, 18 (18.).
[147] Rücker/ Dienst/ Brandt für das Bundesministerium für Wirtschaft und Energie „Umsetzung der BMWi-Stategie „Reallabore als Testräume für Innovation und Regulierung": Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen (Projekt Nr. 113/19-FL1-2/03), 2021 S. 27
[148] Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, S. 5.
[149] Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, S. 6 unter Verweis auf das Urteil des Gerichtshofs vom 19. Oktober 2016, Patrick Breyer gegen Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779.

Gemischte Datensätze

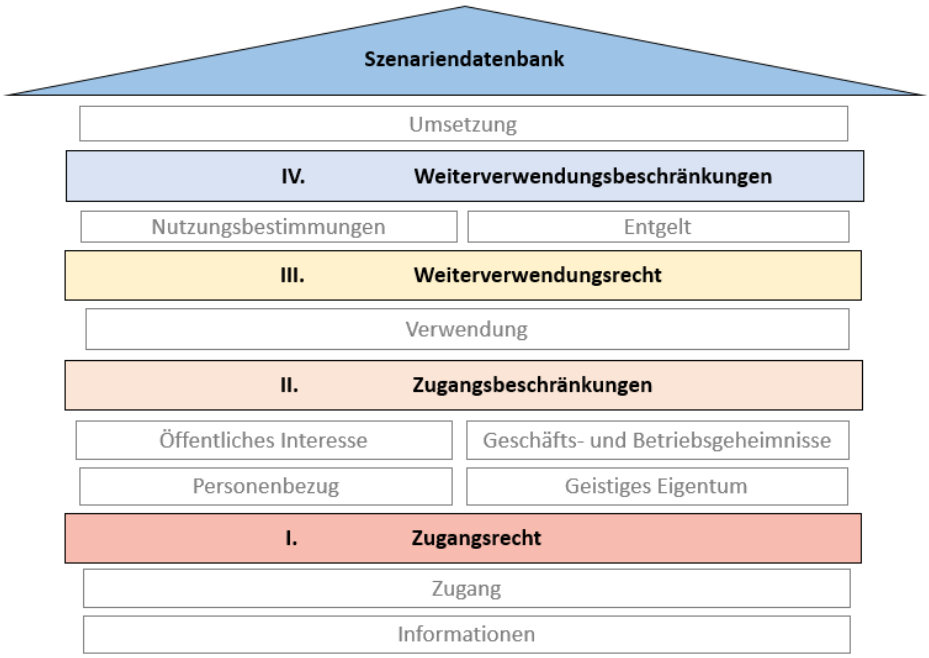
Darüber hinaus können Datensätze nicht lediglich personenbezogene oder nicht-personenbezogene Daten, sondern vielmehr beide Arten enthalten. Derartige gemischte Datensätze, bestehen sowohl aus personenbezogenen als auch aus nicht-personenbezogenen Daten.[150] Sie machen aufgrund der technologischen Entwicklungen den größten Teil der in der Datenwirtschaft geläufigen Datensätze aus (z.B. im Rahmen von IoT, KI und Technologien für die Analyse großer Datenmengen).[151]
Gemäß Art. 2 Abs. 2 der free-flow-of-non-personal-Data-Verordnung gilt dieses nur für den Teil des gemischten Datensatzes, der nicht-personenbezogene Daten enthält. Soweit die Datensätze nicht untrennbar miteinander verbunden sind, ist die DSGVO dagegen auf den gesamten Datensatz anwendbar. Dies gilt auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen.[152] Es zeigt sich insofern, dass in einem Fall, bei welchen ein gemischter Datensatz vorliegt und eine Trennung von personenbezogenen Daten und nicht-personenbezogenen Daten nicht möglich ist, die DSGVO maßgebend ist.

[150] Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, S. 8.
[151] Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, S. 8.
152 Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, S. 8.

Rechtsrahmen Datenzugang und Datenweiterverwendung

Des Weiteren wird der Rechtsrahmen in Bezug auf Datenzugangs- und Datenweiterverwendungsrechte dargestellt. Das folgende Schaubild gibt eine schematische Übersicht, über die Prüfungsschritte, die bei gesetzlichen Ansprüchen auf Datenzugang und Datenweiterverwendung für den zukünftigen Betreiber der Szenariendatenbank zu beachten sind.

Abbildung 3 Systematik: Datenzugangs- und -weiterverwendungsrechte

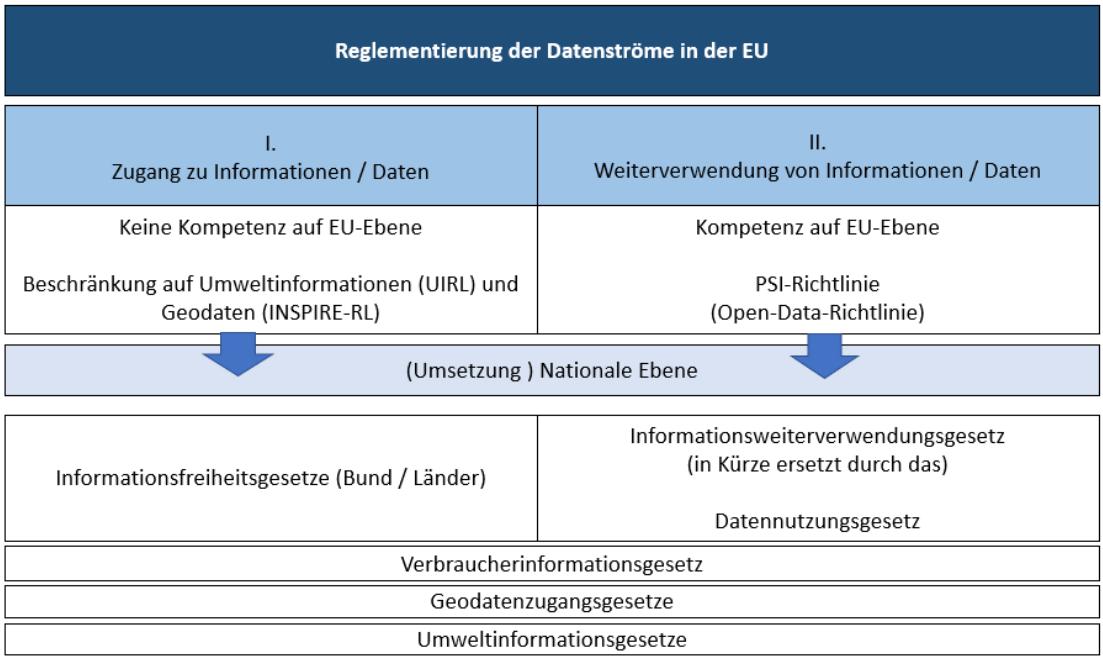


Datenzugangsrechte können durch Zugangsbeschränkungen eingegrenzt werde. Daneben bestehen auch für Weiterverwendungsrechte, die grundsätzlich getrennt von Zugangsrechten zu betrachten sind, Beschränkungsmöglichkeiten. Zur Erfüllung eines Anspruches auf Zugang zu amtlichen Informationen sieht bspw. § 1 Abs. 1 IFG bei Behörden die Erteilung von Auskunft, Gewährung von Akteneinsicht oder die Zurverfügungstellung in sonstiger Weise vor (§ 1 Abs. 2 IFG). In Abgrenzung zum Begriff des Datenzugangs umfasst das Recht auf Weiterverwendung nach § 2 Nr. 3 IWG jede Nutzung von Informationen für kommerzielle oder nichtkommerzielle Zwecke, die über die Erfüllung einer öffentlichen Aufgabe hinausgeht, wobei die intellektuelle Wahrnehmung einer Information und die Verwertung des dadurch erlangten Wissens regelmäßig keine Weiterverwendung darstellen. Grundsätzlich obliegt die Kompetenz zur Regelung des Datenzugangs zu offenen Daten öffentlicher Stellen bei den nationalen europäischen Gesetzgebern.[153] Der Erlass der sog. Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (im Folgenden: **OD-PSI-RL**) in 2003 sollte an der Kompetenzverteilung zwischen EU und Mitgliedsstaaten nichts ändern. Der europäischer Gesetzgeber stellt durch die OD-PSI-RL klar, grundsätzlich alle im öffentlichen

[153] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, S. 535.

Sektor vorhanden Daten zugänglich machen zu wollen, es sei denn, nationale Vorschriften schränken diesen Zugang ausdrücklich ein oder schließen den Zugang aus.[154] Die Entscheidung, ob eine Weiterverwendung genehmigt werde, sollte insoweit auch weiterhin Sache der Mitgliedstaaten bzw. der betreffenden öffentlichen Stelle bleiben.[155] 2019 wurde die OD-PSI-RL neugefasst und an den „Datennutzungsbedarf von Schlüsseltechnologien" angepasst.[156]
Die folgende Abbildung zeigt einen Überblick über europäische und nationale Rechtsakte zur Regelung von Datenströmen. Die Abbildung betrifft die Konstellation in der ein privater Akteur (bsp. Bürger:innen, oder Unternehmen) Zugang zu Informationen des öffentlichen Sektors und/ oder deren anschließende Weiterverwendung begehrt.

Abbildung 4 Reglementierung der Datenströme in der EU



Europäische Gesetzgebung zum Datenzugang

Das europarechtliche Datenzugangs- bzw. -weiterverwendungsrecht wird im Wesentlichen durch die Richtlinien 2003/4/EG über den Zugang der Öffentlichkeit zu Umweltinformationen (im Folgenden: **Umweltinformationsrichtlinie** - UIRL), 2007/2/EG zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (hiernach: **INSPIRE)** und 2019/1024 über die Weiterverwendung von Informationen des öffentlichen Sektors (im Folgenden: **OD-PSI-RL**) geprägt.

[154] Vgl. Erwägungsgrund 8 RL 2013/37 EU.
[155] Vgl. Erwägungsgrund 7 RL 2013/37 EU.
[156] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, S. 535; Richtlinie (EU) 2019/1024 vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Neufassung), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1024&from=DE.

Die europäischen Rechtsakte können nicht isoliert betrachtet werden. Vielmehr bestehen im Anwendungsbereich der Richtlinien teilweise Überschneidungen, wie bspw. bei INSPIRE und der UIRL.[157] Die Ziele der OD-PSI-RL sollen dabei durch die Ziele von **INSPIRE** ergänzt werden.[158] Im Rahmen von Programmen, die durch die EU finanziert werden (bspw. eines Informationssystems für die europäische Verkehrspolitik), soll zur Verbreitung oder Nutzung von Geodaten durch INSPIRE Doppelarbeit vermieden werden.[159]

Zugang zu Geodatensätzen - INSPIRE

INSPIRE regelt die Aufnahme und Nutzung sog. Metadaten, die durch den öffentlichen Sektor innerhalb festgelegter Fristen generiert werden sollen. Sinn und Zweck der Richtlinie ist es den Aufbau einer gemeinsamen europäischen Geodateninfrastruktur zu ermöglichen.[160]
Metadaten sind nach Art. 5 Abs. 2 INSPIRE Informationen, die Geodatensätze und Geodatendienste beschreiben und es ermöglichen, diese zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen. Ein „Geodatensatz“ ist gemäß Art. 3 Nr. 3 INSPIRE eine identifizierbare Sammlung von Geodaten. Nach Art. 3 Nr. 2 INSPIRE sind „Geodaten“ alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geographischen Gebiet.
Thematisch werden Metadaten zu Geodatensätzen nach Art. 6 lit. a INSPIRE nach Anhang I Nr. 7 INSPIRE beispielsweise zu Verkehrsnetzen bereitgestellt. Die Metadaten umfassen auch die zugehörige Infrastruktureinrichtungen für Straßen-, Schienen- und Luftverkehr sowie Schifffahrt. Der Zugriff auf diese Geodatensätze könnte für die Szenariendatenbank und die Zusammensetzung der darin abgebildeten Szenarien relevant sein. Bis 2020 sollen Geodaten nach Anhang I, II und III in interoperablen Datenmodellen organisiert und durch Dienste zur Verfügung gestellt sein (siehe Art. 7 Abs. 3 INSPIRE).[161]

Zugang zu Umweltinformationen – Umweltinformationsrichtlinie

Der Gewährleistung des Rechts auf Zugang zu Umweltinformationen, die bei Behörden vorhanden sind oder für sie bereitgehalten werden, und die Festlegung der grundlegenden Voraussetzungen und praktischer Vorkehrungen für die Ausübung dieses Rechts wird durch die **UIRL** geregelt, vgl. Art. 1 Lit. a) UIRL.
Gemäß Art. 3 Abs. 1 UIRL gewährleisten die Mitgliedstaaten, dass Behörden gemäß den Bestimmungen der UIRL verpflichtet sind, die bei ihnen vorhandenen oder für sie bereitgehaltenen Umweltinformationen allen Antragstellern auf Antrag zugänglich zu machen. Umweltinformationen sind dabei nach Art. 2 Nr. 1 UIRL sämtliche Informationen in schriftlicher, visueller, akustischer, elektronischer oder sonstiger materieller Form über u.a. a) den Zustand von Umweltbestandteilen wie Luft und Atmosphäre, Wasser, Boden, Land, Landschaft und natürliche Lebensräume (…), b) Faktoren wie Stoffe, Energie, Lärm und Strahlung oder Abfall einschließlich radioaktiven Abfalls, Emissionen, Ableitungen oder sonstiges Freisetzen von Stoffen in die Umwelt, die sich auf die unter a) genannten Umweltbestandteile auswirken oder wahrscheinlich auswirken, c) Maßnahmen (einschließlich Verwaltungsmaßnahmen) etc.

[157] Erwägungsgrund 7 der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE).
[158] Erwägungsgrund 8 der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE).
[159] Erwägungsgrund 11 der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE).
[160] BMI, INSPIRE-Flyer, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/geoinformationen/inspire-flyer.pdf?__blob=publicationFile&v=3.
[161] Europäische Kommission, COM (2016), 478final/2, Bericht über die Durchführung der INSPIRE-Richtlinie, 2016, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0478R(01)&from=DE.

Auch die in der UIRL genannten Datenkategorien könnten für die Bildung der Szenarien der Szenariendatenbank relevant sein. Beispielsweise könnte eine „Wildwechselgefahrenzone“ auf lokaler Ebene durch Umweltinformationen nach Art. 2 Nr. 1 Lit. a) UIRL (“Zustand von Umweltbestandteilen wie […] Land, Landschaft und natürliche Lebensräume einschließlich […] die Artenvielfalt und ihre Bestandteile […], sowie die Wechselwirkungen zwischen diesen Bestandteilen,”) gedeckt sein.
Der Zugang zu Umweltinformationsdaten wird gemäß Art. 4 der UIRL nicht ausnahmslos gewährt. Bei einschlägigen Ausnahmen kann die Behörde einen Antrag auf Datenzugang ablehnen. Etwaige Ausnahmetatbestande umfassen u.a. die Fälle, dass die gewünschten Informationen nicht bei der Behörde vorhanden sind, der Antrag offensichtlich missbräuchlich ist, die öffentliche Sicherheit durch Zugang zu den Daten gefährdet werden würde, oder Rechte an geistigem Eigentum verletzt werden könnten.

Nationale Gesetzgebung zum Datenzugang

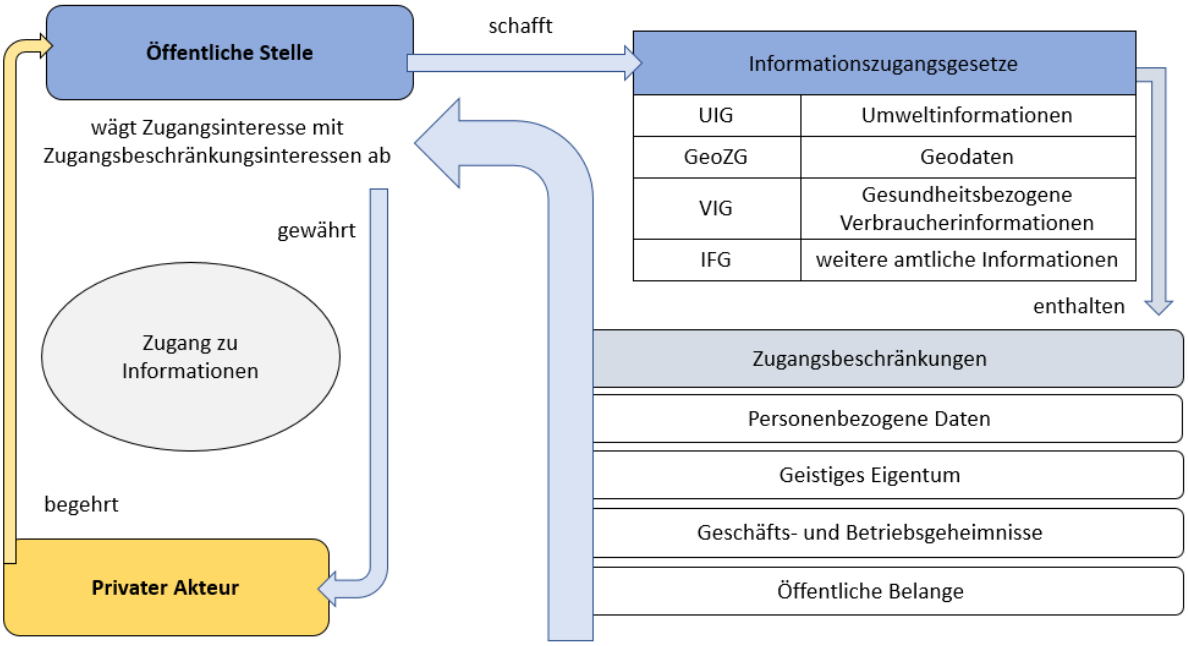
Auf nationaler Ebene wird der Rechtsrahmen des Datenzugangs durch mehrere Rechtsakte ausgestaltet, die miteinander in Wechselwirkung stehen. Die Übersicht über relevante Datenzugangsrechte zur Ausgestaltung der Szenariendatenbank differenziert im Folgenden nach privaten und öffentlichen Akteuren, deren Handlungsoptionen sich unterscheiden.

Zugang privater Akteure zu Informationen von öffentlichen Stellen

Der **Zugang zu amtlichen Informationen** wird national durch das Informationszugangsgesetz (IFG) auf Bundesebene und auf Landesebene durch die Informationszugangsgesetze der Länder und kommunalen Informationssatzungen geregelt. Danach entspricht beispielsweise das Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz Nordrheinwestfalen – IFG NRW) bis auf Einzelheiten dem Aufbau des IFG.

Wie in der Abbildung Abbildung 4 Reglementierung der Datenströme in der EU bereits aufgezeigt, können weitere Gesetze für die Beurteilung des Informationszuganges relevant werden. Hervorzuheben sind hierbei insbesondere die spezifischen Informationszugangsgesetze, wie etwa das Umweltinformationsgesetz (UIG), das Geodatenzugangsgesetz (GeoZG) oder das Verbraucherinformationsgesetz (VIG). Der Zugang kann gegebenenfalls auf Grund gegenläufiger Interessen anderer beschränkt sein. Zu den Gründen der Zugangsbeschränkung gehören der Schutz personenbezogener Daten, des geistigen Eigentums, von Geschäfts- und Betriebsgeheimnissen, sowie öffentlichen Belangen.

Abbildung 5 Zugang zu Informationen



Das **Umweltinformationsgesetz** (UIG) ist ein Informationszugangsgesetz, welches speziell den Zugang zu Umweltinformationen zum Gegenstand hat. § 2 Abs. 3 UIG definiert den Begriff der Umweltinformationen, wie bereits Art. 2 Nr.1 der UIRL. Neben dem Umweltinformationsgesetz des Bundes wird der Zugang zu Umweltinformationen landesrechtlich durch Umweltinformationsgesetze der Bundesländer reglementiert. Als Beispiel sei hier das Thüringer Umweltinformationsgesetz vom 10. Oktober 2006 (ThürUIG) angeführt.[162]

Ferner wird der Zugang zu Informationen im Bereich der Geodaten durch das Geodatenzugangsgesetz (GeoZG) geregelt. Dieses wurde zur Umsetzung der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) geschaffen. Es dient gemäß § 1 Satz 1 GeoZG dem Aufbau einer nationalen Geodateninfrastruktur. Hintergrund ist die Schaffung des rechtlichen Rahmens für den Zugang zu Geodaten, Geodatendiensten und Metadaten von geodatenhaltenden Stellen sowie die Nutzung dieser Daten und Dienste, insbesondere für Maßnahmen, die Auswirkungen auf die Umwelt haben können (§ 1 Satz 2 GeoZG). Gemäß § 3 Abs. 1 GeoZG sind Geodaten alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet. Neben dem GeoZG sind auch die Geodatenzugangsgesetze der Bundesländer zu beachten.[163] Geodaten werden unterschieden in Geobasisdaten (Linien, etwa Straßen) und Geofachdaten. Verkehrsdaten, die für die Einrichtung der Szenariendatenbank relevant sind, könnten daher jedenfalls anteilig als Geodaten anzusehen sein.

[162] Thüringer Umweltinformationsgesetz (ThürrUIG), abrufbar unter: https://landesrecht.thueringen.de/bsth/document/jlr-UIGTHpG1.

[163] Eine Übersicht der Geodatenzugangsgesetze der Bundesländer findet sich auf der Internetpräsenz des BMU, abrufbar unter: https://www.bmu.de/themen/bildung-beteiligung/umweltinformation/umweltinformationsgesetz/uebersicht-der-geodatenzugangsgesetze-der-bundeslaender/.

Zugangsrechte privater Stellen zu Informationen des öffentlichen Sektors nach dem Verbraucherinformationsgesetz (VIG) sind nicht relevant, da die davon umfassten Datensätze für die Szenariendatenbank keinen Mehrwert haben.

Daneben können sich Datenzugangsrechte aus dem Gesetz über den Deutschen Wetterdienst (DWD-Gesetz) ergeben. Dieses betrifft meteorologischen und klimatologischen Daten. So ist etwa eine der Aufgaben des Deutschen Wetterdienstes die Herausgabe amtlicher Warnungen über Wettererscheinungen, die zu einer Gefahr für die öffentliche Sicherheit und Ordnung führen können (§ 4 Abs. 1 Nr. 3 lit. a DWD-Gesetz) oder die in Bezug zu drohenden Wetter- und Witterungsereignissen mit hohem Schadenspotenzial stehen (§ 4 Abs. 1 Nr. 3 lit b DWD-Gesetz). Diese Dienstleistungen an die Allgemeinheit sind gemäß § 6 Abs. 2a Nr. 2 DWD-Gesetz grundsätzlich entgeltfrei.

Zugang privater Akteure zu Informationen anderer privater Akteure

Der Zugang zu Datensätzen im B2B-Bereich kann freiwillig erfolgen, oder unter bestimmten Voraussetzungen durch gesetzliche Ansprüche erzwungen werden.[164] Da gesetzliche Datenzugangsansprüche von Privaten untereinander einen Eingriff in die Privatautonomie darstellen, bedarf es hierfür einer verfassungsmäßigen Rechtfertigung.[165] Da im Verhältnis zwischen privaten Akteuren die Erfüllung einer öffentlichen Aufgabe als legitimer Zweck ausscheidet, sind Datenzugangsansprüche außerhalb des Wettbewerbsrechts schwer begründbar.[166] Der in § 20 Abs. 1a GWB aufgenommene kartellrechtliche Anspruch auf Datenzugang privater Akteure untereinander wurde durch das GWB-Digitalisierungsgesetz geschaffen.[167] Hiernach kann die Verweigerung des Zugangs zu bestimmten Datensätzen gegen ein angebotenes angemessenes Entgelt eine unbillige Wettbewerbsbeschränkung darstellen. Bei der vertraglichen, freiwilligen Vereinbarung zum Datenaustausch im B2B-Bereich wird primär aus ökonomischen Überlegungen gehandelt und die Nutzung gegen Entgelt vereinbart. Daneben besteht die Möglichkeit der sog. „Datenspende" aus altruistischen Gründen.[168] Unternehmen setzen beides bisher in der Praxis jedoch nur zurückhaltend um.[169]

Zugang öffentlicher Stellen zu Informationen privater Akteure

Betrachtet man die Konstellation, in welcher der Staat Datenzugang von einem privaten Akteur verlangt, ist festzuhalten, dass dies für gewöhnlich durch Überlassung der Daten durch die Unternehmen auf Grund freiwilliger Vereinbarungen geschieht.[170]
Eigenständige Zugangsrechte zugunsten des Staates sind jedoch im Bereich des Statistikrechts hinsichtlich der Preisstatistik und einem Zugang des Staates zu Scanner-Daten von Supermarktkassen ersichtlich[171]. Die hiervon umfassten Datensätzen haben jedoch für die Szenariendatenbank keinen Mehrwert.

[164] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 536.
[165] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 536.
[166] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 536.
[167] GWB-Digitalisierungsgesetz, Verabschiedet am 14.02.2021, Bestimmungen treten in Zeitpunkten zwischen dem 05.01.2021 und dem 01.01.20222 in Kraft.
[168] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 536.
[169] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 536.
[170] Vgl. Richter, Zugang des Staates zu Daten der Privatwirtschaft, ZRP 2020, 245.
[171] Gesetz zur Änderung des Gesetzes über die Preisstatistik v. 10.12.2019, Art. 1 Nr. 7 und Nr. 8.; vgl. Richter, a.a.O., 247; Dieser berücksichtigt bei seiner Begutachtung auch rechtsvergleichend die Rechtslage in anderen Staaten. Richter erkennt im Bereich des Statistikrechts einen europaweiten Trend. Derartige Vorhaben lägen in Bezug auf die Bundesrepublik Deutschland jedoch ”weitgehend auf Eis”. Er führt diesbezüglich die Digitale Agenda des Statistischen Bundesamtes an (Fn. 32 ”Vgl. Statistisches Bundesamt, Digitale Agenda, 2019, S. 24 Pkt. B10”).

Auch im Bereich der Daseinsvorsorge können staatliche Stellen auf Daten aus der Privatwirtschaft zurückgreifen, soweit dies mit dem Grundsatz der Privatautonomie vereinbar ist.[172] Anwendungsbeispiele hierfür sieht das neue PBefG für Daten vor, die mit öffentlichen Mitteln finanziert sind.[173] Personenbefördernde Unternehmen werden nach § 3 a PBefG hiernach verpflichtet, dynamische und statische Mobilitätsdaten zu übermitteln.[174]
Daneben wurden Datenspeicherungs- und Übermittlungspflichten an öffentliche Stellen durch das Gesetz zum autonomen Fahren 2021 eingeführt.

Datenweiterverwendung

Wie der Rechtsrahmen des Datenzugangs, wird auch die Thematik der Datenweiterverwendung durch europäische und nationale Vorschriften bestimmt. Diese werden im Einzelnen beschrieben.

Europäische Gesetzgebung zur Datenweiterverwendung

Die ursprüngliche Fassung der Richtlinie 2003/98/EG wurde durch die Richtlinie 2013/37/EU geändert und anschließend durch die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors ersetzt (OD-PSI-RL)[175]. Sie bezweckt das ”Potenzial der Informationen des öffentlichen Sektors”[176] auszuschöpfen. Entsprechend des Grundsatzes des Art. 3 PSI-Richtlinie sollen alle vom Anwendungsbereich umfassten Dokumente der Öffentlichkeit für kommerzielle und nicht-kommerzielle Weiterverwendungszwecke zur Verfügung stehen. Die Richtlinie regelt hierzu die Weiterverwendung von Informationen öffentlicher Stellen, nicht jedoch den Zugang zu diesen.
Nach allgemeinem Verständnis bezeichnet das Konzept “offene Daten” (Open Data) solche Daten, die in einem offenen Format vorliegen und von allen zu jedem Zweck frei verwendet, weiterverwendet und weitergegeben werden können.[177] Zur Umsetzung der Open-Data-Richtlinie soll die Bereitstellung von Open Data auch durch ein zweites Open-Data-Gesetz ausgeweitet werden.[178]
Die PSI-Richtlinie beschreibt verschiedene Datenkategorien, die in ihren Anwendungsbereich fallen. Dies sind Forschungsdaten, normale Daten, dynamische Daten und hochwertige Datensätze.
Forschungsdaten sind gemäß Art. 2 Nr. 9 PSI-Richtlinie Dokumente in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt, und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden, oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden.

172 Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 538.
173 Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 538.
174 Personenbeförderungsgesetz (PBefG), abrufbar unter: https://www.gesetze-im-internet.de/pbefg/__3a.html.
175 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, Erwägungsgrund 2.
176 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, Erwägungsgrund 4.
177 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, Erwägungsgrund 16.
178 BMI, Open Data, abrufbar unter: https://www.bmi.bund.de/DE/themen/moderne-verwaltung/open-government/open-data/open-data-artikel.html.

Nach Art. 2 Nr. 8 PSI-Richtlinie sind **dynamische Daten** Dokumente in digitaler Form, die häufig oder in Echtzeit aktualisiert werden, insbesondere aufgrund ihrer Volatilität oder ihres raschen Verhaltens. So werden von Sensoren generierte Daten in der Regel als dynamische Daten angesehen. Diese sollen unmittelbar nach der Erhebung oder, im Falle einer manuellen Aktualisierung, unmittelbar nach der Änderung des Datensatzes über eine API (Application Programming Interface) zur Verfügung gestellt werden.[179]
Hochwertige Datensätze sind laut Art. 2 Nr. 10 PSI-Richtlinie Dokumente, deren Weiterverwendung mit wichtigen Vorteilen für die Gesellschaft, die Umwelt und die Wirtschaft verbunden ist, insbesondere aufgrund ihrer Eignung für die Schaltung von Mehrwertdiensten, Anwendungen und neuer, hochwertiger und menschenwürdiger Arbeitsplätze sowie aufgrund der Zahl der potenziellen Nutznießer der Mehrwertdienste und -anwendungen auf der Grundlage dieser Datensätze. Als thematische Kategorien für hochwertige Datensätze nennt die Liste nach Art. 13 Abs. 1 i.V.m. Anhang I PSI-Richtlinie Georaum, Erdbeobachtung und Umwelt, Meteorologie, Statistik, Unternehmen und Eigentümerschaft von Unternehmen sowie Mobilität. Für 2021 ist als Schlüsselmaßnahme der Datenstrategie der EU-Kommission ein Durchführungsrechtsakt über hochwertige Datensätze vorgesehen.[180]
„Normale" Daten sind solche, die weder dynamische Daten sind, noch zu hochwertigen Datensätzen gehören.[181] Als Definition sind diese nicht in der OD-PSI-RL enthalten und müssen daher in Abgrenzung zu den anderen Datentypen ermittelt werden.

Für die Einrichtung der Szenariendatenbank und die dafür notwendigen Datenströme können hochwertige Datensätze, sowie Forschungsdaten und das Recht auf Weiterverwendung durch die PSI-Richtlinie relevant sein. So können beispielsweise OEMs durch Nutzung hochwertiger Datensätze innovative Softwarelösungen für immer wieder auftretende Probleme im Straßenverkehr erstellen. Diese könnten dann zu einer verbesserten Fahrsicherheit im Hinblick von automatisierten Fahrfunktionen beitragen.

Nationaler Rechtsrahmen Datenweiterverwendungsrechte

In Deutschland wurde das europäische Weiterverwendungsrecht bisher durch das Informationsweiterverwendungsgesetz (IWG) in nationales Recht umgesetzt.

Das IWG soll künftig durch ein Gesetz für die Nutzung von Daten des öffentlichen Sektors (**Datennutzungsgesetz-DNG-E)** abgelöst werden.[182] Am 10. Februar 2021 wurde vom Bundeskabinett ein Gesetzentwurf zum DNG beschlossen.[183] Die Ablösung durch das DNG wird insbesondere eine Verpflichtung mit sich bringen, in Zukunft offene Daten in maschinenlesbaren Formaten nutzbar zu machen.[184] Der Entwurf sieht eine

[179] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung on Informationen des öffentlichen Sektors, Erwägungsgrund 31.
[180] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 15.
[181] Vgl. Buchholz, Die neue PSI-Richtlinie – Wie viel Datenhoheit verbleibt den öffentlichen Unternehmen?, IR 2019, 197, 199.
[182] Referentenentwurf des Bundesministeriums für Wirtschaft und Energie und des Bundesministeriums des Innern, für Bau und Heimat, Gesetz zur Änderung des E-Government-Gesetzes und zur Einführung des Gesetzes für die Nutzung von Daten vom 17. Dezember 2020, S. 1, abrufbar unter:
https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/referentenentwurf-zweites-open-data-gesetz-und-datennutzungsgesetz.pdf?__blob=publicationFile&v=6
[183] BMWi, https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/zweites-open-data-gesetz-und-datennutzungsgesetz.html
[184] BMWi, abrufbar unter:https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/zweites-open-data-gesetz-und-datennutzungsgesetz.html.

1:1 Umsetzung der OD-PSI-RL vor.[185] Auch das DNG-E etabliert keine eigenen Zugangsrechte, oder Bereitstellungspflichten für Akteure. [186] Es greift, soweit ein anderes Gesetz (z.B. IFG) einen Zugang zu Daten normiert, eine gesetzliche Bereitstellungspflicht besteht, oder die Bereitstellung freiwillig erfolgt.[187]

Daneben wird durch den DNG-E § 12 a EGoVG angepasst. Durch den neuen § 12 a EGoVG wird die Bundesverwaltung einheitlich verpflichtet unbearbeitete Daten von sich aus zugänglich zu machen.[188] Auch die mittelbare Bundesverwaltung, wie Körperschaften, Stiftungen des öffentlichen Rechts und Anstalten, ist von der Vorgabe umfasst.[189] Darüber hinaus werden Behörden verpflichtet sog. Open-Data-Koordinator:innen zu etablieren, die als Ansprechpartner:innen auftreten und Daten bestimmen, die zur Veröffentlichung geeignet sind. § 12 a EGovG erstreckt sich zukünftig auch auf Forschungsdaten.

Flankiert werden die Neuerungen im EGovG durch die Open-Data-Strategie, die Mitte Juli 2021 von der Bundesregierung verabschiedet wurde.[190] Ein Handlungsfeld der Open-Data-Strategie ist das Ziel der Verbesserung der Datenbereitstellung.[191] Hiernach unterstützt das BMWi zukünftig die freiwillige Bereitstellung von offenen Daten durch Unternehmen. In einem aufzustellenden Programm werden sektorspezifische Bereitstellungspflichten geprüft und auch Regulierungsansätze aus anderen europäischen Mitgliedstaaten überprüft.[192]

Eine weitere Möglichkeit zur Weiteverwendung von Informationen der öffentlichen Hand für die Privatwirtschaft besteht durch die Nutzung des **Mobilitäts-Daten-Markplatzes** (MDM). Der MDM ist ein zentrales Online-Portal zur Bereitstellung von Verkehrsdaten.[193] Die Daten werden z.B. für ein bundesweites Baustelleninformationssystem der BASt genutzt.[194]

Keine Dateneigentumsrechte als Zuordnungskriterium

Ein sog. Dateneigentumsrecht ist weder zivil- noch verfassungsrechtlich begründet. Daher kann eine Zuordnung von Datenkategorien, die für die Szenarienbildung und die Datenbank relevant sind, nicht über die Inhaberschaft sog. Dateneigentumsrechte erfolgen.

Ihren Ausgangspunkt hat die Diskussion um ein Dateneigentumsrecht in der Frage der rechtlichen Zuordnung von Daten, die durch vernetzte Fahrzeuge generiert werden.[195] Die rechtliche Zuordnung dieser Daten

[185] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 535.
[186] Hartl/Ludin, Recht der Datenzugänge, MMR 2021, 535.
[187] § 2 Abs. 1 DNG-E, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/referentenentwurf-zweites-open-data-gesetz-und-datennutzungsgesetz.pdf?__blob=publicationFile&v=6.
[188] Artikel 1, Änderung des Gesetzes zur Förderung der elektronischen Verwaltung (E-Government Gesetz- EGOvG), abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/referentenentwurf-zweites-open-data-gesetz-und-datennutzungsgesetz.pdf?__blob=publicationFile&v=6.
[189] Art. 1 Nr. 3 h) Änderung des Gesetzes zur Förderung der elektronischen Verwaltung
[190] BMI, Open Data Strategie der Bundesregierung, Juli 2021, abrufbar unter: https://www.bundesregierung.de/resource/blob/992814/1940386/1d269a2ad1b6346fcf60663bdea9c9f8/2021-07-07-open-data-strategie-data.pdf?download=1.
[191] BMI, Open Data Strategie der Bundesregierung, Juli 2021, S. 19.
[192] BMI, Open Data Strategie der Bundesregierung, Juli 2021, S. 22.
[193] BMVI, Mobilitätsdatenmarktplatz, abrufbar unter: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/mobilitaets-daten-marktplatz.html.
[194] BMVI, Mobilitätsdatenmarktplatz, abrufbar unter: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/mobilitaets-daten-marktplatz.html.
[195] BMVI, "Eigentumsordnung durch Mobilitätsdaten", Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive", 2017, siehe Kapitel 3: Rechtliche Erfassung des "Dateneigentums" im geltenden Recht.

ist für die Automobilindustrie und die Ausgestaltung von Geschäftsmodellen im Zusammenhang mit diesen Datenkategorien von hoher Relevanz, da ihnen ein ökonomischer Wert zugeschrieben wird.[196]

Aus zivilrechtlicher Sicht kann die Figur des Eigentums nicht auf Daten angewendet werden, da diese keine Sachen i.S.d § 903 BGB darstellen. § 903 BGB definiert Sachen als körperliche Gegenstände. Diese Körperlichkeit ist bei Daten nicht gegeben. Durch die fehlende Körperlichkeit und den viralen Charakter von Daten ist die dem Sachenrecht innewohnende Publizitätswirkung nicht gegeben.[197] Auch eine Zuordnung möglicher Eigentumsrechte über Datenträger scheidet aus, da solche beispielsweise durch die Speicherung in Clouds nicht greifbar sind. Daneben ist ein sog. Dateneigentumsrecht auch verfassungsrechtlich nicht begründet. Der verfassungsrechtliche Schutzbereich von Art. 14 GG, dem Recht auf Eigentum, orientiert sich an den zivilrechtlich bestehenden Nutzungs- und Verfügungsbefugnissen.[198] Eine vermögensrechtliche Zuordnung zu einem bestimmten Rechtsträger erfolgt daher nicht.[199]

Dieses Ergebnis wird zuletzt durch die Datenstrategie der Bundesregierung aufgegriffen, die die Debatte über einen fair ausgestalteten Zugang zu und Nutzen von Daten ausspricht, jedoch ausdrücklich darauf hinweist, die « Schaffung eines Dateneigentums » nicht zu befürworten.[200]

Zusammenfassung der rechtlichen Hürden aus dem Recht der Datenzugänge und Datenweiterverwertung

6. Das Recht auf Datenzugang und das Recht auf Datenweiterverwendung wird im europäischen und nationalen Rechtsrahmen getrennt betrachtet.

7. Bei der Untersuchung der Rechte auf Datenzugang sind drei Konstellationen zu unterscheiden: Ansprüche von privaten Akteuren gegen öffentliche Stellen, Ansprüche öffentlicher Stellen gegen private Akteure und Ansprüche privater Akteure untereinander. Je nach Betreiberrolle der Szenariendatenbank kommen andere Anspruchsgrundlagen in Betracht.

8. Die erste Konstellation bietet eine Vielzahl von möglichen Datenzugangsansprüchen mit Relevanz für die Szenariendatenbank, die auf nationaler Ebene maßgeblich geprägt werden durch IFG, UIG und GeoZG. Auf europäischer Ebene sind UIRL und INSPRIE maßgeblich.

9. Die zweite Konstellation sieht gesetzliche Übermittlungspflichten mit Relevanz für die Szenariendatenbank im Gesetz zum automatisierten Fahren und dem PBefG vor. Darüber hinaus erfolgt die Datenbereitstellung von Unternehmen für den öffentlichen Sektor in der Regel auf freiwilliger Basis.

[196] BMVI, “Eigentumsordnung durch Mobilitätsdaten”, Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive”, 2017, siehe Kapitel 4: Ökonomische Analyse: Etablierung von Daten als Wirtschaftsgut als Voraussetzung
[197] Kühling/Sackmann, Irrweg „Dateneigentum“, ZD 2020, S. 25.
[198] Eichberger, Rechte an Daten -Verfassungsrechtliches Eigentum an Daten, VersR 2019, S.713.
[199] Eichberger, Rechte an Daten -Verfassungsrechtliches Eigentum an Daten, VersR 2019, S.713.
[200] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 23.

10. Die dritte Konstellation sieht mit Ausnahme im Wettbewerbsrecht keine gesetzlichen Zugangsansprüche vor. Ein Datenaustausch darüber hinaus muss auf freiwilliger Basis zwischen den Akteuren erfolgen.

11. Die freiwillige Vereinbarung zum Datenaustausch im B2B-Bereich erfolgt auf Grundlage von ökonomischen Anreizen (Entgelt u.a.), oder altruistischen Gründen (Datenspende). Allerdings wird dies in der Praxis durch Unternehmen bisher nur zurückhaltend umgesetzt.

12. Der Rechtsrahmen der Datenweiterverwendungsrechte wird durch die OD/PSI-RL bestimmt, die wiederum mit dem geplanten Datennutzungsgesetz (DNG-E) in nationales Recht umgesetzt wird.

13. Dateneigentumsrechte scheiden als Zuordnungskriterium aus.

Ausblick: Europäische und nationale Datenstrategien

Sowohl auf europäischer[201] als auch nationaler Ebene ist der Bedeutung der zunehmenden Digitalisierung für alle Wirtschaftssektoren durch den Erlass sogenannter Datenstrategien Rechnung getragen worden. Die Datenstrategien stellen Handlungspläne für den Fokus weiterer gesetzgeberischer Entscheidungen, sowie Maßnahmenkataloge vor. Dadurch geben die Strategien einen Ausblick auf Themen, die in den kommenden Jahren auf EU- und Bundesebene gleichermaßen eine verstärkte Rolle spielen werden und relevante Impulse für die Konzeption der Szenariendatenbank geben können. Die Impulse umfassen bspw. die Einführung neuer Rollen (z.B. Datentreuhänder) und die Schaffung von Mobilitätsdatenräumen. Durch das Mehrebenensystem der Europäischen Union sind für Mitgliedstaaten jeweils die politischen Strategien auf europäischer Ebene, sowie (falls vorhanden) auf nationaler Ebene relevant. Durch die sog. Politikverflechtung ist die praktische Zusammenarbeit zur Erreichung der Ziele der Digitalisierungsthemen oft unerlässlich.[202]

Europäische Datenstrategie

Die Europäische Datenstrategie beschreibt das Ziel der Etablierung verschiedener gemeinsamer europäischer Datenräume. Neben acht weiteren Datenräumen soll insbesondere die Einführung eines europäischen Mobilitätsdatenraums Europa zum Vorreiter bei der Entwicklung intelligenter Verkehrssysteme, wie etwa bei vernetzten Fahrzeugen, machen.[203] Ziel des Datenraums ist die Erleichterung von Zugang, Zusammenführung und Nutzung der Daten bestehender bzw. künftiger Verkehrs- und Mobilitätsdatenbanken.[204] Daneben soll die Richtlinie über intelligente Verkehrssysteme, einschließlich ihrer Verordnungen, im Jahr 2021, sowie die geltenden EU-Rechtsvorschriften für die Typgenehmigung von Kraftfahrzeugen im 1. Quartal 2021, ausweislich der Strategie, überprüft werden.[205]

Gemeinsame europäische Datenräume

Die Entwicklung der in der europäischen Datenstrategie beschriebenen Datenräume ist noch nicht abgeschlossen, konkrete Voraussetzungen zu deren Verwirklichung liegen bislang nicht vor. Durch den "Rechtsrahmen für die Governance gemeinsamer europäischer Datenräume" können besondere Regelungen zum Umgang mit personenbezogenen Daten zu wissenschaftlichen Zwecken bei Datenbanken im öffentlichen Besitz getroffen werden.[206] Ebenso kann das Konzept des "Datenaltruismus" näher bestimmt werden. Dieses stellt Einzelpersonen frei, die Nutzung ihrer erzeugten Daten unter Berücksichtigung der Anforderungen aus der DSGVO der Allgemeinheit zur Verfügung zu stellen.[207]

[201] Europäische Kommission, Eine europäische Datenstrategie vom 19. Februar 2020, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066&from=DE.
[202] Bpb, Mehrebenensystem, https://www.bpb.de/nachschlagen/lexika/politiklexikon/17835/mehrebenensystem.
[203] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 26.
[204] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 26.
[205] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 33.
[206] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 14.
[207] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 15.

Rechtsakt über Daten

In einem für 2021 in Aussicht gestellten "Rechtsakt über Daten" könnten durch gesetzgeberische Maßnahmen neue Anreize zur gemeinsamen Datennutzung im Privatsektor gesetzt werden.[208] Ebenso wird als Regelungsgehalt explizit die Zusammenarbeit durch gemeinsames Nutzen von Daten im öffentlichen Interesse durch Behörden und Unternehmen genannt.[209] Betont wird, dass mögliche Neuerungen des Datenzugangs durch verbindliche Zugangsrechte sektorspezifisch geprüft werden. Für die Schaffung von gesetzgeberischen Maßnahmen bedarf es "besonderen Umständen", die als Marktversagen in bestimmten Sektoren, die durch wettbewerbsrechtliche Regelungen allein nicht behoben werden können, ausgewiesen sind.[210] Bisher werden im privatrechtlichen Sektor Fragen rund um Nutzungsrechte an gemeinsam erzeugten Daten üblicherweise durch Privatverträge geregelt.[211]

Sowohl die Governance der gemeinsamen europäischen Datenräume als auch die mögliche Schaffung eines Rechtsakts über Daten sind für mögliche Geschäftsfelder und die besondere Ausgestaltung der Szenariendatenbank (insbesondere durch Neuerungen im Bereich Datenzugang für den Verkehrssektor) perspektivisch von Bedeutung. Soweit die Szenariendatenbank als reine Forschungsdatenbank ausgestaltet wird, könnten die Figur des Datenaltruismus sowie besondere Anforderungen aus dem Datenschutzrecht Neuerungen enthalten.

Datenstrategie des Bundes

Die Bundesregierung hat unter dem Titel "Datenstrategie der Bundesregierung - Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum" eine Kabinettsfassung[212] vorgelegt, welche als Unterrichtung[213] dem Bundestag bereits zugegangen ist.

Datenintermediäre und -treuhänder

Die Datenstrategie der Bundesregierung widmet sich neben vielen weiteren Aspekten insbesondere auch dem Anliegen des Schutzes personenbezogener Daten von verschiedenen Blickwinkeln. In der Strategie wird in dem Zusammenhang das Konzept einer sog. Datentreuhänderhaft thematisiert.[214] Die Datentreuhand ist eine Unterform der Datenintermediäre.[215] Bei **Datenintermediären** handelt es sich um Einrichtun-

[208] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 15.
[209] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 15.
[210] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 16.
[211] Europäische Kommission, Eine europäische Datenstrategie, 19. Februar 2020, Eine Europäische Datenstrategie, S. 16.
[212] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 202, https://www.bundesregierung.de/resource/blob/992814/1845634/5bae389896531854c579069f9a699a8f/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1#:~:text=Die%20Datenstrategie%20umfasst%20vier%20Handlungsfelder,bef%C3%B6rdern%20und%20Innovationpoten%2D%20ziale%20heben.
[213] Unterrichtung durch die Bundesregierung, Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum vom 4. Februar 2021, BT-Drs. 19/26450, https://dip21.bundestag.de/dip21/btd/19/264/1926450.pdf.
[214] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 33 ff.
[215] Vgl. etwa Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 34.

gen, die die Gewährung von Zugang zu Daten und eine Verwendung von Daten durch andere Nutzer miteinander verbinden und in vermittelnder Funktion auftreten.[216] Institutionen mit Treuhandfunktionen und/oder Marktplatzfunktionen sowie andere Methoden der Datenvermittlung sind insoweit von diesem Begriff mitumfasst.[217] Datentreuhandmodelle sind damit eine zentrale Option zur Auflösung der widerstreitenden Datenschutz- und Datenverwertungsinteressen.[218]

Datentreuhänder können beispielsweise Dateninfrastrukturen bereitstellen oder sicherstellen, dass das geltende Datenschutzrecht eingehalten wird bzw. eine Anonymisierung vornehmen.[219] Laut Datenstrategie könnte die Datentreuhand Expertenwissen im Bereich der Anonymisierung, Pseudonymisierung sowie der Erstellung synthetischer Datensätze bündeln, Qualitätssicherung der Datensätze gewährleisten, Zugangsrechte verwalten und die Einhaltung einheitlicher Standards sicherstellen.[220]

Des Weiteren wird zur Sicherstellung des Datenschutzrechts und zur Wahrung der Interessen von Verbrauchern die Etablierung sog. **Personal Information Management Systems** (im Folgenden: PIMS) durch die Strategie in Aussicht gestellt.[221] Daneben fordert die Datenstrategie, die Intensivierung des Datenteilens durch eine effizientere Kontrolle des Datenschutzes und der Cybersicherheit zukünftig zu flankieren.[222] Hierbei könnten **öffentliche Prüf- und Zertifizierungslabore**, die die technische Prüfung datenbasierter Produkte und Dienste auf ihre Datenschutzkonformität vornehmen, einen wichtigen Beitrag leisten.[223]

Mobilitätsdatenräume und Gaia-X

Auch auf nationaler Ebene ist die Etablierung eines **Mobilitätsdatenraums** geplant.[224] Ambitionen der Bundesrepublik dahingehend, im autonomen Fahren und bei der Verkehrswende Vorreiter zu werden, soll auf nationaler Ebene durch ein umfassendes Mobilitätsdatennetzwerk der Weg bereitet werden.[225] Daneben betont die Strategie, dass das Projekt Gaia-X maßgeblich vorangetrieben werden soll.[226] Das GAIA-X-Projekt ist ein auf europäische Werte, Open-Source-Anwendungen und interoperable Standards setzendes europäisches Vorhaben, welches die Bereitschaft zum Datenteilen erheblich steigern soll.[227]

[216] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 107.
[217] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 107.
[218] Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne „Die Datentreuhand", MMR-Beil. 2021, 25 (25).
[219] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 34.
[220] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 34.
[221] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 18.
[222] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 20.
[223] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 20.
[224] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 27.
[225] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 28.
[226] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 12.
[227] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 25.

Die Szenariendatenbank könnte als Teil des Mobilitätsdatenraumes und der GAIA-X-Plattform ausgestaltet werden, um einen möglichst hohen Sicherheitsstandard bei der Bewertung von Szenarien des Straßenverkehrs zu erreichen. Insbesondere das Datenteilen im Bereich der Automobilbranche über die nationalen Grenzen hinweg könnte zu einer Verbesserung der Technologie führen. Sollte die Öffnung in Richtung der europäischen Märkte auch zu einer erhöhten Beteiligung unterschiedlicher Akteure führen, könnte dies so zu einer gesteigerten einfließenden Datenmenge führen. Somit können zu Beginn ggfs. bestehende Informationsdefizite im Informationssystem der Szenariendatenbank stückweise schneller behoben werden.

Forschungsdatenzentren

In den nachgelagerten Bereichen und Einrichtungen der Bundesministerien ist die Einrichtung und der Ausbau von **Forschungsdatenzentren**, falls fachlich erforderlich, geplant.[228] Für die datenschutzkonforme Nutzung von Rohdaten können diese als Ansprechpartner fungieren.[229] Ein Datenaustausch für Forschungseinrichtungen untereinander und mit staatlichen Einrichtungen könnte mit Forschungsdatenzentren als Datentreuhänder verwirklicht werden.[230] Diese sollen einen flexiblen, sicheren, rechtskonformen und zum Teil umfangreichen Datenzugang für die Wissenschaft und weitere berechtigte Nutzer ermöglichen.[231]

Bei Ausgestaltung der Szenariendatenbank als Forschungsdatenbank könnte die Einrichtung von Forschungsdatenzentren demnach für das Betriebsmodell relevant werden. Insoweit mit der Szenariendatenbank auch andere Zwecke, wie die Förderung der Datenpotentiale für die wirtschaftlichen Akteure (bspw. OEMs), verfolgt werden, ergeben sich für das Modell weitere Folgefragen. Das Verhältnis von Forschungsdatenzentren als Datentreuhänder bei Datenaustausch mit wirtschaftlichen Akteuren wäre dann näher zu betrachten und die konkrete rechtliche Ausgestaltung abzuwarten.

[228] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 61.
[229] Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 61.
[230] Vgl. Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 35.
[231] Vgl. Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, Kabinettsfassung vom 27. Januar 2021, S. 112.

IT-Sicherheit

Der Gewährleistung von IT-Sicherheit kommt aufgrund der Bedeutsamkeit der Szenariendatenbank für die Sicherheit im Straßenverkehr und damit für Leib und Leben und Sachwerte eine besondere Bedeutung zu. Ein einheitliches Gesetz, das sämtliche Aspekte der IT-Sicherheit regelt, gibt es bisher nicht, vielmehr werden in verschiedenen Gesetzen punktuell Regelungen getroffen.

Zentrales Gesetz ist das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), welches durch das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom Mai 2021 umfangreich geändert wurde, in Teilen treten diese Änderungen erst zum 1. Dezember 2021 in Kraft. Nach § 2 Absatz 2 BSIG bedeutet „Sicherheit in der Informationstechnik" die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. Das BSIG enthält Regelungen zum Schutz kritischer Infrastrukturen und digitaler Dienste. Die Nichtbefolgung der IT-sicherheitsrechtlichen Normen kann zum Entstehen von Ansprüchen gegenüber dem Normadressaten führen, etwa in Form von Schadensersatzansprüchen bei Schäden durch IT-Sicherheitsvorfälle und Rechte infolge von Mängeln.[232]

Kritische Infrastrukturen sind gem. § 2 Absatz 10 BSIG Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Bei digitalen Diensten gem. § 2 Absatz 11BSIG handelt es sich vor allem um Online- Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste.Die Szenariendatenbank fällt weder unter den Begriff der kritischen Infrastruktur noch der digitalen Dienste, bereichsspezifische Regelungen fehlen aufgrund der Neuartigkeit der Datenbank.

Die Authentizität, Vertraulichkeit und Integrität der verwendeten Datensätze und Verarbeitungsprozesse ist nichtsdestotrotz von herausragender Bedeutung für den Wert und die Relevanz des Informationsgehalts der Szenariendatenbank und damit für die anschließenden Nutzungsmöglichkeiten im sicherheitskritischen Automotive-Bereich. Es besteht die Gefahr der Manipulation der Datenbasis (*Data Poisoning*) und damit einhergehend das Risiko falsche Schlüsse aus der Datengrundlage zu ziehen, die Szenarien und damit einhergehend Algorithmen zu verfälschen und (schlimmstenfalls) unsichere Fahrzeuge auf die Straße zu bringen. Dies gilt umso mehr mit Blick auf drohende straf- und haftungsrechtliche Folgen. Um Gefahren wie *Data Poisoning* beispielsweise in Form der Veränderung oder Löschung der Datensätze zu unterbinden, sind zusätzlich zur allgemeinen Netzwerksicherung, Maßnahmen zum Schutz der Daten(-bank) vor missbräuchlichem Einwirken durch unautorisierte Dritte von Anfang an bei der Konzeptionierung der Datenbank mitzudenken. Gesetzliche Bestimmungen und entsprechende Leitlinien und Standards zu der IT-sicherheitsrechtlichen Beurteilung der in Rede stehenden Datensätze fehlen bislang, weshalb die Möglichkeit einer grundsätzlich denkbaren freiwilligen[233] Zertifizierung nach § 9 BSI-G nicht besteht. Orientierung

[232] Riehm/Meier „Rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit", MMR 2020, 571 (573).
[233] Gitter in Hornung/Schallbruch, IT-Sicherheitsrecht, 1. Auflage 2021, § 15 Recht der IT-Sicherheitsbehörden Rn. 52.

können daher lediglich Forschungsberichte und White-Paper liefern. Sinnvoll wäre zum einen die Sicherstellung, dass die Daten nur aus zulässigen Quellen stammen. (z.B. durch digitale Signaturen),[234] und nicht durch unautorisierte Dritte/ in unzulässiger Weise verändert wurden (z.B. Dokumentation der verschiedenen Versionen der Daten). Datenquellen und Datenverarbeitungen innerhalb der Lieferkette sind sämtlich transparent und nachvollziehbar zu dokumentieren und laufend durch zu diesem Zweck errichtete Checkpoints zu überprüfen, um Auffälligkeiten von vornherein nachgehen zu können. Fehler im Endprodukt sind anderenfalls kaum mehr rückverfolgbar.

Denkbar erscheint auch die Klassifizierung der Daten in verschiedene Gütestufen und IT-Sicherheitskategorien, sodass die Nutzer informiert werden, inwieweit Dokumentation und Sicherungsmaßnahmen garantiert werden können. Dadurch werden die Nutzer in die Lage versetzt, selbst entscheiden zu können, ob die Datenqualität/-sicherheit für sie ausreichend ist.

Die Entwicklung gemeinsamer Leitlinien, Standards und Prüfvorschriften für die IT-sicherheitsrechtliche Zertifizierung der Szenariendatenbank könnte zudem einen zusätzlichen Anreiz für die Beteiligten darstellen.

[234] Schmidt/Pruß in Auer-Reinsdorff/Conrad IT-R-HdB, 3. Auflage 2019, § 2 Daten, Datenbanken und Datensicherheit Rn. 449.

Rechtsform der Datenbank

Eine Rechtsform schafft den rechtlichen Rahmen für eine unternehmerische Tätigkeit, ihre Wahl ist von verschiedenen Faktoren wie etwa der Haftung und der Finanzierung abhängig. Das Forschungsprojekt der GIDAS-Datenbank fußt beispielsweise rechtlich auf einem bilateralen Kooperationsvertrag zwischen der BASt und der Forschungsvereinigung für Automobiltechnik e.V. (FAT). Aufgrund des zunehmenden Ausbaus des Projekts wird aktuell über eine geeignete Rechtsform diskutiert.

Nachteile einer bloßen Forschungskooperation

Eine bloße Forschungskooperation generiert aufgrund fehlender rechtlicher Vorschriften[235] indes Rechtsunsicherheit und ist mit großem vertraglichen Aufwand verbunden.
Zudem besteht die Gefahr, dass die Kooperation nach Außen als Einheit auftritt,[236] mit der Folge, dass eine Außen-GbR im Sinne von § 705 BGB vorliegt, für deren Verbindlichkeit die Partner gemäß § 128 HGB analog unbeschränkt haften[237].

Überblick über Kapital- und Personengesellschaften

Im Folgenden soll ein Überblick über die möglichen Rechtsformen einschließlich ihrer Vor- und Nachteile gegeben werden.

Abbildung 6 Überblick über relevante Kapital- und Personengesellschaften

Gesellschaft bürgerlichen Rechts (GbR) – §§ 705 ff. BGB	**Offene Handelsgesellschaft (OHG) - §§ 105 ff. HGB**	**Kommanditgesellschaft (KG) - §§ 161 ff. HGB**	**Aktiengesellschaft (AG) - §§ AktG**	**Gesellschaft mit beschränkter Haftung (GmbH) - GmbhG**
Kapital: kein festes Kapital, keine Mindesteinlage	Kapital: kein Kapital, keine Mindesteinlage	Kapital: kein Kapital, keine Mindesteinlage. Vorgeschrieben ist jedoch eine Einlage in beliebiger Höhe für den Kommanditisten	Kapital: Mindestens 50.000 € (§ 7 AktG)	Kapital: Mindestkapital 25.000 € (§ 5 GmbHG) bzw. Unternehmergesellschaft (ab 1 € Startkapital)

[235] Eberbach, „Eine Rechtsform für Wissenschaftskooperationen –Ausgangspunkte und Grundlagen“ 02/2018, 51 (66).
[236] Geis, · „Forschungskooperationen: Öffentliches oder Zivilrecht? – Positionsbestimmungen und Regelungszuständigkeiten“, 2/ 2018, 77 (81).
[237] Eberbach, „Eine Rechtsform für Wissenschaftskooperationen –Ausgangspunkte und Grundlagen“ 02/2018, 51 (57).

Haftung: Gesellschaft und Gesellschafter haften auch mit ihrem Privatvermögen	Haftung: Gesellschaft und Gesellschafter haften auch mit ihrem Privatvermögen	Haftung: Kommanditisten haften nur in Höhe der Einlage, Komplementäre haften unbeschränkt auch mit ihrem Privatvermögen	Haftung: Begrenzt auf Gesellschaftsvermögen	Haftung: Begrenzt auf Gesellschaftsvermögen
Entscheidungsbefugnis: Sofern im Vertrag nicht anders geregelt vertreten alle Gesellschafter die GbR	Entscheidungsbefugnis: Sofern im Vertrag nicht anders geregelt vertreten alle Gesellschafter die OHG	Entscheidungsbefugnis: Grundsätzlich vertreten die Komplementäre die Gesellschaft, in besonderen Fällen ist die Beteiligung der Kommanditisten erforderlich	Entscheidungsbefugnis: Vorstand	Entscheidungsbefugnis: Geschäftsführer
Besonderheiten: Rechtsform für Nichtkaufleute und Kleingewerbetreibende (dazu im Folgenden)	Besonderheiten: Die OHG ist eine Gesellschaft, deren Zweck auf den Betrieb eines Handelsgewerbes unter gemeinschaftlicher Firma gerichtet ist. Handelsgewerbe ist eine planmäßige, auf Dauer angelegte selbstständige wirtschaftliche Tätigkeit am Markt unter Ausschluss der freien Berufe sowie wissenschaftlicher oder künstlerischer Tätigkeit.[238]	Besonderheiten: Auseinanderfallen der Gesellschafter in persönliche Haftende und Haftungsbeschränkte. Auch diese Rechtsform gilt nur für Kaufleute.	Besonderheiten: Umfangreiche Formalitäten und hohe Gründungskosten239	Besonderheiten: Unter bestimmten Voraussetzungen kann eine GmbH auch „gemeinnützig“ sein, mit den entsprechenden Vorteilen (Steuerliche Vergünstigungen, Image etc.)

[238] Sprau in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 705 Rn. 6.
[239] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, Einf v § 21, Rn. 14.

Eingetragener Verein

Die Rechtsform des Vereins unterscheidet sich grundsätzlich von den oben genannten Rechtsformen. Ein Verein im Sinne des BGB ist ein auf Dauer angelegter Zusammenschluss von Personen zur Verwirklichung eines gemeinsamen Zwecks mit körperschaftlicher Verfassung, wobei sich die körperschaftliche Organisation in einem Gesamtnamen, in der Vertretung durch einen Vorstand und in der Unabhängigkeit vom Wechsel der Mitglieder äußert. Vereine werden unter anderem danach unterschieden, ob sie wirtschaftlich oder nichtwirtschaftlich handeln.
Gemäß § 22 BGB erlangt ein Verein, dessen Zweck nicht auf wirtschaftlichen Geschäftsbetrieb gerichtet ist, die Rechtsfähigkeit durch Eintragung in das Vereinsregister. Dem gegenüber erlangt gemäß § 22 BGB ein Verein, dessen Zweck auf einen wirtschaftlichen Geschäftsbetrieb gerichtet ist (sog. wirtschaftlicher Verein), seine Rechtsfähigkeit durch staatliche Verleihung. § 22 BGB setzt voraus, dass spezielle gesetzliche Vorschriften fehlen, kraft deren ein wirtschaftlicher Verein Rechtsfähigkeit erlangen kann. Sie fehlen praktisch nie, weil der Erwerb der Rechtsfähigkeit bei Erfüllung der gesetzlichen Bestimmungen (z.B. aus dem GmbH-Gesetz, Aktiengesetz, Genossenschaftsgesetz) stets möglich ist.[240] Eine Konzession für einen wirtschaftlichen Verein wird daher nur im absoluten Ausnahmefall erteilt werden.[241]

Nichtwirtschaftlicher Verein

Für die Abgrenzung zwischen nichtwirtschaftlichem und wirtschaftlichem Verein kommt es darauf an, ob der Verein auf einen wirtschaftlichen Geschäftsbetrieb gerichtet ist. Dieser liegt vor, wenn der Verein, der Leistungen am Markt anbietet und wie ein Unternehmer am Wirtschafts- und Rechtsverkehr teilnimmt. Die Absicht, Gewinn zu erzielen, ist nicht erforderlich.[242] Vereine, die in einem äußeren Markt planmäßig und dauerhaft Leistungen gegen ein Entgelt anbieten sind wirtschaftliche Vereine. Ein nichtwirtschaftlicher Verein liegt hingegen vor, wenn der Geschäftsbetrieb im Rahmen einer ideellen Zielsetzung lediglich Nebenzweck ist.
Dieses Nebentätigkeitsprivileg setzt voraus, dass (1.) der Verein eine Tätigkeit ausübt, die einem wirtschaftlicher Verein zuzuordnen ist, (2.) der Verein in der Satzung einen nichtwirtschaftlichen Hauptzweck festgelegt hat und diesen auch tatsächlich verfolgt und (3.) die unternehmerische Tätigkeit dem nichtwirtschaftlichen Vereinszweck funktionell untergeordnet ist.[243] Der BGH hat zudem klargestellt, dass im Rahmen der Frage nach dem Nebenzweckprivileg, ob die wirtschaftliche Tätigkeit dem nichtwirtschaftlichem Hauptzweck untergeordnet ist, die Gemeinnützigkeit nach §§ 51 ff. AO eine ganz wesentliche Indizwirkung für die Nichtwirtschaftlichkeit hat (siehe oben).

Des Weiteren wird bei einem Verein danach unterschieden, ob er in das Vereinsregister eingetragen ist oder nicht. Wird der Verein nicht eingetragen, so spricht man vom nichteingetragenen Verein oder auch nichtrechtsfähigen Verein gem. § 54 BGB. Sowohl der rechtsfähige als auch der nichtrechtsfähige Verein kann Träger von Rechten und Pflichten sein, kann klagen und verklagt werden und Vermögen erwerben.

[240] Mansel in Jauernig, Bürgerliches Gesetzbuch, 18. Auflage 2021, § 22 Rn. 2.
[241] Mansel in Jauernig, Bürgerliches Gesetzbuch, 18. Auflage 2021, § 22 Rn. 2.
[242] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 21 Rn. 2 ff.
[243] Schöpflin in BeckOK BGB, 58. Edition 2021, § 21 Rn. 118, Dazu auch im Folgenden.

Haftung der Vereinsmitglieder und des Vorstands

Der Hauptunterschied der beiden Formen besteht mit Blick auf die Haftung: Zwar haften die Mitglieder in beiden Fällen nicht persönlich für die Verbindlichkeiten des Vereins. Beim nichteingetragenen Verein haften die für den Verein handelnden Personen aber neben dem Verein auch persönlich für Rechtsgeschäfte, die im Namen des Vereins abgeschlossen werden (§ 54 Satz 2 BGB). Handelnde Person ist jede Person, die im Namen des Vereins direkt tätig wird und in irgendeiner Weise als Teil des Vereins in Erscheinung tritt. Beim rechtsfähigen Verein gibt es eine solche persönliche Haftung der Handelnden hingegen nicht.[244]
Soweit es sich um einen nichtwirtschaftlichen Verein handelt, kann eine Eintragung in das Vereinsregister nur erfolgen, soweit der Verein mindestens 7 Mitglieder hat, § 59 Absatz 3 BGB.

Vereinsmitglieder

Gründungsmitglieder können alle natürlichen Personen sein, aber auch juristische Personen, beispielsweise Aktiengesellschaften, Gesellschaften mit beschränkter Haftung, andere rechtsfähige Vereine, Stadtgemeinden und Landkreise oder auch Offene Handelsgesellschaften, Kommanditgesellschaften und nichtrechtsfähige Vereine.[245]
Auch die Bundesrepublik Deutschland kann als Juristische Person des öffentlichen Rechts Vereinsmitglied sein. Juristische Personen des öffentlichen Rechts sind Körperschaften, Anstalten und Stiftungen, vgl. § 89 BGB. Die Körperschaft öffentlichen Rechts ist ein mitgliedschaftlich organisierter, regelmäßig rechtsfähiger Verband, der durch staatlichen Hoheitsakt entsteht und mit eigenen hoheitlichen Befugnissen ausgestattet ist.[246] Der Bund als solcher ist eine Gebietskörperschaft und daher rechtsfähig. So ist beispielsweise beim Goethe Institut e.V. die Bundesrepublik Deutschland gem. § 3 Absatz 3 der Satzung ordentliches Mitglied.[247]

Für die Szenariendatenbank kommt die Beteiligung der Bundesanstalt für Straßenwesen in Betracht. Der Status als juristische Person kommt zwar nur der jeweiligen Körperschaft selbst zu, hier der Bundesrepublik Deutschland. Eine einzelne Behörde hat hingegen keine Rechtspersönlichkeit. Allerdings bestehen in der „Anordnung über die Vertretung der Bundesrepublik Deutschland im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur“ Vertretungsregelungen. Hiernach erstreckt sich die Vertretung auf alle rechtserheblichen Handlungen. Gemäß § 2 Nr. 2 a) gg) der Anordnung ist die Bundesanstalt für Straßenwesen zur Vertretung des Bundes auf alle in ihrem Geschäftsbereich anfallenden Handlungen befugt. Das Vertretungsverhältnis ist mit der Formel „Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Verkehr und digitale Infrastruktur, dieses vertreten durch die Bundesanstalt für Straßenwesen“ zum Ausdruck zu bringen.

Vergleich zwischen GmbH und eingetragenem Verein

Hauptabgrenzungsmerkmal zu einer Gesellschaft ist beim Verein das flexible Hinzutreten und Ausscheiden von Mitgliedern, was etwa bei einer GbR oder GmbH nicht ohne weiteres möglich ist, da die Mitglieder untereinander einen Gesellschaftsvertrag abschließen. Des Weiteren gilt bei einer Gesellschaft das Prinzip der Einstimmigkeit wohingegen bei einem Verein das Mehrheitsprinzip begriffswesentlich ist.[248] Eine Vereinsgründung erfordert in Abgrenzung zu der Gründung einer GmbH darüber hinaus kein Stammkapital

[244] BMJV – Leitfaden zum Vereinsrecht 2016, S. 13.
[245] BMJV – Leitfaden zum Vereinsrecht 2016, S. 14.
[246] Backert in BeckOK BGB, 58. Edition 2021, § 89 Rn. 1.
[247] Satzung des Goethe Instituts vom 21. September 2000 in der Fassung vom 2. Juli 2020.
[248] Schöpflin in BeckOK BGB, 58. Edition 2021, § 21 Rn. 29.

und erfordert keine komplexe Finanzierung und Buchführung. Weder bei einem eingetragenen Verein noch bei einer GmbH haften die Mitglieder bzw. Gesellschafter mit ihrem persönlichen Vermögen.

Abbildung 7 Vergleich GmbH/ eingetragener Verein

GmbH	Eingetragener Verein
Komplexere Bilanzierungs- und Buchführungspflichten	Einfache Einnahmen-Überschuss-Abrechnung
Prinzip der Einstimmigkeit, Entscheidungsbefugnisse abhängig von Anteilen langfristig effizienter	Mehrheitsprinzip, Einfache, basisdemokratische Entscheidungsfindung langfristigwenig effizient
25.000 EUR (UG: mind. 1 EUR)	Kein Stammkapital erforderlich
Mitglieder im Gesellschaftsvertrag festgeschrieben, weniger flexibel	Offener als GmbH, Mitglieder können flexibel hinzukommen und wieder austreten
Keine persönliche Haftung der Gesellschafter	Keine persönliche Haftung der Mitglieder

Gemeinnützigkeit des Vereins oder der GmbH (ggf. UG)

Darüber hinaus besteht die Möglichkeit den Verein oder die GmbH (ggf. UG) gemeinnützig im Sinne der Abgabenordnung zu konzipieren. Durch diese Einordnung ergeben sich insbesondere steuerrechtliche Vorteile. So sind Körperschaften, die ausschließlich und unmittelbar gemeinnützige, mildtätige oder kirchliche Zwecke selbstlos verfolgen, etwa von der Körperschaftssteuer (§ 5 Absatz 1 Nr. 9 KStG) und der Gewerbesteuer (§ 3 Nr. 6 GewStG) befreit, Zuwendungen an sie sind steuerfrei (§ 13 Absatz 1 Nr. 16b, 17 ErbStG), zudem ermäßigt sich die Umsatzsteuer auf 7 Prozent (§ 12 Absatz 2 Nr. 8 UStG). Bedeutsam für die gemeinnützigen Körperschaften und das Steueraufkommen ist auch der Spendenabzug (§ 10b EStG, § 9 I Nr. 2 KStG).[249]
Die Einordnung als gemeinnützig hätte zudem den Vorteil, dass diese gleichzeitig das Vorliegen eines nichtwirtschaftlichen Vereins und einzelner Voraussetzungen der Einordnung als Forschungsdatenbank indiziert. Gemein ist beiden rechtlichen Privilegierungen, der steuerlichen Vergünstigung und der weniger strengen Anforderungen an die Verarbeitung personenbezogener Daten nämlich, dass sie ihren Ursprung darin haben, dass der Einzelne als Teil der Gemeinschaft auch von dem in Rede stehenden Vorhaben profitiert, sodass seine Interessen bei der gesetzgeberischen Interessenabwägung weniger ins Gewicht fallen. So würde durch die Anerkennung der Gemeinnützigkeit gesichert, dass die Forschung nicht kommerziellen privaten Interessen untergeordnet wird und damit das Kriterium der Freiheit und Unabhängigkeit indiziert. Neben den beschriebenen steuerrechtlichen Privilegierungen hat die Einordnung als gemeinnützig auch Imagevorteile, was sich wiederrum günstig auf die Einwilligung in die Verarbeitung personenbezogener

[249] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 51 Rn. 9.

Daten. Schließlich verspricht sich die Gemeinnützigkeit auch positiv auf datenschutzrechtliche Interessensabwägungen auszuwirken. Nachteilig wirkt sich indes das Gewinnausschüttungsverbot[250] zu Lasten der Gesellschafter aus.
Eine Körperschaft verfolgt nach § 52 Abgabenordnung gemeinnützige Zwecke, wenn ihre Tätigkeit darauf gerichtet ist, die Allgemeinheit auf materiellem, geistigem oder sittlichem Gebiet selbstlos zu fördern. Für die Szenariendatenbank kommt sowohl die Förderung auf materiellem als auch geistigem Gebiet in Betracht. Eine Förderung auf „materiellem Gebiet" ist auf die Verbesserung der finanziellen Ausstattung, der wirtschaftlichen Versorgung, allgemein des körperlichen Lebensstandards gerichtet. Hierzu zählen etwa die Förderung des öffentlichen Gesundheits- und Wohlfahrtswesens, die Entwicklungshilfe sowie die mildtätige Unterstützung Hilfsbedürftiger.[251]Auf „geistigem Gebiet" erfolgt eine Förderung, die sich auf das denkende, erkennende Bewusstsein des Menschen bezieht, dessen Erkenntnisfähigkeit verbessert, zum Verständnis des Seins beiträgt oder die verstandesmäßige Wahrnehmung erweitert. Dies geschieht insbesondere durch eine Förderung der Wissenschaft und Forschung, Bildung und Erziehung, Kunst und Kultur. „Fördern" beinhaltet eine auf Entwicklung gerichtete Betätigung, die jemandem hilft, unterstützt, begünstigt oder seine Lage in irgendeiner Weise verbessert. Die Rechtsprechung geht von der Einbeziehung einer Vielzahl von Werten aus, die dem allgemeinen Besten zu nutzen bestimmt sind. Als prägende Faktoren werden angesehen: die verfassungstragenden Grundlinien des Grundgesetzes, die sozialethischen und religiösen Prinzipien, die geistige und kulturelle Ordnung, die Forschung, Wissenschaft und Technik, die vorhandene Wirtschaftsstruktur, die wirtschaftlichen und sozialen Verhältnisse und die Wertvorstellungen und Anschauungen der Bevölkerung.[252]

§ 52 Absatz 2 AO normiert einen Katalog an Beispielen für Förderungen der Allgemeinheit. Für die Konzeptionierung der Datenbank relevant sind die Förderung von Wissenschaft und Forschung (Nr. 1), die Förderung des öffentlichen Gesundheitswesens (Nr. 3) und die Förderung der Unfallverhütung (Nr. 12).
Forschung ist jede Tätigkeit, die mit wissenschaftlichen Methoden zu neuen Ergebnissen der Erkenntnis im Dienste der Wahrheitsfindung zu gelangen sucht. Das Bundesverfassungsgericht definiert den Begriff der Wissenschaft als alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist. [253] Zur wissenschaftlichen Arbeit gehört, dass die Erkenntnisse von der Methodik her nachprüfbar und nachvollziehbar sind. Die der Wissenschaft und Forschung immanente Suche nach neuen Erkenntnissen ist ein besonderes staatliches Anliegen im Interesse des Gemeinwohls.[254]
Aufgabe des öffentlichen Gesundheitswesens ist die Erhaltung und Förderung der Gesundheit der Bürger. Dies geschieht sowohl durch die Verhinderung und Bekämpfung von epidemischen Krankheiten als auch durch Lebensmittelüberwachung, Unfallverhütung, Arbeitsschutz, Bekämpfung des Missbrauchs von Rauschmitteln und die Förderung der Volksgesundheit.[255] Die Förderung der Unfallverhütung gem. Nr. 12 ist ein Teil des öffentlichen Gesundheitswesens.
Die Szenariendatenbank fusioniert Mobilitätsdaten, um automatisiertes Fahren einerseits wissenschaftlich zu entwickeln und begleiten, andererseits aber auch um die Technologien in der Zukunft im Straßenverkehr zu integrieren und die Verkehrssicherheit insgesamt für die Allgemeinheit zu erhöhen. Damit würden sowohl Wissenschaft und Forschung als auch, im Wege der Eindämmung von Verkehrsunfällen, das öffentliche Gesundheitswesen gefördert werden.

[250]Helm/ Haaf in Beck'sches Handbuch der GmbH, 6. Auflage 2021, § 24 Rn. 55.
[251] Koenig in Koenig, Abgabenordnung, 4. Auflage, 2021 § 52 Rn. 9.
[252] Koenig in Koenig, Abgabenordnung, 4. Auflage, 2021 § 52 Rn. 9.
[253] BVerfG 1 BvB 2/51, BVerfGE 5, 85 (146 f.)).
[254] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 52 Rn. 29.
[255] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 52 Rn. 36. Dazu auch im Folgenden.

In § 55 AO wird der Begriff „Selbstlosigkeit“ legal definiert. Hiernach geschieht eine Förderung oder Unterstützung selbstlos, wenn dadurch nicht in erster Linie eigenwirtschaftliche Zwecke – zum Beispiel gewerbliche Zwecke oder sonstige Erwerbszwecke – verfolgt werden. Nicht in erster Linie eigenwirtschaftliche Zwecke verfolgt das Handeln der Körperschaft, wenn dieses durch Verfolgung des gemeinnützigen Zweckes geprägt ist. Die selbstlose Tätigkeit muss den alleinigen Hauptzweck bilden. Eigenwirtschaftliche Zwecke dürfen allenfalls nebenbei, beiläufig, also in ihrer Bedeutung deutlich hinter den steuerbegünstigten Zweck zurücktretende Begleiterscheinungen sein. Die Feststellung der fehlenden Selbstlosigkeit erfordert eine Abwägung zwischen den eigenwirtschaftlichen Vorteilen und der Förderung der Allgemeinheit. Dabei geht es weniger um die prozentuale Gewichtung als vielmehr um eine Entscheidung, inwieweit wirtschaftliche Vorteile, die durch die fördernde Tätigkeit entstehen, zugunsten der Körperschaft oder ihrer Mitglieder noch im Interesse der Gemeinwohlförderung akzeptabel sind.[256]
Weiterhin muss die Förderung ausschließlich und unmittelbar erfolgen. Ausschließlichkeit ist gem. § 56 AO gegeben, wenn eine Körperschaft nur ihre steuerbegünstigten satzungsmäßigen Zwecke verfolgt. Voraussetzung dafür ist zweierlei: Zunächst die alleinige Verfolgung satzungsmäßiger Zwecke und ferner, dass die Satzungszwecke uneingeschränkt steuerbegünstigt sind. Das Nebeneinander mehrerer steuerbegünstigter Satzungszwecke verstößt nicht gegen die Ausschließlichkeit, sondern allein die kumulative Verfolgung begünstigter und nicht begünstigter Zwecke.[257] Laut § 57 AO bedeutet Unmittelbarkeit die Verwirklichung der steuerbegünstigten satzungsmäßigen Zwecke durch die Körperschaft selbst. Entscheidend ist die Zweckverfolgung durch Selbstverwirklichung, also eigenes oder zurechenbares Verhalten Dritter. Eigenes körperschaftliches Handeln erfolgt durch die vertretungsberechtigten Organe der Körperschaft. [258] Demgegenüber würde eine Körperschaft nur mittelbar handeln, wenn sie die gemeinnützigen Zwecke eines anderen Steuerpflichtigen unterstützen würde.

Fazit

Die Rechtformen der GbR, OHG und KG erscheinen aus hiesiger Sicht nicht praktikabel, da sie umfangreiche Haftungsansprüche auch in das Privatvermögen der Gesellschafter begründen.
In Betracht kommt aus Haftungsgründen aus diesem Grund entweder die Ausgestaltung als GmbH oder als eingetragener Verein, wobei die GmbH wohl langfristig der Vorzug einzuräumen ist.
Die Anerkennung als gemeinnützige GmbH hat zahlreiche Vorteile, ist aber nur dann denkbar wenn das Gewinnausschüttungsverbot durch ein passendes Finanzierungsmodell aufgefangen wird. Vor der Gründung eines Vereins oder einer GmbH, welche die Privilegien des § 51 AO aufgrund ihrer Gemeinnützigkeit erhalten soll, ist es ratsam, bereits vor der Gründung mit den zuständigen Finanzbehörden Kontakt aufzunehmen, um so sicherzustellen, dass die Anforderungen des Gemeinnützigkeitsrechts erfüllt sind.

[256] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 55 Rn. 6.
[257] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 56 Rn. 1.
[258] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 57 Rn.2.

Kartell- und Wettbewerbsrecht

Das Zusammenwirken verschiedener Unternehmen zwecks Betriebs einer Forschungsdatenbank muss daneben marktrechtlichen Vorgaben gerecht werden, wobei nicht jeder kooperative Zusammenschluss im Widerspruch zu nationalen und europarechtlichen marktstrukturrechtlichen Vorgaben steht[259]. Nationale Regelungen folgen aus dem Gesetz gegen Wettbewerbsbeschränkungen (GWB). Sofern ein koordiniertes Verhalten von Unternehmen am Markt geeignet ist, den Handel zwischen den Mitgliedstaaten der Europäischen Union zu beeinträchtigen, unterliegt es nicht nur deutschen, sondern auch europäischen kartellrechtlichen Vorgaben aus Art 101 AEUV, welche im Kollisionsfall vorrangig anzuwenden sind.[260]
Gemäß § 1 GWB sind Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken, verboten (**Kartellverbot**). Der Begriff „Vereinbarungen" erfasst sämtliche zivilrechtliche Vertragsarten, und damit auch Gesellschaftsverträge. [261] Kartelle umfassen daher verschiedene Rechtformen, insbesondere Personengesellschaften und Kapitalgesellschaften.[262]
Im Ergebnis kann offen bleiben, ob die jeweilige Kooperation unter den Kartellbegriff fällt, wenn eine Ausnahme greift. Von dem Verbot wettbewerbsbeschränkender Vereinbarungen freigestellt sind Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen oder aufeinander abgestimmte Verhaltensweisen, die zur Förderung des technischen oder wirtschaftlichen Fortschritts beitragen, ohne dass den beteiligten Unternehmen Beschränkungen auferlegt werden, die für die Verwirklichung dieser Ziele nicht unerlässlich sind, oder Möglichkeiten eröffnet werden, für einen wesentlichen Teil der betreffenden Waren den Wettbewerb auszuschalten, vgl. § 2 Abs. 1 GWB. Gemäß § 2 Abs. 2 S. 1 GWB gelten bei der Anwendung von § 2 Abs. 1 GWB die Verordnungen des Rates oder der Europäischen Kommission über die Anwendung von Art. 101 Abs.3 AEUV auf bestimmte Gruppen von Vereinbarungen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen (Gruppenfreistellungsverordnungen) entsprechend. Dies gilt gemäß § 2 Abs. 2 S. 2 GWB auch, soweit die dort genannten Vereinbarungen, Beschlüsse und Verhaltensweisen nicht geeignet sind, den Handel zwischen den Mitgliedstaaten der Europäischen Union zu beeinträchtigen.
Sofern die Forschungskooperation den Voraussetzungen einer unionsrechtlichen Gruppenfreistellungsverordnung entspricht, wird das Vorliegen der Voraussetzungen des § 2 Abs.1 GWB vermutet und der Zusammenschluss von dem Kartellverbot aus § 1 GWB freigestellt.[263]
Eine entsprechende **Gruppenfreistellungsverordnung existiert auch für den Forschungsbereich** (im Folgenden: GFV-Forschung).[264] Gemäß Art. 2 Abs. 1 GFV-Forschung iVm Art. Abs. 3 AEUV und § 2 Abs. 2 S. 1

[259] Oppermann „Marktrecht" in Oppermann/ Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020 Rn. 48.
[260] Mattfeld in Gummert/ Weipert, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 1 f.
[261] Mattfeld in Gummert/ Weipert, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 4.
[262] Mattfeld in Gummert/ Weipert, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 4.
[263] Mattfeld in Gummert/ Weipert, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 13.
[264] VERORDNUNG (EU) Nr. 1217/2010 DER KOMMISSION vom 14. Dezember 2010 über die Anwendung von Artikel 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Mattfeld in Münchener Handbuch des Gesellschaftsrechts Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 15.Union auf bestimmte Gruppen von Vereinbarungen über Forschung und Entwicklung (GFV-Forschung).

GWB gilt Art. 101 Abs. 1 AEUV nicht für Forschungs- und Entwicklungsvereinbarungen. Vereinbarungen über die gemeinsame Durchführung von Forschungsarbeiten oder die gemeinsame Weiterentwicklung der Forschungsergebnisse bis zur Produktionsreife fallen ausweislich der Verordnungserwägungen regelmäßig nicht unter das Kartellverbot.[265] **Die konkreten Freistellungsvoraussetzungen folgen aus Art. 3 Abs. 2-5 GFV-Forschung.** Allerdings ist darauf hinzuweisen, dass die an der Kooperation beteiligten Unternehmen das Risiko der Freistellung, insbesondere die Beweislast mit Blick auf die Freistellungsvoraussetzungen, tragen.[266] Das Risiko umfasst auch die Veränderungen von Marktverhältnissen und rechtlichen Einordnungen.[267] In dem Zusammenhang ist auch auf die limitierte Geltungsdauer der GFV-Forschung. bis Ende 2022 hinzuweisen. Daher empfiehlt sich eine regelmäßige Überprüfung der Freistellungsvoraussetzungen.

[265] Erwägungsgrund 6 GFV-Forschung.
[266] Mattfeld in Münchener Handbuch des Gesellschaftsrechts Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 15.
[267] Mattfeld in Münchener Handbuch des Gesellschaftsrechts Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 15.

Praktische Handlungsvorgaben ohne regulatorische Anpassungen

1. Die **Gewährleistung von Authentizität, Vertraulichkeit, Qualität und Integrität der verwendeten Datensätze (und Prozesse) ist von Anfang an mitzudenken**, um straf- und haftungsrechtlichen Risiken einzudämmen. Gesetzliche Vorgaben und Standards, welche als Orientierung herangezogen werden könnten, fehlen - **maßgebend ist daher der aktuelle Stand der Wissenschaft und Forschung**. Es ist sicherzustellen, dass die Daten ausschließlich aus zulässigen Quellen stammen. (z.B. durch digitale Signaturen),[268] und nicht durch unautorisierte Dritte/ in unzulässiger Weise verändert wurden (z.B. umfassende Dokumentation der verschiedenen Versionen und Bearbeiter der Daten). Datenquellen und Datenverarbeitungen innerhalb der Lieferkette sind sämtlich transparent und nachvollziehbar zu dokumentieren, und laufend durch zu diesem Zweck errichtete Kontrollinstanzen zu überprüfen, um Auffälligkeiten von vornherein aufspüren und nachgehen und auf diese Weisen die finalen Datensätze gegen Manipulationen absichern zu können. Fehler im Endprodukt sind anderenfalls kaum mehr rückverfolgbar. Denkbar erscheint auch die Klassifizierung der Daten in verschiedene Gütestufen und IT-Sicherheitskategorien, etwa wenn die Lieferketten nicht umfassend nachvollzogen werden können (Import von Drittdaten). Auf diese Weise können die Nutzer informiert werden, inwieweit Dokumentation und Sicherungsmaßnahmen garantiert werden können, und können anschließend selbst entscheiden, ob die Datenqualität/-sicherheit für sie ausreichend ist.

[268] Schmidt/Pruß in Auer-Reinsdorff/Conrad IT-R-HdB, 3. Auflage 2019, § 2 Daten, Datenbanken und Datensicherheit Rn. 449.

2. In die Datenbank sollten **so wenig personenbezogene Daten wie möglich übertragen werden**, was vertraglich mit den verschiedenen Datenlieferanten sichergestellt werden sollte. Dies kann einerseits durch die bevorzugte Anforderung von nicht-personenbezogenen Daten von den Datenlieferanten erfolgen, soweit diese einen ausreichenden Informationsgehalt für den Verarbeitungszweck aufweisen. Radar- und Lidarinformationen sind beispielsweise bei einer generellen Betrachtung gegenüber visuellen Kameradaten wegen der fehlenden Identifikationsmöglichkeit von Dritten mangels der Aufzeichnung von Gesichter und Kennzeichen vorzugswürdig.[269] Während Kameradaten auch Verkehrsschilder und Fahrbahnmarkierungen und eine Aufzeichnung von anderen Verkehrsteilnehmern (Fußgängern, Radfahrern) und Fahrzeugen ermöglichen[270] und somit für Verkehrsszenarien wesentliche Informationen enthalten, geben Lidardaten bloße Punktewolken, wieder, die die Entfernung zu Gebäuden, Verkehrsteilnehmern usw. in der Fahrumgebung anzeigen[271]. Auf den konkreten Fall bezogen kann der Verarbeitungszwecks, die Szenarienerstellung, mit Lidarinformationen nicht erreicht werden. Auch Radardaten geben lediglich Entfernungswerte zu Umgebungsobjekten wieder[272] und verfügen damit über einen geringeren Informationsgehalt als Kameradaten mit Blick auf Informationen, welche für die Szenarienbildung bedeutsam sein können. Daneben können die Datenlieferanten zur Aufhebung des Personenbezugs mittels Aggregierung bzw. Synthetisierung der Rohdaten oder zur Anonymisierung im Wege der Löschung sämtlicher potenzieller Identifikatoren (z.B. Fahrzeugidentifikationsnummer, Fahrzeugkennzeichen und Gesichter aber auch sonstige seltene charakteristische Merkmale[273] wie beispielsweise Tattoos, auffällige Frisuren etc.) durch *Blurring* o.Ä. verpflichtet werden. Auch an dieser Stelle gilt es zu beachten, dass die Anonymisierung unter Umständen den Informationsgehalt mit Blick auf den Verarbeitungszeck mindert. So besteht beispielsweise die Gefahr, dass Fahrzeuge, die für Szenarien mit Verkehrsteilnehmern mit unkenntlich gemachten Gesichtern und Kennzeichen entwickelt werden, echte menschliche Gesichter und Kennzeichen in der Praxis nicht als solche wiedererkennen.

3. **Hilfsweise (falls dennoch personenbezogene Daten in Datenbank einfließen) sollten die Datenverarbeitungsprozesse DSGVO-konform ausgestaltet werden.** Praktisch relevante Rechtfertigungstatbestände mit Blick auf die in die Datenbank eingespeisten Forschungsdaten sind:

   a. **Freiwillige informierte und bestimmte Einwilligung**

   Die Einwilligung erfolgt je nach Geschäftsmodell durch den Fahrzeugerwerber im Kauf-, Miet-, oder Leasingvertrag etc. und den Fahrzeug(dienste)nutzern vor Fahrtantritt oder generell im Rahmen der Einstellungen verschiedener Nutzerprofile.[274] Sinnvoll wäre es, bei sämtlichen vertraglich vorgesehenen Verarbeitungen personenbezogener Daten, welche für die Datenbank relevant sind in dem jeweiligen Rechtsverhältnis neben der vertragsspezifischen Einwilligung auch eine Einwilligung zur nachträglichen Nutzung zu Forschungszwecken einzuholen.

[269] Bundesministerium für Wirtschaft und Energie "Praxishilfe zum Datenschutz in Reallaboren", 2021, S. 19.
[270] Kleinschmidt/ Wagner „Technik autonomer Fahrzeuge" in Oppermann/ Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020, Rn. 26.
[271] Kleinschmidt/ Wagner „Technik autonomer Fahrzeuge" in Oppermann/ Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020, Rn. 26.
[272] Kleinschmidt/ Wagner „Technik autonomer Fahrzeuge" in Oppermann/ Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020, Rn. 26.
[273] Bundesministerium für Wirtschaft und Energie "Praxishilfe zum Datenschutz in Reallaboren", 2021, S. 21.
[274] Vgl. dazu unter XX

Aufgrund der Widerrufbarkeit der Einwilligung sollte die Verarbeitung sicherheitshalber auch auf Grundlage einer weiteren Rechtfertigungsgrundlage erfolgen. Zu beachten ist in dem Zusammenhang, dass eine (widerrufene) Einwilligung unter Umständen den Rückgriff auf eine gesetzliche Rechtfertigungsgrundlage verbauen kann, wenn in der betroffenen Person das (schutzwürdige) Vertrauen geweckt wurde, dass die Datenverarbeitung nur im Rahmen der Einwilligung erfolgt.[275] Aus diesem Grund ist ein Hinweis sinnvoll, dass die Daten auch nach Wegfallen der Einwilligung auf anderer Grundlage verarbeitet werden können.[276]

b. Erforderlichkeit zur Vertragserfüllung

Mit Blick auf neuartige Geschäftsmodelle, gerichtet auf den Fahrzeugerwerb oder fahrzeugbezogene Leistungen kann die Verarbeitung personenbezogener Daten in bestimmten Fällen auch zur Vertragserfüllung erforderlich und somit gerechtfertigt sein, etwa wenn die Datenverarbeitung als solche erst die Fahrfunktion ermöglicht.[277] Handelt es sich um sensible Daten, so ist eine Rechtfertigung der Verarbeitung gemäß Art. 6 Abs. 1 lit. b DSGVO ausgeschlossen.[278]

c. Interessenabwägung (für private Datenverarbeitende)

Auf die Rechtfertigung auf Grundlage einer Interessenabwägung kann durch die Ergreifung verschiedener Maßnahmen zugunsten des Datenverarbeitenden eingewirkt werden, mit der Folge, dass die Datenverarbeitung gerechtfertigt ist. Denkbar sind beispielsweise die effiziente Durchsetzung der Datensparsamkeit, das Pseudonymisieren der Daten[279], das Einbeziehen zusätzlicher Kontrollmaßnahmen (unabhängige Überwachungsinstanzen),[280] die Einbindung von Datentreuhändern[281] sowie das Vorsehen einer besonders engen Zweckbindung und einer besonders kurzen Verarbeitungsdauer[282].

4. **Sämtliche Verarbeitungs-/ Informations-/ und Abwägungsprozesse sind zudem umfassend (mit Blick auf Haftungsrisiken über die allgemeine Rechenschaftspflicht hinaus)[283] zu dokumentieren** um Betroffenenrechten und Nachweispflichten (beispielsweise zwecks Exkulpation gemäß Art 82 DSGVO)[284] nachkommen zu können. Daneben empfiehlt sich, wenn nicht ohnehin die Verpflichtung greift, **die freiwillige Bestellung eines Datenschutzbeauftragten** gemäß Art. 37 Abs. 4 S. 1 DSGVO als zusätzliche Sicherheitsmaßnahme, der dabei hilft die Datenverarbeitenden über datenschutzrechtliche Verpflichtungen zu unterrichten sowie deren Einhaltung zu überwachen, vgl. Art. 39 Abs. 1 DSGVO.

[275] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
[276] Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
[277] Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel, Alexander/ Hornung, Gerrit „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62 ff.
[278] Art. 9 Nr. 1 DSGVO.
[279] Kotter, „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?“ 2019, S. 36.
[280] Bundesministerium für Wirtschaft und Energie “Praxishilfe zum Datenschutz in Reallaboren”, 2021, S. 26.
[281] Schantz in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 6 Abs. 1 DSGVO Rn. 114.
[282] Bundesministerium für Wirtschaft und Energie “Praxishilfe zum Datenschutz in Reallaboren”, 2021, S. 26.
[283] Quaas in: BeckOK DatenschutzR, 36. Ed. 1.5.2021, DS-GVO Art. 82 Rn. 19.
[284] Quaas in: BeckOK DatenschutzR, 36. Ed. 1.5.2021, DS-GVO Art. 82 Rn. 19.

5. Bei der Delegierung datenschutzrechtlicher Pflichten an Auftragsverarbeitende ist die Dokumentation der Einhaltung verbleibender Organisations- und Aufsichtspflichten sicherzustellen, um den Nachweis des fehlenden Verschuldens erbringen zu können.

6. Der Verantwortliche sollte durch ein entsprechendes Schutzkonzept die eigenverantwortliche Einhaltung der Löschpflicht gemäß Art 17 DSGVO (insbesondere bei widerrufener Einwilligung, Zweckfortfall und unrechtmäßiger Datenverarbeitung) sicherstellen.

7. Daneben sollte die **datenschutzrechtliche Privilegierung von Forschungsdaten** (mit Blick auf Zweckbindung und Speicherbegrenzung) genutzt werden. Daneben sollte die **datenschutzrechtliche Privilegierung von Forschungsdaten** (mit Blick auf Zweckbindung und Speicherbegrenzung) genutzt werden. **Das Konzept des Forschungsvorhabens (insbesondere Fragestellung, Verantwortlichkeiten, herangezogene Datenarten, ggf. Abwägungsgründe, Methodik, Gemeinschaftsnutzen und die Veröffentlichung der wesentlichen Ergebnisse)[285] und das Ergreifen geeigneter Garantien gemäß Art 89 Abs. 1 und Abs. 2 DSGVO sollte transparent dargestellt werden**. Wenn die Datenbank privat betrieben wird, ist darauf zu achten, dass die **rein kommerzieller Nutzung und der Bereich der Forschung und Entwicklung voneinander getrennt sind**, sodass sich das Aufziehen einer ausgelagerten Forschungsdatenbank empfiehlt. [286] **Bei privater Finanzierung und/oder der Verfolgung privater Eigeninteressen oder politischer Interessen ist ein Konzept zu entwickeln, welches eine direkte Einflussnahme auf den Erkenntnisprozess (z.B. durch Weisungen) ausschließt**. Daneben ist **darzulegen, dass private (z.B. wirtschaftliche) Interesse das Forschungsinteresse nicht dominieren**.

[285] Weichert, „„Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20, 23).
[286] Bundesministerium für Wirtschaft und Energie “Praxishilfe zum Datenschutz in Reallaboren”, 2021 S. 29.

8. Insgesamt ist es lohnenswert, im **kooperativen Austausch mit der verantwortlichen Datenschutzbehörde zu stehen** und so für Transparenz zu sorgen. In der DSGVO gibt es gemäß Art. 40 DSGVO beispielsweise die Möglichkeit für Vereinigungen und Verbände, eigenständig, im Wege der Selbstregulierung[287] datenschutzrechtliche Verhaltensregeln zu entwerfen und der Behörde zur Genehmigung vorzulegen. Vorlageberechtigt sind neben klassischen Vereinen und Verbänden sämtliche freiwilligen Zusammenschlüsse, soweit diese eine bestimmte homogene Gruppe vertreten, nicht jedoch einzelne Unternehmen.[288] **Genehmigte Verhaltensvorgaben generieren eine gewisse Rechtssicherheit dahingehend, dass die abstrakten Vorschriften der DSGVO eine branchenspezifische Präzisierung und Konkretisierung erfahren**.[289] Ab Bestandskraft der Genehmigung ist die Datenschutzbehörde an die genehmigten Regeln bei Auslegung der DSGVO gebunden,[290] mit Blick auf eine gerichtliche Überprüfung ist das genehmigte Regelwerk indes unverbindlich.[291] **Die Einhaltung genehmigter Verhaltensregeln und Zertifizierungsverfahren wirkt sich zudem, im Falle eines unvermeidbaren Verstoßes gegen Vorschriften der DSGVO, positiv auf die Bußgeldhöhe aus, vgl. Art. 82 Abs. 2 S 2 lit j DSGVO.** Daneben besteht die Möglichkeit der Zertifizierung von Datenverarbeitungsvorgängen, vgl. Art. 42 DSGVO. In der Praxis sind die vorgestellten Selbstregulierungsmechanismen bisher jedoch kaum bedeutsam.[292] **Darüber hinaus kann auch über die gesetzlich vorgesehenen Kooperationen mit der Aufsichtsbehörde ein informeller Austausch angestrebt werden.[293]**

9. Der **Betrieb der Datenbank durch eine Forschungskooperation ist ungeeignet**. Eine solche Kooperation generiert aufgrund fehlender rechtlicher Vorschriften Rechtsunsicherheit und ist mit großem vertraglichen Aufwand verbunden, sodass von Anfang an eine passende Rechtsform gefunden werden sollte. **In Betracht kommt aus Haftungsgründen entweder die Ausgestaltung als GmbH oder als eingetragener Verein, wobei der GmbH wohl langfristig der Vorzug einzuräumen ist.** Die **Anerkennung als gemeinnützige GmbH hat zahlreiche Vorteile**, ist aber nur dann denkbar, wenn das Gewinnausschüttungsverbot durch ein passendes Finanzierungsmodell und einer nicht-kommerziell-orientierten Akteursstruktur im Kernbetrieb aufgefangen wird. Vor der Gründung eines Vereins oder einer GmbH, welche die Privilegien des § 51 AO aufgrund ihrer Gemeinnützigkeit erhalten soll, ist es ratsam, bereits vorab mit den zuständigen Finanzbehörden Kontakt aufzunehmen, um so sicherzustellen, dass die Anforderungen des Gemeinnützigkeitsrechts erfüllt sind.

10. In der Regel ist davon auszugehen, dass die **Forschungskooperation vom Kartellverbot durch eine EU-Gruppenfreistellungsverordnung freigestellt** wird. Allerdings gilt es zu beachten, dass die an der **Kooperation beteiligten Unternehmen das Risiko der Freistellung**, insbesondere die Beweislast mit Blick auf die Freistellungsvoraussetzungen, tragen. Daher empfiehlt sich eine **regelmäßige Überprüfung der Freistellungsvoraussetzungen**.

[287] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 40 DSGVO Rn. 32.
[288] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 40 DSGVO Rn. 33.
[289] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 40 DSGVO Rn. 1.
[290] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 40 DSGVO Rn. 69.
[291] Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 40 DSGVO Rn. 68.
[292] Rücker/ Dienst/ Brandt für das BMWI „Umsetzung der BMWi-Stategie „Reallabore als Testräume für Innovation und Regulierung“: Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen, 2021, S. 49 f.
[293] Rücker/ Dienst/ Brandt für das BMWI „Umsetzung der BMWi-Stategie „Reallabore als Testräume für Innovation und Regulierung“: Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen, 2021, S. 51.

Regulierungspotenzial mit Blick auf den nationalen Rechtsrahmen

Neben der Anpassung des gesamten europäischen Datenschutzrechts (insbesondere der DSGVO), was realistisch allenfalls eine mittel- bis langfristige Option darstellt,[294] besteht die kurz- bis mittelfristig realisierbare[295] Möglichkeit innerhalb der den Mitgliedstaaten verbleibenden Regelungsspielräume punktuell nationale Vorgaben zu treffen.[296]

Nationale Formulierung von rechtlichen Verpflichtungen

Mit Blick auf die Verarbeitung von Daten, die erforderlich ist, um rechtliche Verpflichten oder eine Aufgabe, die im öffentlichen Interesse liegt, zu erfüllen, kann der nationale Gesetzgeber durch die Formulierung entsprechender Verpflichtungen bzw. Rechtsgrundlagen gemäß Art. 6 Abs 1, S. 1 lit. c und e DSGVO iVm Art. 6 Abs. 3, S.1 lit. b DSGVO im öffentlichen Interesse auf die Rechtfertigungsebene einwirken und auf diese Weise Rechtssicherheit schaffen.[297] Die Anforderungen an die Rechtsgrundlage werden abstrakt in Art. 6 Abs. 3, S. 2 f. DSGVO definiert. [298] Die Rechtsgrundlage kann neben bundes- oder landesrechtlicher auch satzungsrechtlicher Natur (kommunale Satzungen oder Satzungen anderer juristischer Personen), mangels Außenwirkung nicht aber Verwaltungsvorschrift sein.[299]
Neben der Schaffung neuer Rechtsgrundlagen für die Datenverarbeitung können die Mitgliedstaaten auch gemäß Art. 6 Abs. 2 DSGVO in den Fällen der Datenverarbeitungen gemäß Art. 6 Abs 1, S. 1 lit. c und e DSGVO Anforderungen für die Verarbeitung sowie sonstige Maßnahmen bestimmen und für Verarbeitungen zu Forschungszwecken gemäß Art. 89 Abs. 2 DSGVO in begrenztem Umfang Ausnahmen regeln.[300]
Der in Deutschland bestehenden Überregulierung von Forschungsdaten sollte durch gesetzliche Anpassungen begegnet werden, Wertungswidersprüche sind zu beseitigen, bereichsspezifische Datenschutznormen sind zu harmonisieren.[301]

[294] Rücker/ Dienst/ Brandt für das BMWI „Umsetzung der BMWi-Strategie „Reallabore als Testräume für Innovation und Regulierung“: Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen, 2021, S. 56.
[295] Ebenda, S. 60.
[296] Ebenda, S. 53.
[297] Ebenda, S. 57.
[298] Frenzel in Paal/Pauly DSGVO und BDSG, 3. Aufl. 2021 Art. 6 DSGVO, Rn. 37.
[299] Ebenda, Rn. 36.
[300] Pauly in Paal/Pauly, DSGVO und BDSG, 3. Aufl. 2021, Art. 89 DSGVO Rn. 13.
[301] Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (23).

Literaturverzeichnis

ARTIKEL-29-DATENSCHUTZGRUPPE „Stellungnahme 5/2014 zu Anonymisierungstechniken".

Auer-Reinsdorff/Conrad IT-R-HdB, 3. Auflage 2019.

BeckOK Datenschutzrecht, 36. Ed. 1.5.2021.

Beck'sches Handbuch der GmbH, 6. Auflage 2021.

Berning, Wilhelm „Erfüllung der Nachweispflichten und Beweislast im Unternehmen", ZD 2018, 348.

Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. April 2019.
Bischoff, Claudia „Pseudonymisierung und Anonymisierung von personenbezogenen Forschungsdaten im Rahmen klinischer Prüfungen von Arzneimitteln (Teil I) – Gesetzliche Anforderungen", erschienen in PharmR 2020, 309.

Brockmeyer, Henning „Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge", ZD 2018, 258 (259).

Buchholz, Wolf "Die neue PSI-Richtlinie – Wie viel Datenhoheit verbleibt den öffentlichen Unternehmen?", IR 2019, 197.

Bundesministerium der Justiz und für Verbraucherschutz, "Leitfaden zum Vereinsrecht", 2016.

Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen" Version 1.1, 2020.

Bundesministerium für Wirtschaft und Energie "Praxishilfe zum Datenschutz in Reallaboren", 2021.

Eberbach, Wolfgang „Eine Rechtsform für Wissenschaftskooperationen –Ausgangspunkte und Grundlagen" (2) 2018, 51.

Eichberger, Michael "Rechte an Daten -Verfassungsrechtliches Eigentum an Daten", VersR 2019, 709.

Geis, Max-Emanuel · „Forschungskooperationen: Öffentliches oder Zivilrecht? – Positionsbestimmungen und Regelungszuständigkeiten", 2/ 2018, 77.

Gola, Peter / Heckmann, Dirk, Bundesdatenschutzgesetz Kommentar, 13. Auflage, 2019.

Gummert, Hans/ Weipert, Lutz, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019.

Hartl, Andreas/ Ludin, Anna, Recht der Datenzugänge, MMR 2021, 534.

Hau,Wolfgang/ Poseck,Roman, Beck'scher Onlinekommentar BGB, 58. Edition 2021.

Hornung, Gerrit/Schallbruch, Martin, IT-Sicherheitsrecht, 1. Auflage 2021.

Jauernig, Bürgerliches Gesetzbuch Kommentar, 18. Auflage, 2021.

Jüngling, Alexander "Die Digitalstrategie der EU-Kommission: Regulierung von Künstlicher Intelligenz", MMR 2020, 440

Koenig, Ulrich, Abgabenordnung Kommentar, 4. Auflage 2021.

Kotter, Philip, Datenschutz beim vernetzten und autonomen Fahren. Welche Rahmenbedingungen können sensible Daten schützen?, 2019.

Kühling, Jürgen/Sackmann, Florian, "Irrweg „Dateneigentum"", ZD 2020, 24.

Lüdemann, Volker, "Connected Cars - Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück", ZD 2015, 247.

Metzger, Axel, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129.

Oppermann, Bernd H./Stender-Vorwachs, Jutta „Autonomes Fahren- Technische Grundlagen, Rechtsprobleme, Rechtsfolgen" 2. Auflage 2020.

Paal, Boris „Schadensersatzansprüche bei Datenschutzverstößen - Voraussetzungen und Probleme des Art. 82 DSGVO", MMR 2020, 14.

Paal, Boris/ Pauly, Daniel "DSGVO und BDSG", 3. Auflage 2021.

Palandt, Bürgerliches Gesetzbuch Kommentar, 77. Auflage 2018.

Peffer, Raphael „Szenariobasierte simulationsgestützte funktionale Absicherung hochautomatisierter Fahrfunktionen durch Nutzung von Realdaten", 2020.

Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz", 2. Auflage 2020

Richter, Heiko "Zugang des Staates zu Daten der Privatwirtschaft", ZRP 2020, 245.

Riehm, Thomas / Meier, Stanislaus; "Rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit - Behörden, Private und Verbände in der Gesamtverantwortung", erschienen in MMR 2020, 571.

Robrahn, Rasmus/Brehmert, Benjamin „Interessenskonflikte im Datenschutzrecht - Rechtfertigung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO" ZD 2018, 291.

Roßnagel, Alexander "Datenlöschung und Anonymisierung-Verhältnis der beiden Datenschutzinstrumente nach DS-GVO", ZD 2021, 188.

Roßnagel, Alexander "Datenschutz in der Forschung - Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen", ZD 2019, 157.

Roßnagel, Alexander/ Hornung, Gerrit Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019.

Rücker, Daniel/ Dienst, Sebastian/ Brandt, Alexander für das Bundesministerium für Wirtschaft und Energie „Umsetzung der BMWi-Strategie „Reallabore als Testräume für Innovation und Regulierung": Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen (Projekt Nr. 113/19-FL1-2/03), 2021.

Schlimme, Hauke Christian „Zulassungsrechtliche Probleme automatisierter Kraftfahrzeuge – Eine Betrachtung der jüngsten Entwicklungen", 2016.

Schuster, Gerald/Spindler, Fabian, Recht der elektronischen Medien, 4. Auflage 2019.

Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Auflage 2019.

Specht-Riemenschneider, Louisa, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, im Auftrag des Bundesministeriums für Bildung und Forschung, abrufbar unter: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf, August 2021.

Specht-Riemenschneider, Louisa/ Blankertz, Alina/ Sierek, Pascal/Schneider, Ruben/ Knapp, Jakob/ Henne, Theresa „Die Datentreuhand", MMR-Beil. 2021, 25.

Steege, Hans „Ist die DS-GVO zeitgemäß für das autonome Fahren?", MMR 2019, 509.

Stelkens, Paul/Bonk, Heinz Joachim/ Sachs, Michael, Verwaltungsverfahrensgesetz Kommentar, 9. Auflage 2018.

Weichert, Thilo, Die Forschungsprivilegierung in der DS-GVO, ZD 2020, 18.

Wiesche, Manuel/Sauer, Petra/ Krimmling, Jürgen /Krcmar, Helmut, Management Digitaler Plattformen, 2018.

Wybitul, Tim; Haß, Detlef; Albrecht, Jan Philipp „Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung", erschienen in NJW 2018, 113.

Ziekow, Jan, Öffentliches Wirtschaftsrecht, 4. Auflage 2016.

Ansprechpartner beim IKEM:
Mathilde Krampitz
Anne Freiberger

IKEM – Institut für Klimaschutz, Energie und Mobilität e.V.
Berlin • Greifswald • Stuttgart

www.ikem.de

Magazinstraße 15 – 16
10179 **Berlin**
T +49 (0)30 408 1870 10
F +49 (0)30 408 1870 29

info@ikem.de

Domstraße 20a
17489 **Greifswald**
T +49 (0)38 34 420 2100
F +49 (0)38 34 420 2002

lsrodi@uni-greifswald.de

IKEM

Juni 2021

A3: Rollenmodell und Betriebsarchitektur einer AD/ADAS Szenariendatenbank

Auswertung einer Expert*innenbefragung per Fragebogen

ERSTELLT VON
Alexander Klinge

IM AUFTRAG DER
Bundesanstalt für Straßenwesen (FE 82.0719/2018)

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis 3

Ziele und Leitfragen 4

Die zentralen Folgerungen 5

Hintergrund 7

Entwicklung des Rollenmodells 7

Anreiz- und Hindernisevaluation 7

Zielgruppen 9

Ergebnisse 10

Abschnitt I: Rollenzuschreibungen 11

Rollenzuschreibung der eigenen Institution 11
Fehlende Rollen 14
Rollenzuschreibungen anderer Institutionen 15

Abschnitt II: Anreiz- und Hemmnisevaluation 16

Anreizevaluation 16
Hemmnisevaluation 21
Weitere Anreize und Hemmnisse der Partizipation 26

Fazit 27

Rollenverteilung 27

Anreize und Hemmnisse der Partizipation 28

Anreize und Hemmnisse der Partizipation im Kernbetrieb 28
Anreize und Hemmnisse der Datenlieferung und Nutzung 29

Mögliche Incentivierung der Akteure 30

Abbildungs- und Tabellenverzeichnis

Abbildung 1: Anzahl der Befragten und ihre Verteilung auf die Stakeholdergruppen bzw. Cluster 9
Abbildung 2: Schematische Darstellung der Boxplot-Diagramminhalte 10
Abbildung 3: Schematische Darstellung des Rollenmodells 11
Abbildung 4: Gesamtübersicht Antworten I 12
Abbildung 5: Antworten I nach Stakeholdercluster 13
Abbildung 6: Rollenverteilung nach Stakeholdercluster 14
Abbildung 7: Darstellung der Fragestellung III 15
Abbildung 8: Antworten IV Gesamtübersicht 16
Abbildung 9: Antworten V Gesamtübersicht 17
Abbildung 10: Antworten VI Gesamtübersicht 18
Abbildung 11: Antworten VII Gesamtübersicht 19
Abbildung 12: Antworten VIII Gesamtübersicht 20
Abbildung 13: Antworten IX Gesamtübersicht 21
Abbildung 14: Antworten X Gesamtübersicht 22
Abbildung 15: Antworten XI Gesamtübersicht 23
Abbildung 16: Antworten XII Gesamtübersicht 24
Abbildung 17: Antworten XIII Gesamtübersicht 25
Abbildung 18: Zusammenfassung der hypothetischen Rollenverteilung im Datenbankbetrieb 27

Tabelle 1: Rollenbeschreibungen und Anforderungen 7
Tabelle 2: Anreize und Hürden der Partizipation 8
Tabelle 3: Antworten III Gesamtübersicht 15
Tabelle 4: Differenzierung der Antworten IV nach Stakeholdercluster 17
Tabelle 5: Differenzierung der Antworten V nach Stakeholdercluster 17
Tabelle 6: Differenzierung der Antworten VI nach Stakeholdercluster 18
Tabelle 7: Differenzierung der Antworten VII nach Stakeholdercluster 19
Tabelle 8: Differenzierung der Antworten VIII nach Stakeholdercluster 20
Tabelle 9: Differenzierung der Antworten IX nach Stakeholdercluster 21
Tabelle 10: Differenzierung der Antworten X nach Stakeholdercluster 22
Tabelle 11: Differenzierung der Antworten XI nach Stakeholdercluster 23
Tabelle 12: Differenzierung der Antworten XII nach Stakeholdercluster 24
Tabelle 13: Differenzierung der Antworten XIII nach Stakeholdercluster 25
Tabelle 14: Weitere zu berücksichtigende Hemmnisse 26
Tabelle 15: Weitere zu berücksichtigende Anreize 26

Ziele und Leitfragen

Die Ziele der Expertenbefragung lauten wie folgt:

- Externe Validierung des vorab entwickelten und intern konsolidierten Rollenmodells
- Identifikation fehlender Rollen im Modell
- Einordnung der verschiedenen Stakeholdergruppen in das Rollenmodell
- Stakeholderspezifische Priorisierung verschiedener Anreize bzw. Hürden der Partizipation
- Identifikation fehlender Anreize bzw. Hürden der Partizipation
- Entwicklung einer stakeholderspezifischen Anreizevaluation

Um diese Ziele zu erreichen, lassen sich folgende Leitfragen für den Fragebogen formulieren:

- In welche Rolle im Szenariendatenbankbetrieb ordnen sich die Befragten selbst ein?
- Welche Rolle im Szenariendatenbankbetrieb schreiben Befragte anderen Stakeholdern zu?
- Welche Priorisierung schreiben die Befragten verschiedenen Anreizen bzw. Hürden zur Besetzung der jeweiligen Rollen zu?

Die zentralen Folgerungen

Rollenverteilung:

- Die große Mehrheit der Stakeholder sieht sich selbst mit hoher Wahrscheinlichkeit in der Nutzerrolle der Szenariendatenbank.
- Die Partizipation an der Datenbank durch eigene Datenlieferung ist abhängig davon, ob es sich um öffentliche, öffentlich-private oder private Akteure handelt.
    - Private Akteure schätzen dies eher wahrscheinlich ein.
    - Öffentlich-private Akteure schätzen dies eher wahrscheinlich ein.
    - Öffentliche Akteure schätzen dies eher unwahrscheinlich ein.
- Die Mehrheit der Befragten sieht Akteure aller Stakeholdercluster (Privat / Öffentlich-Privat / Öffentlich) in den Rollen Nutzer und Datenlieferant.
- Die nach Umfrageergebnissen wahrscheinlichste Rollenverteilung im Kernbetrieb nach Priorisierung ist:
    - Veredler → Privat → KI-Unternehmen / Tech. StartUp
    - Betreiber → Privat → Toolhersteller / IT-Infrastruktur
    - Auditor → Öffentlich / Privat→ 1. Bund / Bundesbehörde
      2. Technische Dienste

Anreize der Rollenbesetzung

- Datenlieferung: Der am höchsten priorisierte Anreiz aller Cluster stellt eine gesetzliche Notwendigkeit der Datenlieferung dar.
- Veredlung: Der am höchsten priorisierte Anreiz der Cluster Privat bzw. Öffentlich-Privat sehen die Befragten in einem strategischen Marktvorteil. Öffentliche Akteure priorisieren eine Mitwirkung an der Standardisierung.
- Betrieb: Der am höchsten priorisierte Anreiz der Cluster Privat bzw. Öffentlich-Privat sehen die Befragten in einem strategischen Marktvorteil. Öffentliche Akteure priorisieren den Anreiz der politischen Zielstellungen.
- Auditierung: Der am höchsten priorisierte Anreiz aller Cluster impliziert die Mitwirkung an der Standardisierung.
- Datenbanknutzung: Der am höchsten priorisierte Anreiz der Cluster Privat bzw. Öffentlich-Privat stellt eine komfortable Nutzung der Daten (vereinfacht, vereinheitlichtes Datenformat, geclustert) dar. Öffentliche Akteure priorisieren den Anreiz des Kompetenzzugewinns.

Hemmnisse der Rollenbesetzung

- Datenlieferung: Der am höchsten priorisierte Hemmer der Cluster Privat bzw. Öffentlich ist die Problematik der Legal Compliance insbesondere mit Blick auf die Einhaltung datenschutzrechtlicher Vorgaben. Öffentlich-Private bzw. Private Akteure priorisieren die Privilegierung von Konkurrenten.
- Veredlung: Der von allen Clustern am höchsten priorisierte Hemmer ist die Problematik der Legal Compliance insbesondere mit Blick auf die Einhaltung datenschutzrechtlicher Vorgaben.
- Betrieb: Der von allen Clustern am höchsten priorisierte Hemmer ist die Verantwortung für die Richtigkeit der Daten sowie die Datensicherheit.
- Auditierung: Der am höchsten priorisierte Hemmer der Cluster Privat bzw. Öffentlich-Privat ist ein möglicher defizitärer Betrieb. Öffentliche Akteure priorisieren die Unvorhersehbarkeit der zu verarbeitenden Datenmenge.
- Datenbanknutzung: Der am höchsten priorisierte Hemmer der Cluster Privat ist die Unsicherheit mit Blick auf die Korrektheit der Szenarien. Öffentlich-Private Akteure sehen die Kosten der Nutzung als größtes Hemmnis, öffentliche Akteure die rechtlichen Vorgaben.

Hintergrund

Entwicklung des Rollenmodells

Im Rahmen des Projekts wurden notwendige Rollen (Datenlieferant, Veredler, Betreiber, Auditor und Nutzer) für einen erfolgreichen Datenbankbetrieb identifiziert (Tabelle 1). Zusätzlich wurden Anforderungen an die jeweiligen Rollen in einem hypothetischen Betrieb vordefiniert.

Tabelle 1: Rollenbeschreibungen und Anforderungen

Rolle	Beschreibung	Anforderung an die Rolle
Daten-lieferant	• Zulieferung der beim jeweiligen Stakeholder vorhandenen Daten zur Erstellung der Szenarien • Unterschiede in den zur Verfügung stehenden Datenarten sowie der Möglichkeit der Weitergabe und der Incentivierung.	• Möglichkeit zur Vorab-Aufbereitung der Daten • Anreiz zur Datenweitergabe
Veredler	• Labeling der zur Verfügung stehenden Datensätze, um eine Einspeisung der Datensätze in die Datenbank zu ermöglichen • Eventuell Automatisierung möglich	• Verarbeitung unterschiedlicher Datenquellen • Kompetenz zur Erstellung maschinenlesbarer Labels • Umgang mit Labeling-Tools
Betreiber	• Finale Auswahl und Festlegung der Szenarien • Betrieb der Datenbank: Maintenance, Hosting, etc. • Compliance in rechtlichen und ethischen Fragestellungen • Kooperation mit weiteren Partnern möglich	• Kompetenz im Umgang mit annotierten Daten • Erstellung von Testumgebungen • Planung von Testfällen, Analyse von Testdaten • Ableitung und Identifizierung von Szenarien
Auditor	• Auditieren der Prüfszenarien in der Datenbank ○ Sind die Prüfszenarien auf dem neuesten Stand der Technik?	• Unabhängigkeit • Lizensierung
Nutzer	Nutzung der Datenbank für: • Zulassung autonomer Fahrfunktionen • Ausweitung der technischen Kompetenz • Identifizierung von Infrastrukturbedarf • Toolverbesserung / -development • R&D	

Anreiz- und Hindernisevaluation

Eine Besetzung der jeweiligen Rollen ist unter anderem vom Anreiz zur Partizipation abhängig. Während öffentliche Akteure geringere Hürden für eine Datenlieferung haben, muss für Akteure aus der Privatwirtschaft entweder ein monetärer oder strategischer Vorteil entstehen, um diese zur Teilnahme an der Datenbank zu motivieren. Dies bezieht sich in erster Linie auf die Datenlieferung, welche zunächst einen strategischen Nachteil für privatwirtschaftliche Akteure darstellt, welcher nur ausgeglichen werden kann, wenn die Nutzung einer kollaborativen Datenbank dem Verlust des Wettbewerbsvorteils überwiegt oder die Datenlieferung monetär entschädigt wird.

Zur Vorbereitung der Anreiz- bzw. Hemmnisevaluation wurden im Rahmen eines internen Workshops die Anreize und Hürden für die jeweiligen Akteursgruppen in Bezug auf die Partizipation an der Szenariendatenbank in unterschiedlichen Rollen sowie unter den verschiedenen Gesichtspunkten technischer, rechtlicher und ökonomischer Hürden und Anreize betrachtet. Sämtliche erörterten Anreize und Hürden auf Rollenebene sind in Tabelle 2 dargestellt.

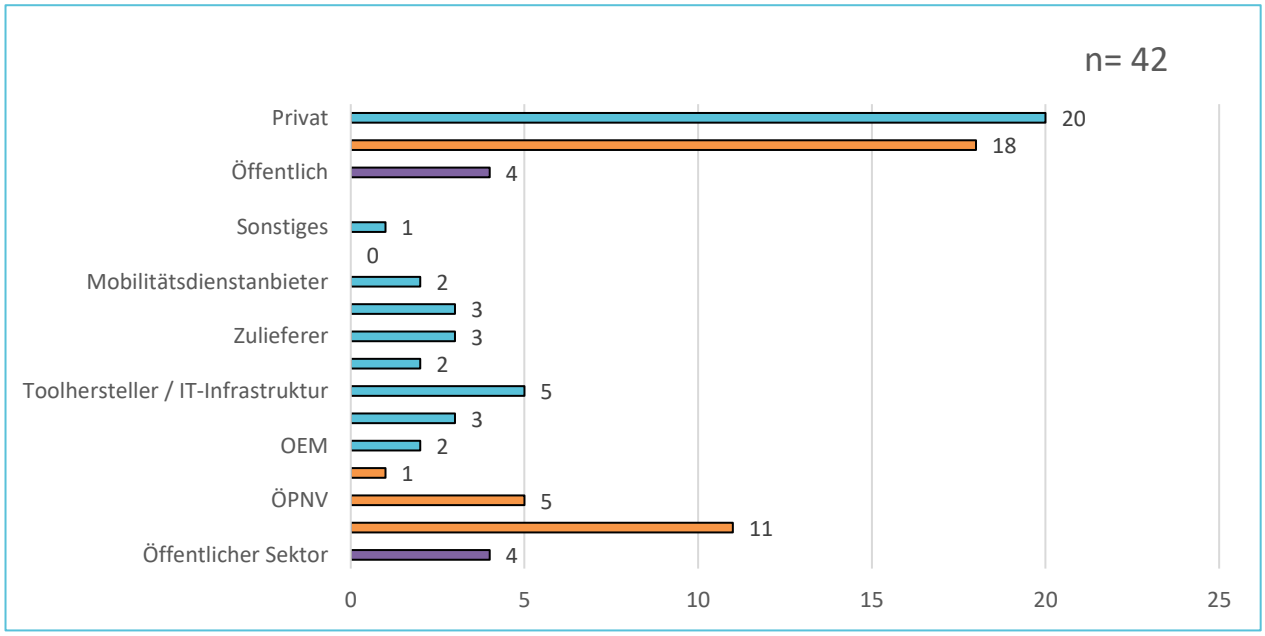
Tabelle 2: Anreize und Hürden der Partizipation

Anreize	Hürden
Datenlieferant	
Monetärer Ausgleich für Datenlieferung	Vorteile für Konkurrenten
Wertschöpfung durch Partizipation	
Ethische Notwendigkeit	Datenqualitätsanforderungen
Gesetzliche Notwendigkeit	
Relevanz für Typengenehmigung	Legal Compliance -Datenschutz
Möglichkeit der Entscheidung, ob Szenarien öffentlich zugänglich sind	
Absicherung durch Validierung	Reverse Engineering
Datenaltruismus – EU / National	
Veredler	
Strategischer Marktvorteil	Risiko des Absatzes der veredelten Datensätze
Wertschöpfung durch Partizipation	Unvorhersehbarkeit der Datenmenge
Mitwirkung an Standardisierung	Legal Compliance -Datenschutz
Betreiber	
Gewinnmaximierung	Möglicher defizitärer Betrieb
Kostendeckung	Verlust des Standortvorteils
Strategischer Marktvorteil	Unvorhersehbarkeit der Datenbankgröße (des Risikos)
Datenaltruismus – EU / National	Bürokratischer Aufwand
Politische Zielstellungen	Verantwortung für Richtigkeit und Datensicherheit
Absicherung gegen Datenverantwortlichkeit	Reverse Engineering
Auditor	
Strategischer Marktvorteil	Unvorhersehbarkeit der Datenmenge
Wertschöpfung durch Partizipation	Möglicher defizitärer Betrieb
Mitwirkung an Standardisierung	
Nutzer	
Vorteile für Homologation	Unsicherheit bezüglich der Korrektheit der Szenarien
Generierung gesellschaftlicher / wissenschaftlicher Akzeptanz	
Outsourcing eigener Datenbank	Technische Hürden (unpassendes Datenformat, fehlende Interoperabilität)
Kompetenzzugewinn	
Abgleich eigener Datenbanken (Validierung)	Rechtliche Vorgaben
Quantität der Datenszenarien – kritische Szenarien	
Komfortable Nutzung der Daten (vereinfacht, vereinheitlichtes Datenformat geclustert)	Kosten der Nutzung

Zielgruppen

Die Zielgruppen der Expert*innenbefragung umfassen alle Stakeholder mit einem direkten oder indirekten Nutzen an der Entwicklung einer umfassenden Datenbank mit Simulationsszenarien zur prospektiven und retrospektiven Betrachtung der Sicherheitswirkungen von AD / ADAS (Autonomous Driving / Autonomous Driving Assistance Systems). Die in der Befragung fokussierten Zielgruppen und die Verteilung der Partizipation je Interessensgruppe sind in Abbildung 1 dargestellt.

Abbildung 1: Anzahl der Befragten und ihre Verteilung auf die Stakeholdergruppen bzw. Cluster



Es ist zu erkennen, dass mehrheitlich privatwirtschaftliche sowie öffentlich/private Akteure unter den Befragten vertreten sind. Die Umfrage konnte lediglich vier Akteure aus dem öffentlichen Sektor erreichen, was eine Interpretation der Ergebnisse für dieses Stakeholdercluster erschwert und der Bildung genereller Thesen entgegensteht.

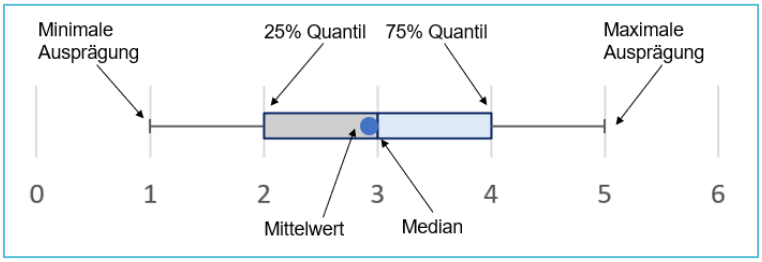
Ergebnisse

Im Folgenden werden die Ergebnisse der Befragung grafisch aufbereitet. Zur Darstellung der Ergebnisse von Fragen auf Basis einer Likert-Skala wurden Boxplot-Diagramme gewählt, um die Verteilungen der Antworten detailliert darzustellen. In allen Fragen wurde eine Skala von 1 bis 5 gewählt, wobei 1 für unwahrscheinlich in Bezug auf die Rollenbesetzung und eine geringe Priorität in Bezug auf Anreize bzw. Hürden verwendet wird, während 5 für sehr wahrscheinlich bzw. hohe Priorität steht.

Der Aufbau der Boxplot-Diagramme ist in Abbildung 2 zusammengefasst. Der untere Fehlerindikator beschreibt die minimale Ausprägung der Datenreihe, der obere Fehlerindikator folglich die maximale Ausprägung. Der graue Kasten stellt das Spektrum zwischen dem 25%-Quantil und Median, der blaue Kasten das Spektrum Median bis 75% Quantil, dar. Der Median ist als Strich zwischen den beiden Kästen und der Mittelwert als blauer Punkt eingetragen. Alle Boxplot Diagramme sind absteigend nach dem Mittelwert sortiert.

Diese Darstellungsform wurde gewählt, um die Verteilungen innerhalb der Datenreihen zu veranschaulichen. Durch die Verwendung des Boxplot-Diagramms ist die Streuung der Antworten schneller zu erfassen. Ist das Boxplot linksschief, liegt dieses also im linken bzw. unteren Bereich der Wertungsskalen, liegen die meisten Werte im unteren Skalenbereich. Umgekehrte/ Spiegelbildliche Schlussfolgerungen sind für rechtsschiefe Ausprägungen des Boxplots gültig.

Abbildung 2: Schematische Darstellung der Boxplot-Diagramminhalte



Abschnitt I: Rollenzuschreibungen

Im folgenden Abschnitt soll die Wahrscheinlichkeit der jeweiligen Rollenbesetzungen (vgl. Tabelle 1) bewertet werden. Hierfür wurden die Wahrscheinlichkeiten der Besetzung der jeweiligen Rollen von den durch die Teilnehmer*innen vertretenen Institutionen bewertet, um als Ergebnis das Rollenmodell zu validieren oder entsprechend anzupassen.

Kurzdefinition institutioneller Rollenmodelle:

"Institutionelle Rollenmodelle sind gegenüber Betreibermodellen weitergehender, weil Betreibermodelle eine hierarchische Zusammenarbeit beschreiben, mit nach der Definition gesellschaftsrechtlich festgeschriebenen Rollen und einer begrenzten Erweiterungsfähigkeit. Mit dem Begriff Betreibermodell wird die konzeptionelle Ebene charakterisiert. Die konkrete Durchführung wird mit dem Begriff Betreibergesellschaft adressiert. Die Durchführung eines institutionellen Rollenmodells wird zutreffend mit institutioneller rollenbasierter Kooperation beschrieben."

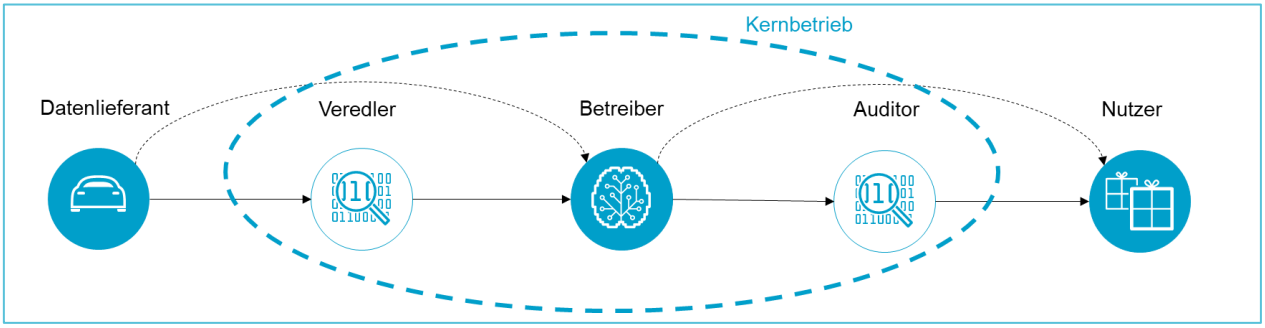
(Schulz, Joisten, und Mainka 2013, 15)

Rollenzuschreibung der eigenen Institution

Frage I:

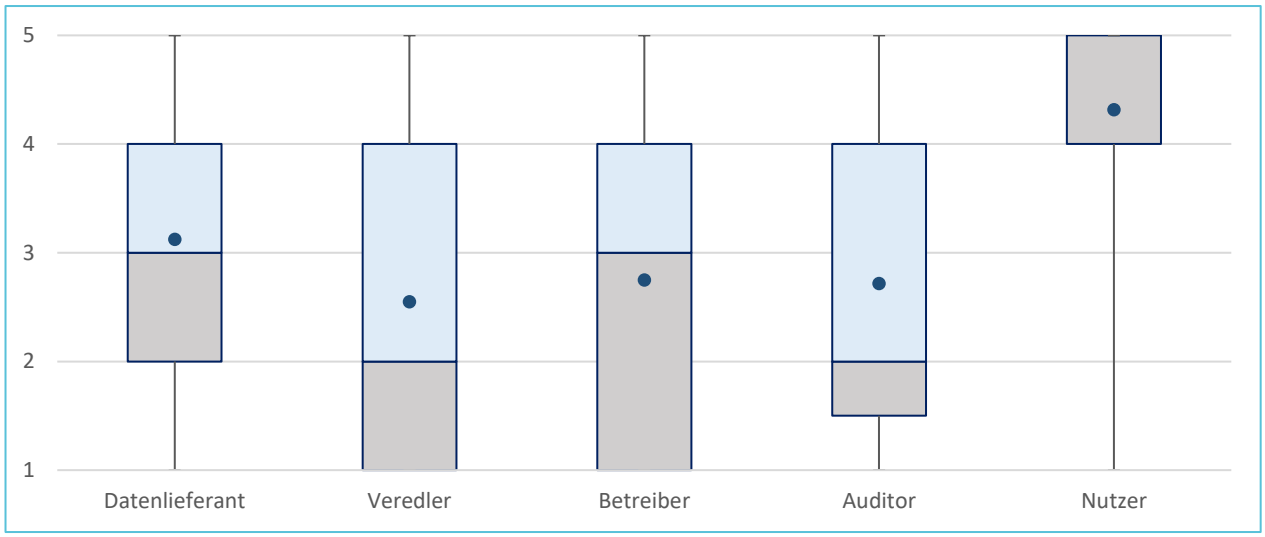
In welcher Rolle (vgl. Abbildung 3) sehen Sie die von Ihnen repräsentierte Institution in einem hypothetischen Szenarienbankbetrieb. Für wie wahrscheinlich (1 = unwahrscheinlich | 5 = sehr wahrscheinlich) halten Sie die Besetzung der folgenden Rollen durch die von Ihnen repräsentierte Institution?

Abbildung 3: Schematische Darstellung des Rollenmodells



Antworten I: Gesamtübersicht

Abbildung 4: Gesamtübersicht Antworten I



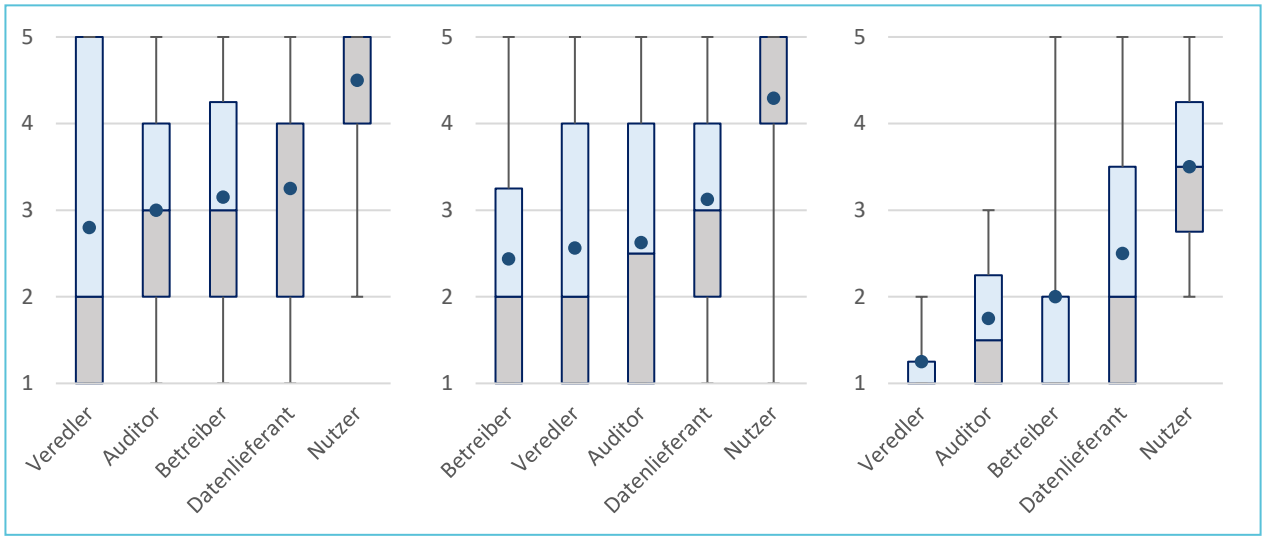
Interpretation:

Die am wahrscheinlichsten zu besetzende Rolle ist die Nutzerrolle, gefolgt von der Rolle des Datenlieferanten. Die Besetzung der Rolle des Auditors, Betreibers und Veredlers scheint ähnlich wahrscheinlich, während der Median der Betreiberrolle höherliegt und der untere Interquantilsabstand in der Datenreihe Auditor kleiner ist. Daraus lässt sich schlussfolgern, dass die Befragten, neben der Besetzung der Rollen Datenlieferant und Nutzer, die eigene Institution mehrheitlich in der Rolle des Betreibers sehen. Mit absteigender Wahrscheinlichkeit werden darauffolgend die Rollen Auditor und Veredler besetzt.

Eine differenzierte Betrachtung der Ergebnisse nach der Stakeholdergruppenzugehörigkeit ist dem nachfolgenden Kapitel zu entnehmen.

Antworten I: Aufgeteilt nach Stakeholdercluster (Privat / Öffentlich-Privat / Öffentlich):

Abbildung 5: Antworten I nach Stakeholdercluster



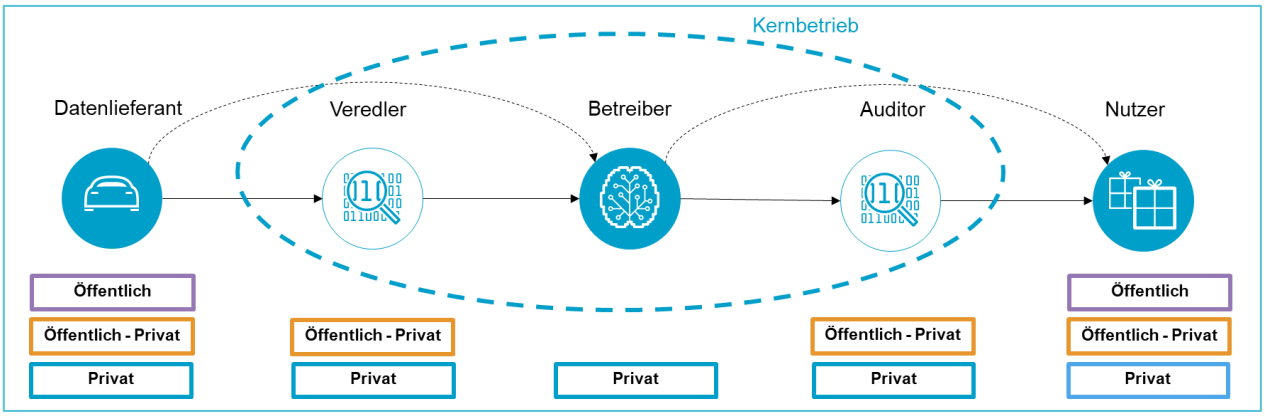
von links: Private Akteure (n=20); Öffentlich - Private Akteure (n=17); Öffentliche Akteure (n=4)

Interpretation:

Es ist anhand der Streuung der Antworten erkennbar, dass auch innerhalb der einzelnen Stakeholdercluster verschiedene Stakeholdergruppen die Wahrscheinlichkeit der Rollenbesetzungen unterschiedlich einschätzen. Es lässt sich feststellen, dass private Akteure generell die Rollenbesetzungen als wahrscheinlicher einschätzen als öffentliche Akteure.

Wie im vorherigen Kapitel festgestellt, sehen sich alle Befragten nahezu unabhängig von der Stakeholdergruppenzugehörigkeit am wahrscheinlichsten in der Nutzer- bzw. Datenlieferantenrolle. Öffentliche und private Akteure sehen sich am drittwahrscheinlichsten in der Betreiberrolle, während sich öffentlich-private Akteure in der Auditorrolle sehen. Jedoch bewerten öffentliche Akteure die Besetzung der Rollen Veredler, Auditor und Betreiber bereits als eher unwahrscheinlich, wobei eine Antwort auch die Besetzung der Betreiberrolle als sehr wahrscheinlich einschätzt. Aufgrund der vorliegenden Ergebnisse scheint eine Besetzung der Rollen im Kernbetrieb (Veredler, Betreiber, Auditor) durch private oder öffentlich-private Akteure wahrscheinlich. Die vorstellbare Rollenbesetzung auf Basis des Stakeholderclusters ist in Abbildung 6 grafisch veranschaulicht.

Abbildung 6: Rollenverteilung nach Stakeholdercluster



Fehlende Rollen

Frage II:

Fehlt Ihrer Meinung nach eine Rolle? Wenn ja, welche?

Antworten II:

- Regulation
- Vertrieb
- Qualitätssicherung der Daten und des Labellings hinsichtlich: IID (independently and identically distributed), IT-Sicherheit (Posioning Angriffe), Bias, Abdeckung von Corner Cases

Interpretation:

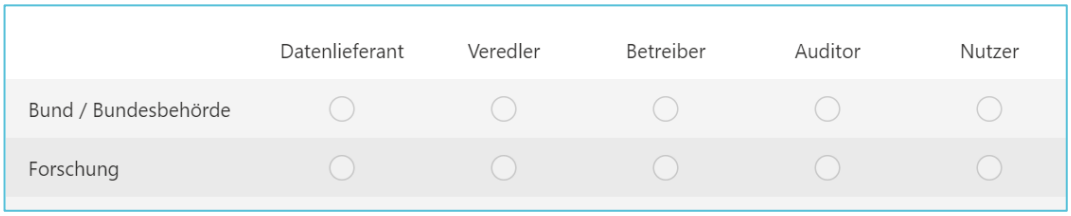
Neben den bereits ausdifferenzierten Rollen wurden von den Befragten weitere wichtige Rollen für einen möglichen Szenariendatenbankbetrieb identifiziert. Die Rolle der Regulierung ist definitiv eine der wichtigsten für die Erfolgsaussichten der Datenbank. Jedoch findet sie im vorliegenden Rollenmodell keine separate Betrachtung, da die Rolle durch die stattlichen Institutionen besetzt wird und damit in der Frage der Rollenverteilung für das Betreibermodell nicht ausschlaggebend ist. Der Vertrieb wird nach dem Verständnis im vorliegenden Rollenmodell in der Betreiberrolle gesehen und wird demnach auch in der Rollenbeschreibung ergänzt, während die Qualitätssicherung durch diverse Mechanismen, wie beispielsweise eine umfängliche Nachvollziehbarkeit des Ursprungs der Daten (Traceability), eines externen Zertifizierers (z.B. der Auditor) oder durch eine Partnerschaft zwischen Veredler und Betreiber, erreicht werden kann.

Rollenzuschreibungen anderer Institutionen

Frage III:

Welche Stakeholder sehen Sie in welcher Rolle?
(Für jede Stakeholdergruppe konnte jeweils eine Rolle ausgewählt werden (vgl. Abbildung 7))

Abbildung 7: Darstellung der Fragestellung III



Antworten III: Gesamtübersicht

Die Antworten werden als Häufigkeit der Auswahl der jeweiligen Stakeholder für die jeweilige Rolle dargestellt (vgl. Tabelle 3). N beschreibt die Gesamtzahl der Auswahl des jeweiligen Stakeholders in der jeweiligen Rolle.

Tabelle 3: Antworten III Gesamtübersicht

Datenlieferant		Veredler		Betreiber		Auditor		Nutzer	
n	**Stakeholder**	**n**	**Stakeholder**	**n**	**Stakeholder**	**n**	**Stakeholder**	**n**	**Stakeholder**
23	Infrastrukturunternehmen	25	KI-Unternehmen / Tech. StartUp	19	Toolhersteller/ IT-Infrastruktur	15	Bund / Bundesbehörde	20	OEMs
22	ÖPNV	17	Forschung	11	Bund / Bundesbehörde	14	Technische Dienste	15	ÖPNV
22	Logistik	14	Toolhersteller/ IT-Infrastruktur	10	Integratoren	4	Integratoren	15	Zulieferer (Tier1)
18	OEMs	11	Integratoren	8	Technische Dienste	2	Forschung	15	Mobilitätsdienstanbieter

Interpretation:

Die in der ersten Zeile der Tabelle 3 zusammengefassten Ergebnisse und damit die am häufigsten in dieser Kernbetriebsrolle assoziierten Stakeholdergruppen stützen die bereits in der Interpretation der Frage II herausgestellten Ergebnisse. So werden im Kernbetrieb KI-Unternehmen / Tech. Start-Ups von 25 Befragten in der Veredlerrolle, Toolhersteller / IT-Infrastruktur Unternehmen von 19 Befragten in der Betreiberrolle und der Bund / Bundesbehörde bzw. die Technischen Dienste von 14 bzw. 15 Befragten in der Auditorrolle gesehen.

Besonders hervorzuheben ist die Fremdsicht auf die Betreiberrolle, in welcher auf zweiter Stufe der öffentliche Sektor als Stakeholder gesehen wird, wohingegen in der Selbstsicht der Akteure (Frage II) der öffentliche Sektor sich als eher unwahrscheinlich in der Betreiberrolle sieht. Zusätzlich sehen 17 bzw. 14 der Befragten auch die Möglichkeit der Übernahme der Veredlerrolle durch Forschungsinstitute bzw. Toolhersteller / IT-Infrastruktur Unternehmen.

Abschnitt II: Anreiz- und Hemmnisevaluation

Die bereits identifizierten Anreize und Hürden (vgl. Hintergrund) wurden durch die Fragen im folgenden Abschnitt anhand einer Likert-Skala evaluiert. Die Ergebnisse sind wie im vorstehenden Abschnitt in Boxplot-Diagrammen zusammengefasst. Die Reihenfolge der Anreize und Hemmnisse wird durch den Mittelwert bestimmt. Der Anreiz bzw. das Hemmnis mit der höchsten Ausprägung des Mittelwerts wird an oberster Stelle aufgeführt. Es wurde der Mittelwert zur Priorisierung trotz ordinaler Verteilung gewählt, da der Median in vielen Bewertungen dieselbe Ausprägung besitzt. In der Tabellarischen Darstellung wird der Mittelwert in der höchsten Ausprägung in Klammern angegeben, um trotz gleichem Median eine Priorisierung zu ermöglichen.

Anreizevaluation

a) Datenlieferant

Frage IV: Anreize für Datenlieferung

Die von Ihnen repräsentierte Institution ist (hypothetisch) Datenhalter von, in der Szenariendatenbank verwertbaren, Datensätzen. Wie würden Sie die folgenden Anreize priorisieren, um eine Datenlieferung durch die von Ihnen repräsentierte Institution zu motivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten IV: Gesamtübersicht

Abbildung 8: Antworten IV Gesamtübersicht

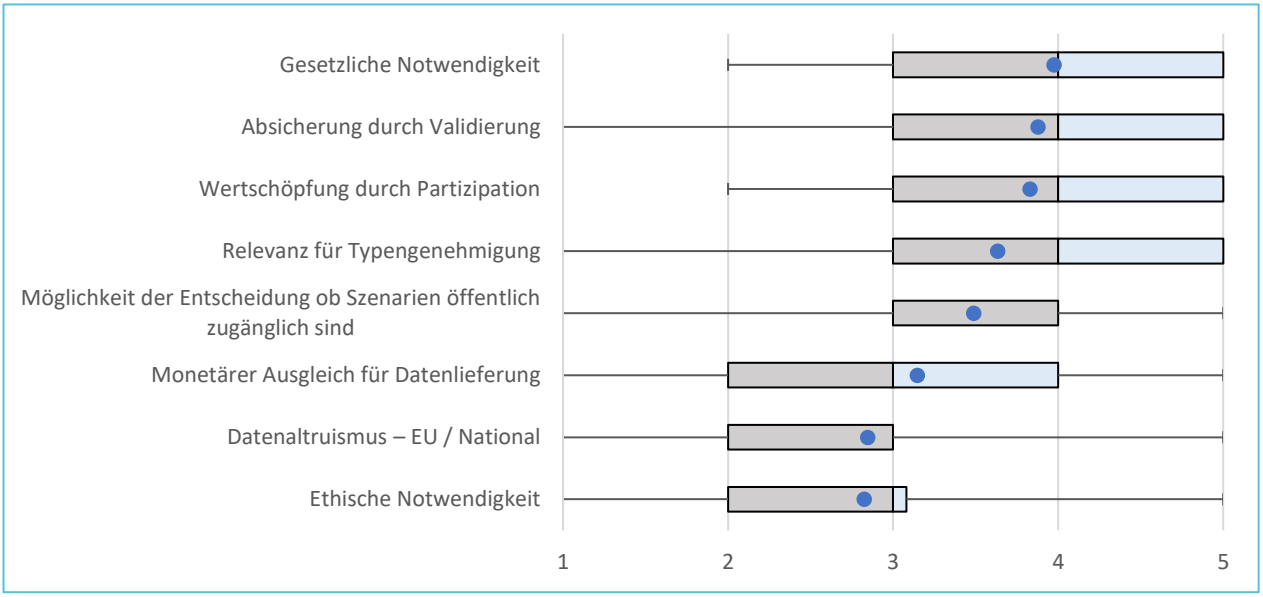


Tabelle 4: Differenzierung der Antworten IV nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Anreiz	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Gesetzliche Notwendigkeit	**5 (5,0)**	4	**4 (3,9)**
Absicherung durch Validierung	3	4	4
Wertschöpfung durch Partizipation	3	**4 (4,2)**	4
Relevanz für Typengenehmigung	3	4	4
Möglichkeit der Entscheidung, ob Szenarien öffentlich zugänglich sind	3	4	3
Monetärer Ausgleich für Datenlieferung	1	3	3,5
Datenaltruismus – EU / National	3	3	2
Ethische Notwendigkeit	4	3	2

b) Veredler

Frage V: Anreize für Datenveredelung

Die von Ihnen repräsentierte Institution ist (hypothetisch) zuständig für die Rohdaten-Anonymisierung, das Labelling und der Szenariencreation zur Aufbereitung der Datensätze für die Szenariendatenbank. Wie würden Sie die folgenden Anreize priorisieren, um eine Datenveredelung durch die von Ihnen repräsentierte Institution zu motivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten V: Gesamtübersicht

Abbildung 9: Antworten V Gesamtübersicht

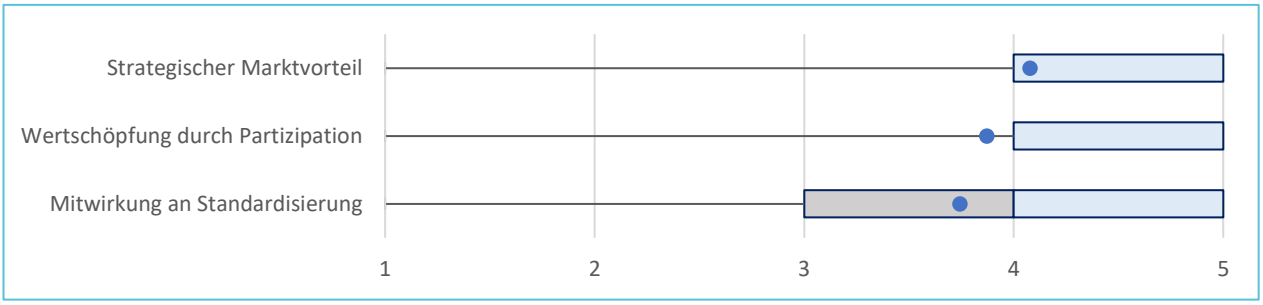


Tabelle 5: Differenzierung der Antworten V nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Anreiz	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Strategischer Marktvorteil	2	**4 (4,3)**	**4,5 (4,1)**
Wertschöpfung durch Partizipation	3,5	4	4
Mitwirkung an Standardisierung	**3,5 (3,8)**	4	4

c) Betreiber

Frage VI: Anreize für Datenbankbetrieb

Die von Ihnen repräsentierte Institution ist (hypothetisch) Betreiber der Szenariendatenbank. Wie würden Sie die folgenden Anreize priorisieren, um einen Datenbankbetrieb durch die von Ihnen repräsentierte Institution zu motivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten VI: Gesamtübersicht

Abbildung 10: Antworten VI Gesamtübersicht

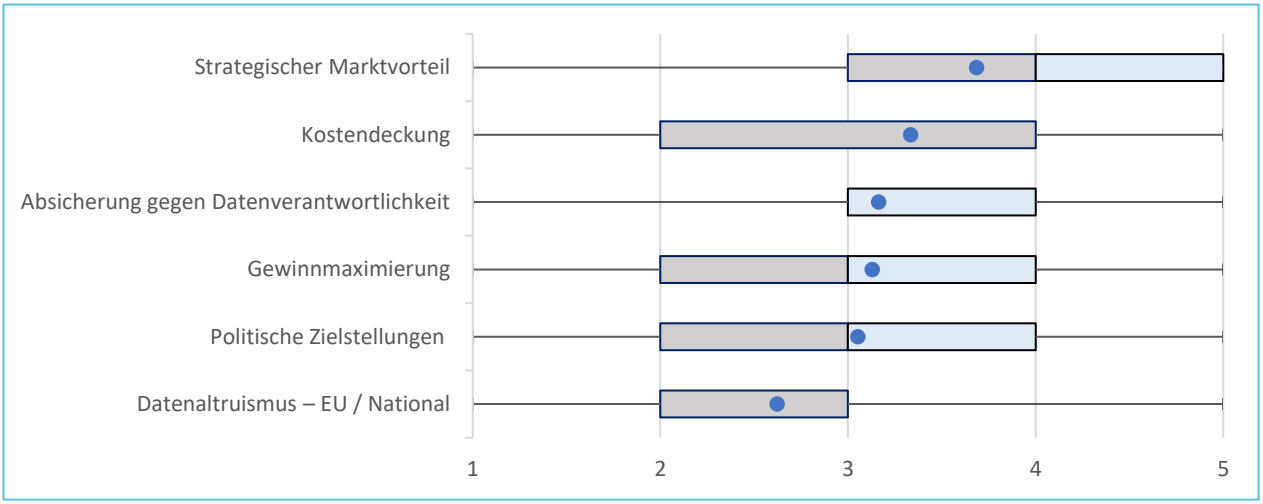


Tabelle 6: Differenzierung der Antworten VI nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Anreiz	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Strategischer Marktvorteil	2	**4 (3,5)**	**5 (4,2)**
Kostendeckung	1	4	4
Absicherung gegen Datenverantwortlichkeit	3	4	3
Gewinnmaximierung	1	3	4
Politische Zielstellungen	**4,5 (4,3)**	3	2
Datenaltruismus – EU / National	3	3	2

d) Auditor

Frage VII: Anreize für Datenbankauditierung

Die von Ihnen repräsentierte Institution ist (hypothetisch) der Auditor der Szenariendatenbank. Wie würden Sie die folgenden Anreize priorisieren, um eine Auditierung durch die von Ihnen repräsentierte Institution zu motivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten VII: Gesamtübersicht

Abbildung 11: Antworten VII Gesamtübersicht

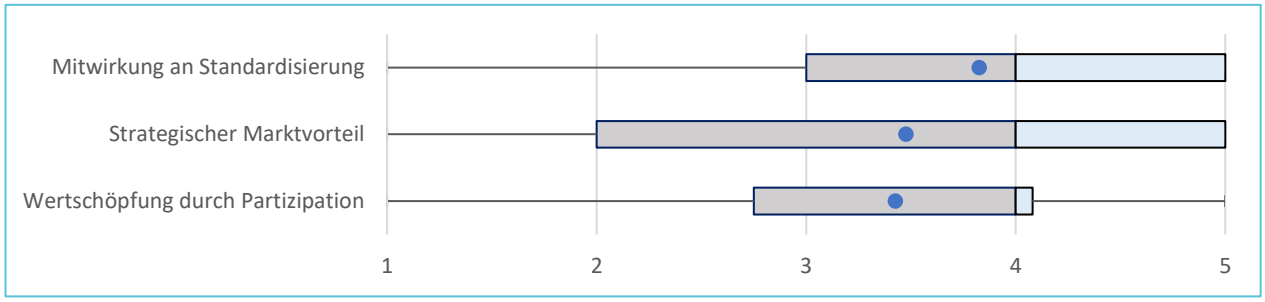


Tabelle 7: Differenzierung der Antworten VII nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Anreiz	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Mitwirkung an Standardisierung	**3,5 (3,3)**	**4 (4,1)**	**4(3,8)**
Strategischer Marktvorteil	1,5	4	4
Wertschöpfung durch Partizipation	2	4	4

e) Nutzer

Frage VIII: Anreize für Datenbanknutzung

Die von Ihnen repräsentierte Institution ist (hypothetisch) Nutzer der Szenariendatenbank. Wie würden Sie die folgenden Anreize priorisieren, um einen Nutzung der Datenbank durch die von Ihnen repräsentierte Institution zu motivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten VIII: Gesamtübersicht

Abbildung 12: Antworten VIII Gesamtübersicht

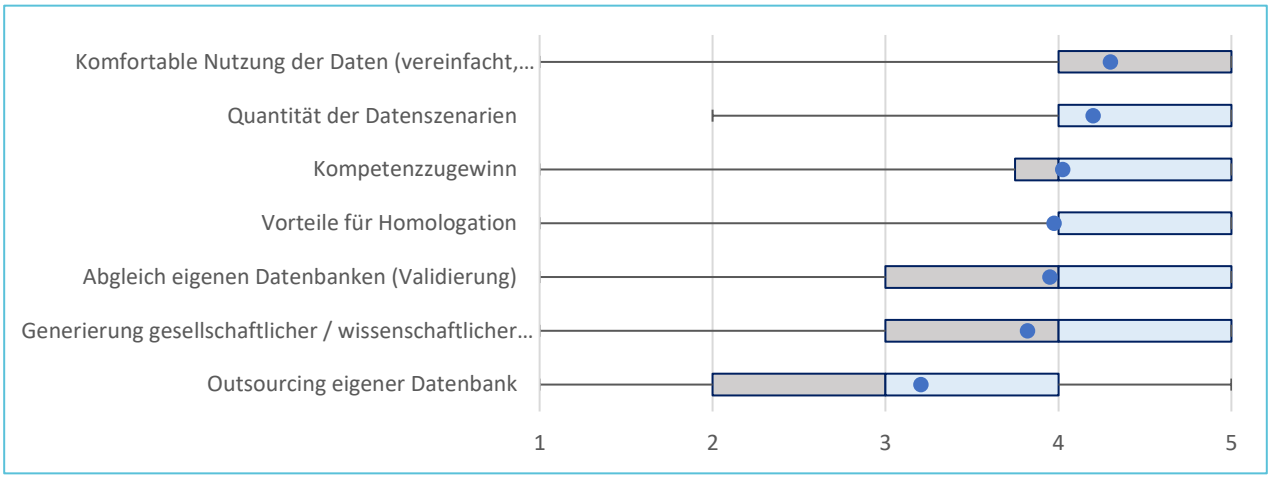


Tabelle 8: Differenzierung der Antworten VIII nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Anreiz	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Komfortable Nutzung der Daten (vereinfacht, vereinheitlichtes Datenformat geclustert)	4	**5 (4,5)**	**5 (4,2)**
Quantität der Datenszenarien	3,5	4	4,5
Kompetenzzugewinn	**4,5 (4,5)**	4	4
Vorteile für Homologation	1,5	4	4,5
Abgleich eigenen Datenbanken (Validierung)	3	5	4
Generierung gesellschaftlicher / wissenschaftlicher Akzeptanz	4	4	4
Outsourcing eigener Datenbank	1	4	3

Hemmnisevaluation

a) Datenlieferant

Frage IX: Hürden der Datenlieferung

Die von Ihnen repräsentierte Institution ist (hypothetisch) Datenhalter von, in der Szenariendatenbank verwertbaren, Datensätzen. Wie würden Sie die folgenden Hürden priorisieren, welche die von Ihnen repräsentierte Institution an einer Datenlieferung hindern? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten IX: Gesamtübersicht

Abbildung 13: Antworten IX Gesamtübersicht

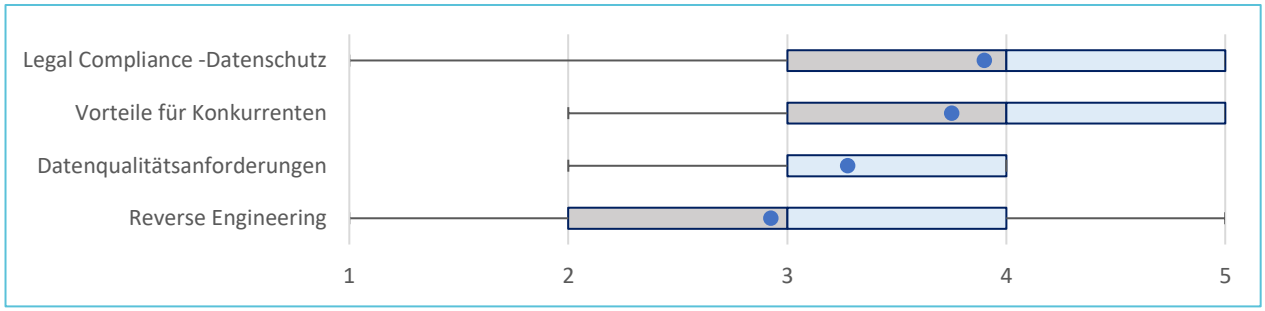


Tabelle 9: Differenzierung der Antworten IX nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Hemmnis	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Legal Compliance -Datenschutz	**4,5 (4,0)**	4	**4 (4,0)**
Vorteile für Konkurrenten	1	**4,5 (4,1)**	**4 (4,0)**
Datenqualitätsanforderungen	3,5	3	3
Reverse Engineering	2,5	3	3,5

b) Veredler

Frage X: Hürden der Datenveredelung

Die von Ihnen repräsentierte Institution ist (hypothetisch) zuständig für die Rohdaten-Anonymisierung, das Labelling und der Szenariencreation zur Aufbereitung der Datensätze für die Szenariendatenbank. Wie würden Sie die folgenden Hürden priorisieren, welche eine Datenveredelung durch die von Ihnen repräsentierte Institution hindern? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten X: Gesamtübersicht

Abbildung 14: Antworten X Gesamtübersicht

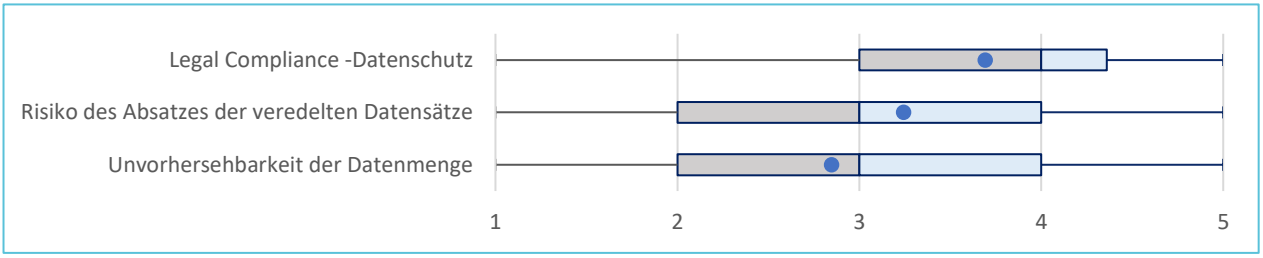


Tabelle 10: Differenzierung der Antworten X nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Hemmnis	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Legal Compliance -Datenschutz	**2,5 (3,5)**	**3,5 (3,6)**	**4 (4,0)**
Risiko des Absatzes der veredelten Datensätze	1	3	4
Unvorhersehbarkeit der Datenmenge	2,5	3	3

c) Betreiber

Frage XI: Hürden des Datenbankbetriebs

Die von ihnen repräsentierte Institution ist (hypothetisch) Betreiber der Szenariendatenbank. Wie würden Sie die folgenden Hürden priorisieren, welche einen Datenbankbetrieb durch die von Ihnen repräsentierte Institution demotivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten XI: Gesamtübersicht

Abbildung 15: Antworten XI Gesamtübersicht

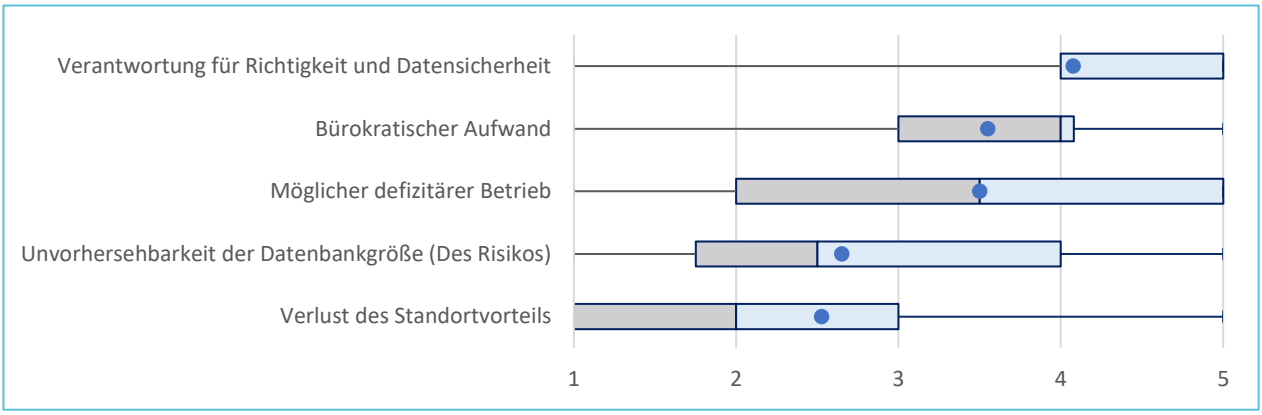


Tabelle 11: Differenzierung der Antworten XI nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Hemmnis	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Verantwortung für Richtigkeit und Datensicherheit	**4,5 (4,0)**	**4,5 (4,1)**	**4 (4,1)**
Bürokratischer Aufwand	3	4	4
Möglicher defizitärer Betrieb	1,5	3,5	4
Unvorhersehbarkeit der Datenmenge	2,5	3	3
Verlust des Standortvorteils	1	2	2

d) Auditor

Frage XII: Hürden der Datenbankauditierung

Die von Ihnen repräsentierte Institution ist (hypothetisch) der Auditor der Szenariendatenbank. Wie würden Sie die folgenden Hürden priorisieren, welche eine Auditierung durch die von Ihnen repräsentierte Institution hindern? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten XII: Gesamtübersicht

Abbildung 16: Antworten XII Gesamtübersicht

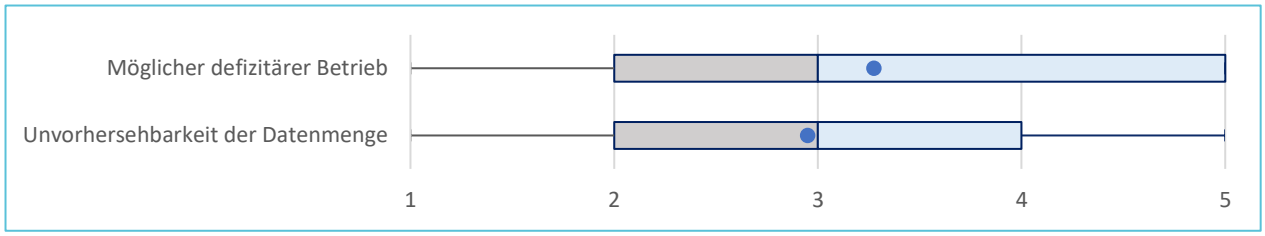


Tabelle 12: Differenzierung der Antworten XII nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Hemmnis	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Möglicher defizitärer Betrieb	1,5	**3,5 (3,4)**	**4 (3,5)**
Unvorhersehbarkeit der Datenmenge	**2,5 (2,8)**	3	3

e) Nutzer

Frage XIII: Hürden der Datenbanknutzung

Die von ihnen repräsentierte Institution ist (hypothetisch) Nutzer der Szenariendatenbank. Wie würden Sie die folgenden Hürden priorisieren, welche eine Datenbanknutzung durch die von Ihnen repräsentierte Institution demotivieren? (1 = niedrige Priorität | 5 = hohe Priorität)?

Antworten XIII: Gesamtübersicht

Abbildung 17: Antworten XIII Gesamtübersicht

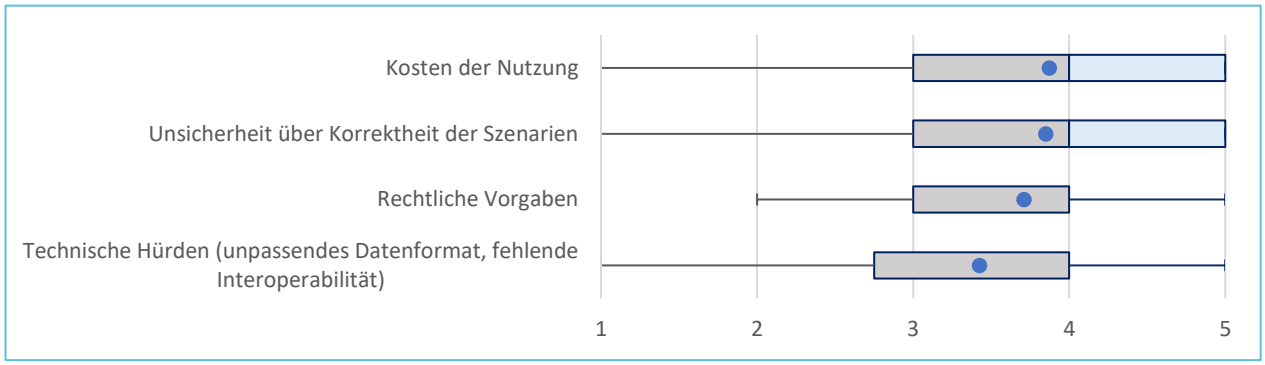


Tabelle 13: Differenzierung der Antworten XIII nach Stakeholdercluster

	Median (Mittelwert höchster Priorisierung)		
Hemmnis	**Öffentlich**	**Öffentlich / Privat**	**Privat**
Kosten der Nutzung	3	**4 (4,1)**	4
Unsicherheit über Korrektheit der Szenarien	3,5	4	**4 (4,0)**
Rechtliche Vorgaben	**4,5 (4,5)**	4	4
Technische Hürden (unpassendes Datenformat, fehlende Interoperabilität)	3	4	4

Weitere Anreize und Hemmnisse der Partizipation

Neben den bereits erarbeiteten Anreizen und Hürden, wurden von den Befragten weitere Hemmnisse (vgl. Tabelle 14) und Anreize (vgl. Tabelle 15) der Partizipation identifiziert. Weitere Hürden können besonders im Bereich der rechtlichen Vorgaben insbesondere des Datenschutzrechts, der Einfachheit der Nutzerzugänge und im benötigten Grundstock an Szenarien zur Nutzbarkeit der Datenbank gesehen werden. Diese Bereiche wurden versucht durch die ausgewiesenen und evaluierten Hemmnisse abzudecken. Es bedarf im weiteren Verlauf an dieser Stelle noch einer klareren Differenzierung. Mit Blick auf die Anreize wurden bereits genannte Anreize noch einmal detaillierter ausdifferenziert, sowie auf die Anreizwirkung der Partizipation von Schlüsselskateholder (OEMs, Tier1s und technische Dienste) eingegangen. Diese Anreizwirkung wird auch Teil der abschließenden Evaluation.

Tabelle 14: Weitere zu berücksichtigende Hemmnisse

Gesellschaftliche und rechtliche Akzeptanz
Datenvorratshaltung - Gültigkeit des Datenbestandes
Anonymisierung von Daten und Nutzen von anonymisierten Daten
Auditor - Gesetzesvorgaben, Regulative
Das nun private Entitäten Geld verdienen und öffentliche Institutionen wie Verkehrsunternehmen oder Kommunen nur Aufwand haben
ggf unvorteilhafte Nutzungsbedingungen
Potentielle Hürde als Nutzer/Lieferant: Es gibt zu wenig Beitragende (sowohl als Lieferant als auch als Nutzer). Wenn die Datenbank nicht in der Breite genutzt/unterstützt wird (insbesondere von OEMs, Tier1s, TÜV,...) fallen viele der Anreize weg diese zu nutzen.

Tabelle 15: Weitere zu berücksichtigende Anreize

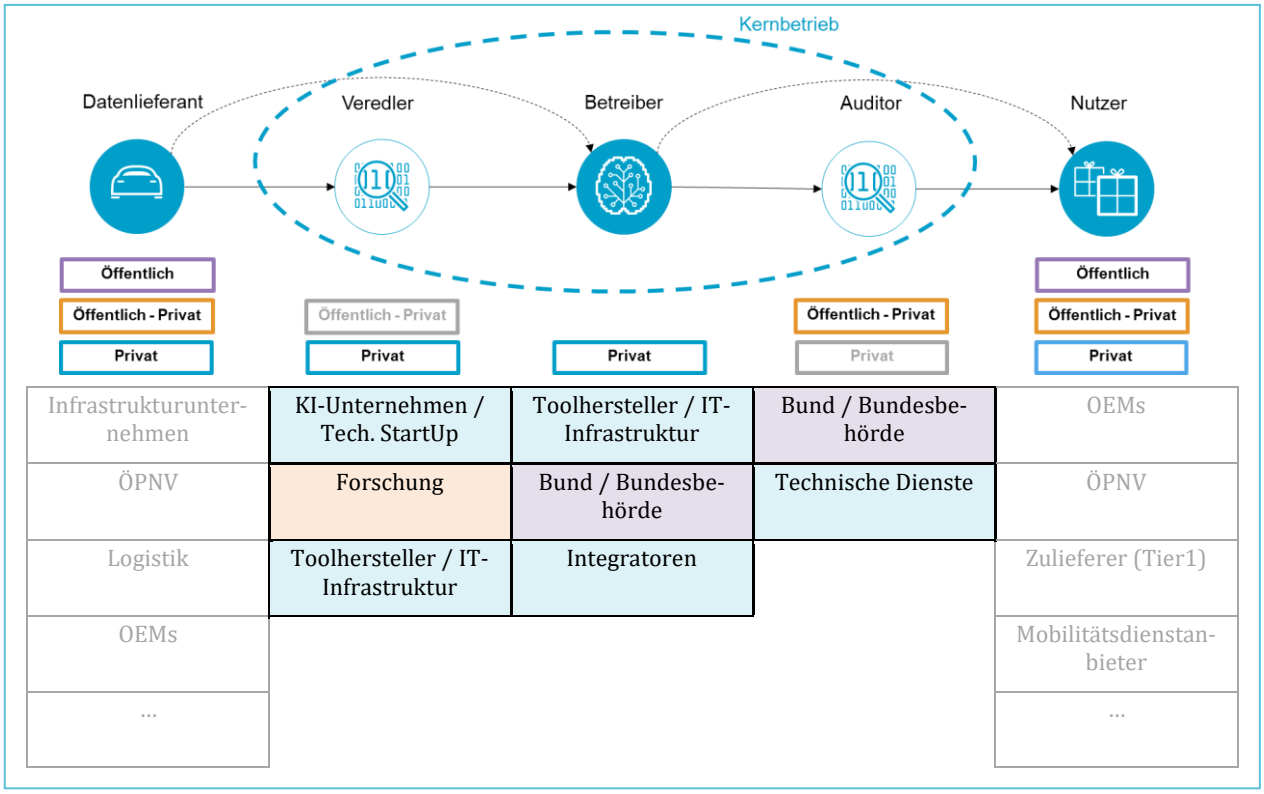
Standardisierung hinsichtlich Erhebung, Nutzung und Auswertung
Redundante (hier Betreiber der Infrastruktur Datenbank) Datawarehouses/Datacenter - in welchen Lokationen (nur Germany, nur Europa, ...)
Gesetzliche Regelung
Wenn sich OEMs/Tier1s/TÜV gemeinsam zur Nutzung einer bestimmten Datenbank "bekennen" ist der Anreiz diese zu nutzen um ein Vielfaches höher.

Fazit

Rollenverteilung

Aus den Umfrageergebnissen lassen sich Rückschlüsse auf die Rollenverteilung in einem hypothetischen Datenbankbetrieb ableiten. Nachdem die Befragten zunächst selbst die Wahrscheinlichkeit der Rollenbesetzung durch die eigene Institution bewerten konnten, wurde aufbauend die Einschätzung der Rollenbesetzung durch andere Institutionen abgefragt. Die Ergebnisse fasst Abbildung 18 zusammen.

Abbildung 18: Zusammenfassung der hypothetischen Rollenverteilung im Datenbankbetrieb



Generell wurden hohe Wahrscheinlichkeiten für die Besetzung der Nutzer- und Datenlieferantenrolle wahrgenommen, daher liegt der Fokus der anschließenden Folgerungen zunächst auf dem Kernbetrieb.

Die Veredlerrolle ist nach der Positionierung der eigenen Institutionen am wahrscheinlichsten durch private Akteure besetzt. Die Befragten sehen die Stakeholdergruppe KI-Unternehmen / Tech. Start-Ups am häufigsten in dieser Rolle.

Die Betreiberrolle ist nach der Positionierung der eigenen Institutionen am wahrscheinlichsten durch private Akteure besetzt. Die Befragten sehen die Stakeholdergruppe Toolhersteller / IT-Infrastruktur am häufigsten in dieser Rolle.

Die Auditorrolle ist nach der Positionierung der eigenen Institutionen am wahrscheinlichsten durch öffentlich-private Akteure besetzt. Abweichend davon sehen die Befragten die Stakeholdergruppe Bund / Bundesbehörde bzw. die technischen Dienste in dieser Rolle.

Anreize und Hemmnisse der Partizipation

Ausgehend von der zuvor beschriebenen Rollenverteilung können aus den Umfrageergebnissen die am stärksten wahrgenommenen Hemmnisse und Anreize für die jeweilige Rollenbesetzung im Kernbetrieb abgeleitet werden. Wenn die Priorisierung der einzelnen Anreize bzw. Hemmnisse gleich ausfällt, werden alle am höchsten bewerteten Anreize bzw. Hürden angegeben.

Anreize und Hemmnisse der Partizipation im Kernbetrieb

Veredler:

Prio.	Stakeholder	Größter Anreiz	Größtes Hemmnis
1	KI-Unternehmen / Tech. StartUp	• Strategischer Marktvorteil	• Legal Compliance -Datenschutz • Risiko des Absatzes der veredelten Datensätze • Unvorhersehbarkeit der Datenmenge
2	Forschung	• Strategischer Marktvorteil • Wertschöpfung durch Partizipation • Mitwirkung an Standardisierung	• Legal Compliance – insbes. Datenschutz
3	Toolhersteller / IT-Infrastruktur	• Strategischer Marktvorteil	• Legal Compliance -Datenschutz • Risiko des Absatzes der veredelten Datensätze

Betreiber:

Prio.	Stakeholder	Größter Anreiz	Größtes Hemmnis
1	Toolhersteller / IT-Infrastruktur	• Strategischer Marktvorteil	• Verantwortung für Richtigkeit und Datensicherheit • Bürokratischer Aufwand
2	Bund / Bundesbehörde	• Politische Zielstellungen	• Verantwortung für Richtigkeit und Datensicherheit
3	Integratoren	• Strategischer Marktvorteil	• Verantwortung für Richtigkeit und Datensicherheit • Bürokratischer Aufwand

Auditor:

Prio.	Stakeholder	Größter Anreiz	Größtes Hemmnis
1	Bund / Bundesbehörde	• Mitwirkung an Standardisierung	• Unvorhersehbarkeit der Datenmenge
2	Technische Dienste	• Mitwirkung an Standardisierung • Strategischer Marktvorteil • Wertschöpfung durch Partizipation	• Möglicher defizitärer Betrieb

Anreize und Hemmnisse der Datenlieferung und Nutzung

Neben den Anreizen und Hürden zur Besetzung der Kernbetriebsrollen werden im Folgenden auch die evaluierten Anreize bzw. Hürden der Datenlieferung und Nutzung zusammengefasst. Da für beide Rollen eine Vielzahl verschiedener Stakeholdergruppen als Besetzung in Frage kommen wurden die zusammenfassenden Tabellen nach den Stakeholdercluster (Privat / Öffentlich-Privat / Öffentlich) gegliedert.

Datenlieferant:

Stakeholder-cluster	Größter Anreiz	Größtes Hemmnis
Privat	• Gesetzliche Notwendigkeit • Absicherung durch Validierung • Wertschöpfung durch Partizipation • Relevanz für Typengenehmigung	• Legal Compliance -Datenschutz • Vorteile für Konkurrenten
Öffentlich-Privat	• Gesetzliche Notwendigkeit • Absicherung durch Validierung • Wertschöpfung durch Partizipation • Relevanz für Typengenehmigung • Möglichkeit der Entscheidung, ob Szenarien öffentlich zugänglich sind	• Vorteile für Konkurrenten
Öffentlich	• Gesetzliche Notwendigkeit	• Legal Compliance -Datenschutz

Nutzer:

Stakeholder-cluster	Größter Anreiz	Größtes Hemmnis
Privat	• Komfortable Nutzung der Daten (vereinfacht, vereinheitlichtes Datenformat geclustert)	• Kosten der Nutzung • Unsicherheit über Korrektheit der Szenarien • Rechtliche Vorgaben • Technische Hürden (unpassendes Datenformat, fehlende Interoperabilität)
Öffentlich-Privat	• Komfortable Nutzung der Daten (vereinfacht, vereinheitlichtes Datenformat geclustert) • Abgleich eigenen Datenbanken (Validierung)	• Kosten der Nutzung • Unsicherheit über Korrektheit der Szenarien • Rechtliche Vorgaben • Technische Hürden (unpassendes Datenformat, fehlende Interoperabilität)
Öffentlich	• Kompetenzzugewinn	• Rechtliche Vorgaben

Mögliche Incentivierung der Akteure

Aus den Umfrageergebnissen können diverse Schlussfolgerungen bezüglich der Incentivierung abgeleitet werden. So würde eine gesetzliche Notwendigkeit zur Datenlieferung alle Akteure am stärksten motivieren, ihre Daten in der Datenbank zur Verfügung zu stellen. Simultan müssten die Vorteile für Konkurrenten über geeignete Mechanismen wie zum Beispiel ein Punktesystem zum Austausch möglichst gering gehalten werden und die Datenschutzanforderungen aus der Verantwortung der

Datenlieferanten durch beispielsweise eine im Betrieb integrierte Anonymisierung genommen werden. Dies hätte jedoch eine Wechselwirkung durch die Verantwortungsverlagerung auf die Betreiberrolle zur Folge und würde im Rückschluss diese Besetzung deattraktiveren.

Da die Veredlerrolle nach Einschätzung der Befragten durch Akteure aus dem privatwirtschaftlichen Bereich besetzt werden sollte, müsste der sich ergebende strategische Marktvorteil klar herausgearbeitet werden, um private Akteure für diese Rolle zu motivieren. Eine weitere Hürde stellt für die Akteure der Veredler das Risiko dar, nach bereits vorgenommener Veredelung einen zu kleinen Absatz für die erstellten Szenarien zu erzielen. Hier könnte beispielsweise eine Sicherstellung der Kostendeckung durch einen öffentlichen Finanzier einen Lösungsansatz darstellen.

Da auch die Betreiberrolle nach Einschätzung der Befragten am wahrscheinlichsten durch das private Cluster besetzt wird, müssten hier Akteure über den strategischen Marktvorteil motiviert werden. Die Verantwortung für die Richtigkeit der zur Verfügung gestellten Daten, könnten wiederrum durch einen externen Gutachter bzw. Auditor gemindert werden. Da auch die Kostendeckung des Betriebs als hoher Anreiz eingeschätzt wird, könnte ähnlich dem Lösungsvorschlag zur Besetzung der Veredlerrolle eine Kostendeckung durch Drittmittel generiert werden.

Die Besetzung der bereits angesprochenen Rolle des Auditors durch einen privaten bzw. öffentlich-privaten Akteur wird, den Umfrageergebnissen zufolge, besonders durch die Mitwirkung an der Standardisierung motiviert und durch einen möglichen defizitären Betrieb gehemmt. Hierfür könnte der Kontext der Standardisierung noch weiter in den Mittelpunkt der Szenariendatenbank gerückt werden und durch die bereits beschriebenen Maßnahmen ein defizitärer Betrieb mit Auswirkung auf den Auditor ausgeschlossen werden.

Die Nutzung durch private bzw. öffentlich-private Akteure wird durch einen komfortablen Zugriff und ein vereinheitlichtes Dateiformat motiviert. Dies kann durch die Integration der Veredlung in den Datenbankkernbetrieb erreicht werden und wird nochmals verstärkt durch das Anpassen der Nutzerzugänge je nach Use Case und Clusterzugehörigkeit. Öffentliche Akteure incentiviert der mögliche Kompetenzzugewinn. Hemmer der Datenbanknutzung stellen Kosten der Nutzung, Unsicherheit betreffend die Korrektheit der Szenarien und die Einhaltung rechtlicher Vorgaben dar. Die Kosten der Nutzung könnten je nach zugreifender Stakeholdergruppe angepasst werden. So müssten zum Beispiel OEMs mehr Tauscheinheiten zum Einkauf eines Szenarios aufwenden als beispielsweise Forschungsinstitute. Die Korrektheit der Szenarien könnte wie oben beschrieben durch einen externen Zertifizierer oder durch die Verantwortungsverlagerung in Richtung des Datenlieferanten (Traceability der Daten) sichergestellt werden.

Es lässt sich zusammenfassen, dass die Partizipation in der Szenariendatenbank stark vom Stakeholdercluster bzw. der Stakeholdergruppenzugehörigkeit abhängt. So werden einige Anreize von öffentlichen Akteuren sehr hoch priorisiert, während private bzw. öffentlich-private Akteure diesen eher eine geringe Priorität zuordnen. Dennoch konnten, auf Grundlage der vorliegenden Ergebnisse, die einzelnen Rollenverteilungen nach der höchsten Wahrscheinlichkeit durch einzelne Stakeholdergruppen hypothetisch besetzt werden. Zudem wurden aus der Evaluation der Anreize und Hindernisse stakeholderspezifische Hebel der Umsetzung für die vorab bewertete Rollenbesetzung entwickelt.

IKEM – Institut für Klimaschutz, Energie und Mobilität e.V.

Berlin • Greifswald • Stuttgart

www.ikem.de

Magazinstraße 15 – 16
10179 **Berlin**

T +49 (0)30 408 1870 10
F +49 (0)30 408 1870 29

info@ikem.de

Domstraße 20a
17489 **Greifswald**

T +49 (0)38 34 420 2100
F +49 (0)38 34 420 2002

lsrodi@uni-greifswald.de

A4: Lastenheft für die kooperative Szenariendatenbank

FE 82.0719/2018 - Entwicklung eines Lastenhefts für eine Szenariendatenbank zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen

ERSTELLT VON

Christopher Wiegand

dSPACE

Alexander Klinge

Institut für Klimaschutz, Energie und Mobilität e.V.

Heiko Ehrich, Andre Simon
TÜV NORD Mobilität GmbH & Co. KG

IM AUFTRAG DER
Bundesanstalt für Straßenwesen

Inhalt

1 Gesamtziel ... 3

2 Ziel des Lastenheft ... 3

3 Struktur des Lastenheft ... 5

4 Anforderungen ... 7

4.1 Technische Rahmenarchitektur ... 7

Grundlegende Architektur ... 7

Anwenderschnittelle und Anwenderdialog ... 8

Effiziente Ressourcennutzung zur Realisierung der Datenbank ... 8

Wartbarkeit und Erweiterbarkeit ... 9

Datenbank in den Wartungsmodus versetzen ... 9

4.2 Anwendungsfall 1: Szenarien im Entwicklungs- und Absicherungsprozess ... 9

Organisation und Speicherung von Szenariodaten in der Datenbank ... 10

Metadaten zu anonymisierten, personenbezogenen Daten ... 11

4.3 Anwendungsfall 2: Einspeisen von Szenarien in die Datenbank (ggf. Veredelung) ... 11

Lieferung von Szenariodaten ... 11

Externe Anonymisierung der gelieferten Szenariodaten ... 11

Uploadmanager für das Einspeisen von Szenarien ... 12

Prüfung und Bewertung von gelieferten Szenariodaten ... 12

Veredelung der gelieferten Szenariodaten ... 12

Auditierung der veredelten Daten ... 13

Informationssicheres Datenbankkonzept ... 13

Absicherung nicht anonymisierter, personenbezogener Daten ... 14

Verschlüsselung von personenbezogenen Daten ... 15

Löschung personenbezogener Daten ... 15

Löschen von Szenariodaten in der Datenbank ... 16

Privater Bereich zum organisieren eigener Szenarien ... 16

4.4 Anforderungsfall 3: Anbindung weiterer Datenquellen ... 16

Anbindung externer Datenquellen 16
Ontologie der Szenariendatenbanken 17
4.5 Anforderungsfall 4: Effiziente Nutzung durch hochwertige Mechanismen zum finden passender Szenarien 17
Suchen und Filtern von Szenarien 17
Abrufen von ausgewählten Szenariodaten 18
Detailansicht einzelner Szenarien 18
Downloadmanager für den Abruf von Szenariodaten 18
Datenpipline für Rohdaten Upload 19
Definition der eigenen ODD 19
ODD Management 19
4.6 Anforderungsfall 5: Abrechnungs- und Zugriffsmodell 19
Mitgliedsbeitragfinanzierung für die Datenbanknutzung 20
Anwender- und Rechtemanagement 20
Anlegen neuer Anwender 21
Administratives Bearbeiten von Anwenderdaten 21
Deaktivieren von Datenbankanwendern 21
Reaktiveren von Datenbankanwendern 22
Löschen von Datenbanknutzern 22
Als neuer Nutzer oder Datenlieferant registrieren 22
Anwenderdaten bearbeiten 23
Anwendersupport 23

1 Gesamtziel

Mit der Öffnung des Straßenverkehrsgesetzes 2017 und dem Gesetzesvorhaben zum autonomen Fahren wurden auf nationaler Ebene die normativen Weichen für Fahrfunktionen höherer Automatisierungsgrade gestellt.

Als Grundlage für die Entwicklung und Bewertung der verkehrssicherheitstechnischen Auswirkungen des Einsatzes automatisierter Fahrfunktionen im öffentlichen Raum sind geeignete Szenarienkataloge erforderlich, welche den Einsatzbereich und die funktionsrelevanten Parameter des Fahrzeugs abdecken.

Bislang stehen lediglich vereinzelt singuläre Datenquellen zur Verfügung, welche nur begrenzt für jedermann zugänglich sind. Eine fusionierte Datengrundlage könnte einen großen Erkenntnisgewinn generieren, auf dessen Grundlage entwickelt, Regulierungsbedarf eruiert und demokratische Debatten geführt werden können.

In dem Zusammenhang wurde mit Umsetzung des Projekts (FE 82.0719/2018) im Auftrag der Bundesanstalt für Straßenwesen (BASt) in Kollaboration der Partner Consulting4Drive, dSPACE, IKEM und TÜV NORD Mobilität eine Analyse der technischen, wirtschaftlichen und wissenschaftlichen Rahmenbedingungen für eine kollaborative Szenariendatenbank durchgeführt. Als Teilergebnis der durchgeführten Arbeiten wurde das vorliegende Anforderungslastenheft erstellt, welches bei der möglichen Implementierung der Datenbank berücksichtigt werden sollte.

Das vorliegende Lastenheft ist Anlage des Projektschussberichts FE 82.07/19/2018 SzeDaBa.

2 Ziel des Lastenheft

Ziel des Lastenhefts für die kooperative Datenbank ist die Beschreibung eines Anforderungskatalogs über notwendige Leistungsmerkmale der Datenbank, welche bei einer Implementierung berücksichtigt werden sollten.

Hierzu wurden die Forschungsergebnisse der einzelnen Partner aus den umgesetzten Arbeitspaketen zur Analyse und Entwicklung der technischen Rahmenarchitektur, der Marktarchitektur und den rechtlichen Rahmenbedingungen einem konsolidierten Review unterzogen und in strukturierte Anforderungen überführt. Die Erarbeitung der Ergebnisse in den drei betrachteten Teilbereichen wurde durch die Partner über die Projektlaufzeit kontinuierlich weiterentwickelt und präzisiert. Die Identifikation und Spezifikation der Anforderungen und die Ausgestaltung der Lastenheftstruktur erfolgte daher iterativ in den einzelnen Projektphasen. Somit konnte im Hinblick auf die Anforderungsidentifikation eine kontinuierliche Evaluation der Forschungsergebnisse und eine Ableitung von Fragestellungen für die weitere Analyse und Konzeption erfolgen.

Als Basis für die Strukturierung und Ausgestaltung der Lastenheftinhalte wurden mögliche Zielsetzungen der Datenbank identifiziert und evaluiert. Als Ergebnis der Evaluation wurde festgelegt, dass mit der kooperativen Datenbank eine Datenbasis geschaffen werden soll, welche eine möglichst breite Datenbasis zur Entwicklung, Erprobung, Einführung und zum Betrieb von Funktionen für automatisierte und autonome Fahrzeuge liefern kann. Um die Datenbank möglichst nachhaltig nutzbar zu gestalten, sollte der mögliche Anwendungsbereich der

Datenbank unabhängig von definierten Fahrzeugfunktionen und Fahrzeugtechnologien ausgestaltet werden.

Funktionen und Technologien für automatisierte Fahrzeuge stellen einen maßgeblichen Innovationssektor zukünftiger Mobilität dar. Eine Beschränkung des Datenbankkonzepts auf aktuelle Entwicklungen und Trends könnte einer langfristigen Nutzbarkeit entgegenstehen.

Maßgeblicher Erfolgsfaktor für die Etablierung und den Betrieb einer kooperativen Forschungsdatenbank ist zudem die Schaffung einer breiten Nutzergruppe. Diese muss einerseits ein starkes Eigeninteresse an der kontinuierlichen Datennutzung aufweisen und andererseits den Aufbau einer hinreichenden Datenbasis und die kontinuierliche Weiterentwicklung auf Grundlage des technologischen Fortschritts und die veränderlichen Marktbedürfnisse sicherstellen können. Grundlegende Basis der Lastenheftgestaltung war die Entscheidung, dass die Datenbank keine Abbildung einer verpflichtenden oder vollständigen Menge von Fahrszenarien oder Szenarioparametern darstellen soll, welche für eine sicherheitstechnische Bewertung oder eine Fahrzeughomologation zwingend zu berücksichtigen sind. Jedoch kann und sollte die Datenbank eine mögliche Datenquelle darstellen, welche in der Konzeption von Entwicklungsmaßnahmen (z.B. Anreicherung von Trainingssets) oder der Ausgestaltung von Validierungsszenarien Anwendung finden und somit eigene Datenbasen von Nutzern sinnvoll anreichern können.

Auf Basis der entwickelten Konzepte zu den technischen, rechtlichen und marktspezifischen Rahmenbedingungen erfolgte die Herleitung von Anforderungen an die Datenbank anhand der identifizierten öffentlichen und gewerblichen Nutzergruppen sowie deren Anwendungsfälle und rollenabhängige Bedürfnisse an Datengrundlagen, Datenzugängen und Datenbankfunktionen.

Durch die Betrachtung der unterschiedlichen Nutzerinteressen und den spezifischen Anwenderszenarien ergeben sich insbesondere Anforderungen an Inhalte, Struktur und Organisation der Daten und an die Anwenderschnittstellen, die in der Rahmenarchitektur berücksichtigt werden müssen. Dabei werden neben den eigentlichen Szenariodaten auch nutzerspezifische Anforderungen an zusätzliche Metadaten erforderlich. Vor dem Hintergrund der betrachteten Use Case Varianten mit internen und externen Datenlieferanten ergaben sich konkrete Anforderungen an die Datengüte sowie an die Aufbereitung, Veredelung, Validitätsprüfung und Einspeisung von Daten.

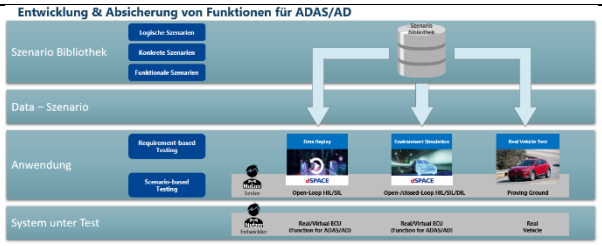
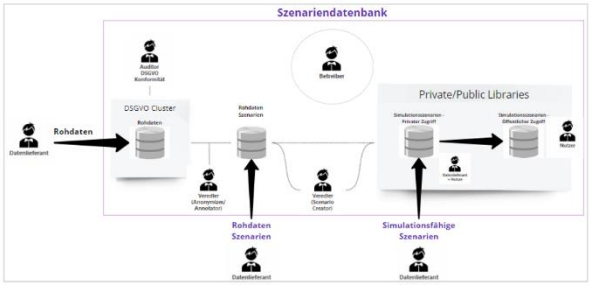
Im 2. Stakeholder-Workshop wurde die gewählte Strategie und die Zielsetzung zur Ableitung von Lastenheft-Anforderungen vorgestellt und mit den Teilnehmern diskutiert. Im Ergebnis konnte das gewählte Vorgehen bestätigt und zudem weitere Erkenntnisse zur notwendigen Unterscheidung der Datennutzung durch verschiedene Nutzergruppen und der notwendigen Unterscheidung der benötigten Metadaten identifiziert werden. In den weiteren Arbeitsschritten wurden zu den drei behandelten Teilgebieten mehrere Workshops mit den Projektpartnern durchgeführt, in denen die Anforderungen in einem strukturierten Vorgehen identifiziert, diskutiert und in einer Anforderungsliste dokumentiert wurden. Die Erkenntnisse aus den Workshops konnten zur und weiteren Ausgestaltung und Finalisierung der Forschungsergebnisse im vorliegenden Schlussbericht herangezogen werden.

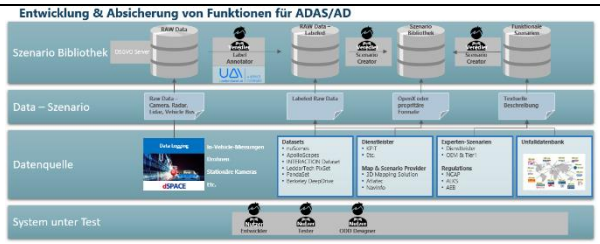
Im weiteren Arbeitsschritt wurde auf Basis der erstellten Anforderungsliste und der im Schlussbericht dokumentierten Ergebnisse die Anforderungsspezifikation erarbeitet und in die gewählte Lastenheftstruktur überführt. Zur Evaluation der Lastenheftinhalte wurden die beschriebenen Anforderungen anhand eines ausgewählten und für die betrachtete Nutzergruppe repräsentativen Anwendungsfalls betrachtet.

3 Struktur des Lastenheft

Der in Abschnitt 4 dokumentierte Anforderungskatalog gliedert sich in die nachfolgend dargestellten fünf Anwendungsfälle. Der Anforderungsspezifikation ist dabei eine eindeutige Nummer und Bezeichnung sowie die relevante Stakeholder-Gruppe zugeordnet. In Bezug auf die Stakeholder-Gruppen sei auf die Stakeholder- und Rollendefinitionen im Schlussbericht verwiesen.

Die zu entwickelnde kollaborative Szenario-Datenbank soll die Anwendungsfälle in der folgenden Tabelle abdecken. Zu jedem der dargestellten Anwendungsfälle werden in einem separaten Kapiteln die notwendigen Anforderungen dargestellt. Neben den zu unterstützenden Anwendungsfällen wird noch die Rahmenarchitektur vorangestellt.

Anwendungsfall	**Beschreibung**
AF1: Szenarien im Entwicklungs- und Absicherungsprozess	 Im Entwicklungs- und Absicherungsprozess von ADAS/AD werden Szenarien unterschiedlicher Art benötigt, um Data Replay, Hardware-in-the-Loop Simulationen, Software-in-the-Loop Simulationen und reale Testfahrten zu unterstützen. In diesem Abschnitt werden Anforderungen zur Nutzung der Szenarien im Hinblick auf die Datenhaltung dargelegt.
AF2: Einspeisen von Szenarien in die Datenbank (ggf. Veredelung)	 Die Szenario-Datenbank muss Mechanismen unterstützen, die es erlauben, unterschiedliche Szenarien oder Formate einzuspeisen und muss gemäß rechtlicher Rahmenbedingungen aber auch infrastruktureller Implikationen diesen Anforderungen genügen. Dieser Abschnitt beschreibt diese Anforderungen.

AF3: Anbindung weiterer Datenquellen	 Da schon im Markt Data-Sets aber auch Szenario-Bibliotheken existieren, und die Datendiversität bei der Entwicklung und Absicherung von ADAS/AD wichtig ist, soll die Datenbank es ermöglichen, die schon existierenden Daten auch nutzbar zu machen. Dabei beschreibt dieser Abschnitt die notwendigen Anforderungen, um andere Datenquellen anbinden zu können, die dadurch eine hohe Diversität und somit einen hohen Nutzen gewährleisten.
AF4: Effiziente Nutzung durch hochwertige Mechanismen zum finden passender Szenarien	Ein wichtiger Aspekt einer Datenbank ist es, die Daten zu strukturieren aber auch einfach gemäß des zu betrachtenden Anwendungsfalls finden zu können. Dabei beschreibt dieses Kapitel neben den Anforderungen der Suchmechanismen auch die Anforderungen an die notwendigen Meta-Daten.
AF5: Abrechnungs- und Zugriffsmodell	Um die Mitgliedsbeitragfinanzierung und die Anwender abhängigen Berechtigungen insbesondere Zugriffsrechte zu verwalten, benötigt die Datenbank entsprechende Mechanismen.

4 Anforderungen

4.1 Technische Rahmenarchitektur

Anforderungsnummer	**Stakeholder**
RA_01	Betreiber

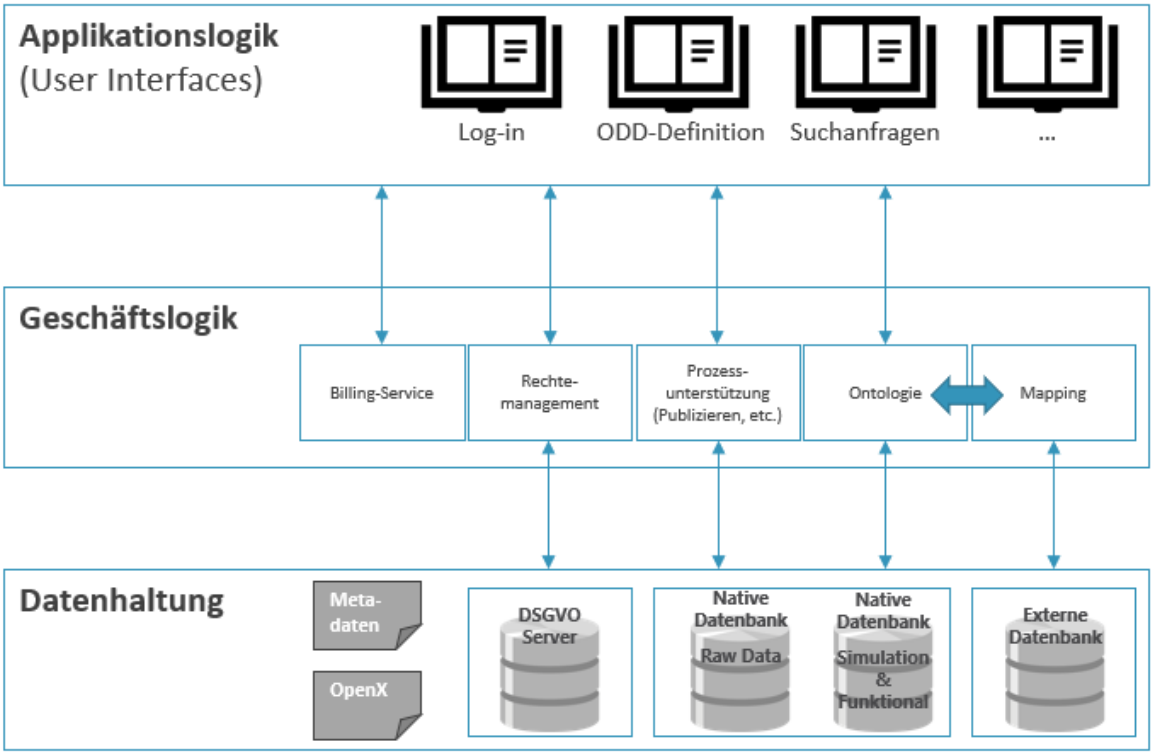
Anforderungsbezeichnung

Grundlegende Architektur

Anforderungsbeschreibung

Die Architektur besteht im Wesentlichen aus den folgenden 3 Software-Schichten:

- Applikationslogik: Dies sind die User Interfaces, um sich zu registrieren, einzuloggen, Suchanfragen zu stellen, die ODD zu definieren oder auch Daten hochzuladen.
- Geschäftslogik: Dies sind die Module für den Billing-Service, das Rechte- und Nutzer-Management, Prozessunterstützende Module (z.B. Anlegen und Management eigener Szenario-Kataloge und ODDs, hochladen von Daten oder auch eigenes Tagging) und auch die Ontologie sowie das Mapping-Modul zum Anbinden weiterer Datenquellen.
- Datenhaltung: Neben den Metadaten mit einem kontrollierten Vokabular sind hier die unterschiedlichen Datentöpfe verortet, um z.B. auch rechtlich sensible zu schützen.



Anforderungsnummer	**Stakeholder**
RA_02	Betreiber
Anforderungsbezeichnung	
Anwenderschnittelle und Anwenderdialog	
Anforderungsbeschreibung	
Für alle Anwenderfunktionen innerhalb der Datenbank soll eine geeignete graphische Anwenderschnittstellen und ein organisierter Anwenderdialog implementiert werden. Die Implementierung eines rollenspezifischen Dashboards zur Darstellung der Anwenderspezifischen Rechte und Funktionen wird empfohlen. Es sind folgende Dialoge zu implementieren: • Login & Registration • ODD Definition & Management • Szenario-Details (Preview & Metadaten) • Account Information (Name, Firma, etc.) • Abrechnung – Darstellung, der Zugriffsrechte auf die dedizierten Daten • Dashboards (Anzahl der Szenarien bezogen auf die Fahrfunktion, Anzahl der Szenarien bezogen auf die unterschiedlichen Datasets oder angebundenen Bibliotheken, Anzahl der Szenarien, bezogen auf den Szenariotypen (Logische, Konkrete, Abstrakte und Funktionale Szenarien), genutzter Speicher, etc.)	

Anforderungsnummer	**Stakeholder**
RA_03	Betreiber
Anforderungsbezeichnung	
Effiziente Ressourcennutzung zur Realisierung der Datenbank	
Anforderungsbeschreibung	
Um den benötigten Ressourcenbedarf der Datenbank möglichst gering zu halten, soll das Datenbankkonzept hinsichtlich nachfolgend genannter Parameter auf Effizienz ausgelegt werden. • Datenspeicherung • Datenübertragung • Energieverbrauch	

Anforderungsnummer	**Stakeholder**
RA_04	Betreiber
Anforderungsbezeichnung	

Wartbarkeit und Erweiterbarkeit
Anforderungsbeschreibung Das Datenbankkonzept soll auf für eine kontinuierliche Wartbarkeit und Erweiterbarkeit ausgelegt werden. Dabei sollen mindestens Möglichkeiten zur Anpassung und Erweiterbarkeit der folgenden Funktionen berücksichtigt werden: • Taxonomie und Ontologie • Anwenderfunktionen und Benutzerschnittstellen • Anbindung an experte Datenquellen • Exportfunktionen • Mitgliedsfinanzierungsmodell • Rollen- und Rechtemodell

Anforderungsnummer	**Stakeholder**
RA_05	Betreiber
Anforderungsbezeichnung Datenbank in den Wartungsmodus versetzen	
Anforderungsbeschreibung Dem Betreiber soll es ermöglicht werden, die Datenbank für Wartungsarbeiten in einen Wartungsmodus zu versetzen. Im Wartungsmodus soll der Anwender beim Aufrufen der Datenbank eine entsprechende Meldung erhalten. Größere Wartungsarbeiten sollen möglichst in weniger frequentieren Zugriffszeiten durchgeführt werden.	

4.2 Anwendungsfall 1: Szenarien im Entwicklungs- und Absicherungsprozess

Anforderungsnummer	**Stakeholder**
AF1_01	Betreiber
Anforderungsbezeichnung Kontrolliertes Vokabular und Metadaten.	
Anforderungsbeschreibung	

Zur Organisation der Szenariodaten soll eine Metadatenstruktur definiert werden. Mithilfe der Taxonomie (kontrolliertes Vokabular) sollen die Informationen und Parameter der Szenariobeschreibung klassifiziert werden.

Die Metadaten sollen mindestens nachfolgend dargestellte Kriterien für Rohdaten, Simulationsdaten und Labeldaten berücksichtigen:

- Name des Szenarios
- Angaben zum Datenlieferant und zur Datenbasis
- Datums- und Ortsangaben zum Szenario
- Funktionale Beschreibung des Szenarios und Zuordnung von Schlagworten
- Anwendungszwecke des Szenarios
- Beschreibung der enthaltenen situativen Ereignisse und Fahrmanöver
- Arten der Szenariodaten (z.B. Kamera-, Lidar-, Radar-, V2X-, Mess-, Simulationsdaten, Labeldaten)
- Datenquelle der Szenariodaten (z.B. Fahrzeugkamera, Road Side Unit, Messequipment, Prüf- oder Simulationswerkzeug, Expertenwissen)
- Qualitätseigenschaften der Szenariodaten (z.B. zeitliche und räumliche Auflösung der Szenariodaten, Genauigkeit und Bandbreite der gelabelten Parameter, Menge und Umfang der abgedeckten situativen Ereignisse und Umgebungsparameter, anonymisierte personenbezogene Daten)
- Dateinamen, Dateibeschreibungen und Dateiformate der Szenariodaten
- Änderungshistorie
- Status des Szenarios (z.B. angeliefert, veredelt, auditiert, zur Anwendung freigegeben)

Ein Teil der Metadaten stellt die Operational Design Domain dar, die mit Hilfe eines oder mehrerer Standards (idealerweise OpenODD, BSI PAS 1883 und NHTSA) implementiert werden soll und stellt einen wichtigen Aspekt des kontrollierten Vokabulars dar.

Um Szenarien kollaborative nutzen zu können, sind gängige Standards zu unterstützen. Entsprechend sollen die OpenX Standards verwendet werden und somit musss ein Simulations-Szenario mindestens aus einer OpenDrive und OpenSecanrio Datei bestehen. Zusätzlich kann auch ein OpenCRG File hinterlegt werden. Für Rohdaten-Szenarien sollten diese mit einer Datei gemäß OpenLabel hinterlegt sein. Weiter soll es möglich sein, auch andere Dateiformate hochzuladen und zu nutzen.

Anforderungsnummer	**Stakeholder**
AF1_02	Betreiber
Anforderungsbezeichnung	
Organisation und Speicherung von Szenariodaten in der Datenbank	
Anforderungsbeschreibung	
Die Szenariodaten sollen in der Datenbank organisiert werden. Die Organisation von Szenariodaten erfolgt über definierte Metadaten (vgl. AF_01).	

Sofern die Szenarien durch extern gespeicherte Daten angereichert werden, soll eine Verknüpfung (vgl. AF3_01) zu den Datenquellen und den spezifischen Inhalten erfolgen.

Anforderungsnummer	**Stakeholder**
AF1_03	Betreiber, Veredler, Auditor
Anforderungsbezeichnung	
Metadaten zu anonymisierten, personenbezogenen Daten	
Anforderungsbeschreibung	
In den Metadaten sollen Informationen zur Anonymisierung der Rohdaten hinterlegt werden. Dabei soll die Möglichkeit bestehen, den Qualitätseigenschaften der Szenariobeschreibungen Informationen zu den anonymisierten Elementen der Rohdaten (z.B. Verpixeln von Gesichtern oder Kennzeichen) hinzuzufügen.	

4.3 Anwendungsfall 2: Einspeisen von Szenarien in die Datenbank (ggf. Veredelung)

Anforderungsnummer	**Stakeholder**
AF2_01	Datenlieferant
Anforderungsbezeichnung	
Lieferung von Szenariodaten	
Anforderungsbeschreibung	
Dem Datenlieferant soll es ermöglicht werden, Szenariodaten in einen gesonderten nicht öffentlich zugänglichen Bereich der Datenbank einzustellen und bei Annahme dieser durch den Betreiber, für die Lieferung eine Monetarisierung oder Gewährung von weiterem Zusatznutzen gemäß der Nutzerrolle zu erhalten.	

Anforderungsnummer	**Stakeholder**
AF2_02	Datenlieferant
Anforderungsbezeichnung	
Externe Anonymisierung der gelieferten Szenariodaten	
Anforderungsbeschreibung	

Dem Datenlieferanten soll die Lieferung eigenständig anonymisierter Szenariodaten ermöglicht werden. Hierzu sollen dem Datenlieferanten die Bedingungen zur Anonymisierung zugänglich gemacht werden. Zudem soll der Lieferant von System aufgefordert werden, die umgesetzte Anonymisierung in den Metadaten des Szenarios zu dokumentieren.

Anforderungsnummer	**Stakeholder**
AF2_03	Betreiber
Anforderungsbezeichnung	
Uploadmanager für das Einspeisen von Szenarien	
Anforderungsbeschreibung	
Die Datenbank soll einen Uploadmanager für das Hochladen der einzuspeisenden Szenarien bereitstellen. Dieser soll folgende Funktionen/Features beinhalten: • Erstellung einer Up-Liste zur Priorisierung • Planung der Uploadzeiten • Festlegung der genutzten Bandbreite • Unterbrechung von laufenden Uploads • Fortsetzung von unterbrochenen Uploads • Löschung der Uploadliste	

Anforderungsnummer	**Stakeholder**
AF2_04	Betreiber, Veredler, Auditor
Anforderungsbezeichnung	
Prüfung und Bewertung von gelieferten Szenariodaten	
Anforderungsbeschreibung	
Neu angelieferte oder überarbeitete Szenariodaten sollen dem Betreiber automatisiert angezeigt werden. Dieser kann die Daten zur Prüfung, Bewertung und Veredelung an den Veredler oder zur Auditierung an den Auditor übergeben. Der Betreiber soll die Lieferung von Daten annehmen oder ablehnen können.	

Anforderungsnummer	**Stakeholder**
AF2_05	Veredler
Anforderungsbezeichnung	
Veredelung der gelieferten Szenariodaten	

Anforderungsbeschreibung
Dem Veredler soll es ermöglicht werden, Szenariodaten angenommener Lieferungen jederzeit zu bearbeiten. Dabei soll die Möglichkeit bestehen, die eingestellten Datensätze zu modifizieren oder anzureichern. Nachfolgende Anwendungsfälle der Szenariobearbeitung sollen dabei mindestens abgedeckt werden: • DSGVO-konforme Anonymisierung von gespeicherten Szenariodaten • Herstellung Konformität von Szenariodaten mit der Taxonomie und Ontologie gemäß AF1_01 • Anreicherung von Szenariodaten gemäß Parametern der Taxonomie und Ontologie gemäß AF1_01 Den einzelnen Szenariodaten sollen zusätzlicher Metadaten zur Änderungshistorie hinzugefügt werden. Diese soll eine Beschreibung der erfolgten Modifikationen und Veredelungen von Szenarien enthalten. Der Veredler soll nach Änderung von Daten zur Eingabe einer Beschreibung aufgefordert werden.

Anforderungsnummer	**Stakeholder**
AF2_06	Auditor
Anforderungsbezeichnung	
Auditierung der veredelten Daten	
Anforderungsbeschreibung	
Nach Veredelung von Abschluss Szenariodaten soll der Auditor automatisch vom System informiert werden. Der Auditor kann die Daten dann hinsichtlich der DSGVO Konformität überprüfen. Dem Auditor soll zur Überprüfung Einsicht in die vollständigen Datensätze, inklusive der Änderungshistorie gewährt werden. Positiv überprüfte Szenarien sollen zur Anwendung freigegeben werden und anschließend in dem Nutzerbereich zur Verfügung gestellt werden. Negativ geprüfte Szenarien sollen zur erneuten Bearbeitung an den Veredeler zurückgegeben werden können.	

Anforderungsnummer	**Stakeholder**
AF2_07	Betreiber, Auditor
Anforderungsbezeichnung	
Informationssicheres Datenbankkonzept	
Anforderungsbeschreibung	
Die Datenbank soll gegen unautorisierten Zugriff und Datenverlust abgesichert sein. Die allgemeinen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sind dabei umzusetzen und ein fortlaufendes IT-Sicherheitsmanagement soll betrieben werden.	

Die Datenbank soll mindestens die nachfolgend genannten Mechanismen berücksichtigen:

- Zugriffsprotokoll: Die Zugriffe auf die Datenbank sollen protokoliert und für eine spätere Auswertung gespeichert werden.
- Datenbackup: Die gespeicherten Daten sollen gegen Verlust gesichert sein. Dies kann über eine automatische Backup Funktion gesehen.
- Multilogin soll verhindert werden: Es sollen keine mehrfachen Anmeldungen mit den gleichen Anwender-Daten ermöglicht werden.
- Abmelden inaktiver Nutzer: Bei einer Inaktivität eines Nutzers soll eine automatische Abmeldung erfolgen.

Es wird empfohlen die Informationssicherheit der Datenbank regelmäßig zu auditieren.

Anforderungsnummer	**Stakeholder**
AF2_10	Betreiber, Auditor
Anforderungsbezeichnung	
DSGVO-konformes Datenbankkonzept	
Anforderungsbeschreibung	
Das Datenbankkonzept soll DSGVO-konform ausgestaltet und umgesetzt werden. Die gespeicherten Daten, sowie die verwendete Infrastruktur sollen den geltenden Datenschutzanforderungen genügen. Die kontinuierliche Einhaltung von DSGVO-Anforderungen soll sichergestellt werden. Hierzu soll eine regelmäßige Auditierung der DSGVO Konformität und Überprüfungen der IT-Sicherheit erfolgen.	

Anforderungsnummer	**Stakeholder**
AF2_11	Betreiber, Veredler, Auditor
Anforderungsbezeichnung	
Absicherung nicht anonymisierter, personenbezogener Daten	
Anforderungsbeschreibung	
Die Speicherung personenbezogener Daten soll nach Möglichkeit vermieden werden. Soll eine Speicherung bestimmter Daten erforderlich sein, sollen diese gegen unautorisierten Zugriff abgesichert werden. Sofern nicht anonymisierte, personenbezogene Informationen in den Szenariodaten hinterlegt werden, soll zusätzlich zu den in AF1_01 dargestellten Attributen zusätzliche Metadaten mit folgendem Inhalt abgelegt werden: • Rechtsgrundlage der Erhebung	

- Rechtsgrundlage des Forschungszwecks (insbesondere Fragestellung, Verantwortlichkeiten, herangezogene Datenarten, ggf. Abwägungsgründe, Methodik, Gemeinschaftsnutzen und die Veröffentlichung der wesentlichen Ergebnisse)
- Rechtfertigungstatbestände (z.B. Einwilligung der betroffenen Personen, Nutzung anlassbezogener Daten zu Forschungszwecken, Interessenabwägung)
- Angaben zum Gemeinschaftsnutzen
- Ablaufdatum
- Schutzmaßnahmen

Bei Erreichen des Ablaufdatums für nicht anonymisierte Rohdaten soll der Betreiber über die Datenbank automatisch informiert werden, sodass eine Verlängerung des Ablaufdatums oder eine Löschung der Daten umgesetzt werden kann.

Anforderungsnummer	**Stakeholder**
AF2_12	Betreiber
Anforderungsbezeichnung	
Verschlüsselung von personenbezogenen Daten	
Anforderungsbeschreibung	
Bestimmte personenbezogene, insbesondere Anwender-spezifische Daten (z.B. Bankinformation und Passwörter) sollen nur verschlüsselt in der Datenbank hinterlegt werden.	

Anforderungsnummer	**Stakeholder**
AF2_13	Betreiber
Anforderungsbezeichnung	
Löschung personenbezogener Daten	
Anforderungsbeschreibung	
Die Löschung von personenbezogene Daten auf Wunsch des zu Rechteinhabers soll ermöglicht werden. Sind personenbezogene Daten für einen bestimmten Zweck erhoben wurden und ist dieser Zweck erfüllt worden, ist eine Löschung der Daten umzusetzen. Die Daten sollen so in der Datenbank gespeichert werden, dass ein Löschen der Daten jederzeit möglich ist und dieses nicht die Integrität der Datenbank verletzt.	

Anforderungsnummer	**Stakeholder**
AF2_14	Betreiber, Veredler

Anforderungsbezeichnung
Löschen von Szenariodaten in der Datenbank
Anforderungsbeschreibung
Dem Betreiber und Veredler soll es ermöglicht werden, gespeicherte Szenariodaten und einzelne Datensätze zu löschen. Gelöschte Szenariodaten sollen für eine definierte Zeit aufbewahrt werden, jedoch nicht mehr für Nutzer abrufbar sein.

Anforderungsnummer	**Stakeholder**
AF2_15	Nutzer
Anforderungsbezeichnung	
Privater Bereich zum organisieren eigener Szenarien	
Anforderungsbeschreibung	
Dem Nutzer soll die Möglichkeit gegeben werden, in einem nur für ihn sichtbaren Bereich eigene Szenario-Kataloge anzufertigen, mit eigenen Szenarien zu füllen und auch mit eigenen Tags versehen. Weiter soll der Nutzer dort die Möglichkeit haben das kontrollierte Vokabular der Datenbank zu verwenden, um dann auch in seinen Daten mit den gleichen Suchmechanismen wie in der Datenbank zu arbeiten.	

4.4 Anforderungsfall 3: Anbindung weiterer Datenquellen

Anforderungsnummer	**Stakeholder**
AF3_01	Betreiber
Anforderungsbezeichnung	
Anbindung externer Datenquellen	
Anforderungsbeschreibung	
Die Datenbank soll eine Schnittstelle zur Anbindung anderer Datenquellen bereitstellen. Hierdurch soll eine Verknüpfung zur Anreicherung von Szenarien mit Daten und Informationen aus externen Datenquellen ermöglicht werden. Diese Schnittstellen oder Mapping-Schicht ist zwischen der Ontologie und der externen Datenquelle zu verorten.	

Anforderungsnummer	**Stakeholder**
AF3_02	Betreiber

Anforderungsbezeichnung
Ontologie der Szenariendatenbanken
Anforderungsbeschreibung
Zur Suche in der nativen Datenbank aber auch in externen Datenquellen soll ein ontologischer Ansatz implementiert werden, der es ermöglicht aus den gestellten Suchanfragen weitere Schüsse zu ziehen und somit weitere Szenarien für die Suchanfrage zu identifizieren. Als Teil der Ontologie für diese kollaborative Szenario-Datenbank ist ASAM OpenXOntology zu integrieren. Die Datenbank soll die Anbindung von Datasets oder Szenariendatenbanken über einen ontologischen (z.B. ASAM OpenXOntology) Ansatz ermöglichen.

4.5 Anforderungsfall 4: Effiziente Nutzung durch hochwertige Mechanismen zum finden passender Szenarien

Anforderungsnummer	**Stakeholder**
AF4_01	Nutzer
Anforderungsbezeichnung	
Suchen und Filtern von Szenarien	
Anforderungsbeschreibung	
Um die Suche nach geeigneten Szenarios zu ermöglichen, soll den Anwendern der Datenbank ermöglicht werden, Anwender-spezifische Suchanfragen zu definieren. Diese sollen die in AF1_01 beschriebenen Taxonomie- und Ontologie-Parameter abdecken. Die Definition von Suchanfragen soll anhand von graphischen und tabellarischen Benutzeroberflächen ermöglicht werden. Dem Anwender soll zudem ermöglicht werden, definierte Suchanfragen in seinem Anwenderprofil mittels einer Dashboard-Funktion zu verwalten. Die Verwaltung von Suchanfragen sollen Funktionen zur Speicherung, Anzeige, Modifizierung, Löschung beinhalten. Zur Visualisierung von Suchergebnissen soll eine Ergebnisdarstellung erzeugt werden. Dabei soll eine Sortierung, bzw. Filterung nach einzelnen Suchkriterien ermöglicht werden. Zudem soll die Möglichkeit bestehen, die Suchergebnisse auf eine vollständige oder teilweise Entsprechung der eingegebenen Suchparameter anzupassen.	

Anforderungsnummer	**Stakeholder**
AF4_02	Nutzer

Anforderungsbezeichnung
Abrufen von ausgewählten Szenariodaten
Anforderungsbeschreibung
Dem Nutzer soll es ermöglicht werden, aus den Ergebnissen von Suchanfragen ausgewählte Szenariodaten abzurufen. Der Zugriff auf die angeforderten Daten soll den Nutzerstatus berücksichtigen und entsprechend des gebuchte Paketierungs-Modell oder der Möglichkeit „Pay per Dataset“ ermöglicht werden. Zum Abruf von ausgewählten Szenarien soll dem Nutzer eine Exportfunktion und ein konfigurierbarer Downloadmanager gemäß AF4_04 zur Verfügung stehen.

Anforderungsnummer	**Stakeholder**
AF4_03	Betreiber
Anforderungsbezeichnung	
Detailansicht einzelner Szenarien	
Anforderungsbeschreibung	
Die Datenbank soll eine detaillierte Ansicht einzelner Szenarien ermöglichen. Die Detailansicht soll die Metadaten der Szenarien in einer übersichtlichen Form darstellen. Für ausführbare Szenarien soll eine Preview angezeigt werden.	

Anforderungsnummer	**Stakeholder**
AF4_04	Betreiber
Anforderungsbezeichnung	
Downloadmanager für den Abruf von Szenariodaten	
Anforderungsbeschreibung	
Die Datenbank soll einen Downloadmanager für das Herunterladen der ausgewählten Szenarien bereitstellen. Dieser soll folgende Funktionen implementieren: • Erstellung einer Download-Liste zur Priorisierung • Planung der Downloadzeiten • Festlegung der genutzten Bandbreite • Unterbrechung von laufenden Downloads • Fortsetzung von unterbrochenen Downloads • Löschung der Downloadliste	

Anforderungsnummer	**Stakeholder**
AF4_05	Nutzer
Anforderungsbezeichnung	
Datenpipline für Rohdaten Upload	
Anforderungsbeschreibung	
Die Datenbank soll eine ausreichend ausgelegte Datenpipline zu Übertragung vieler und großer Rohdaten implementieren.	

Anforderungsnummer	**Stakeholder**
AF4_06	Nutzer
Anforderungsbezeichnung	
Definition der eigenen ODD	
Anforderungsbeschreibung	
Dem Nutzer soll es ermöglicht werden, seine eigene ODD anhand des kontrollierten Vokabulars basierend auf der Metadatenstruktur zu definieren und damit die Datenbank zu durchsuchen.	

Anforderungsnummer	**Stakeholder**
AF4_07	Nutzer
Anforderungsbezeichnung	
ODD Management	
Anforderungsbeschreibung	
Es soll für den Nutzer möglich sein, mehrere ODDs zu definieren und diese strukturiert ablegen zu können. Auch eine Kombination mehrerer ODDs soll durch entsprechende Suchanfragenverknüpfungen möglich sein.	

4.6 Anforderungsfall 5: Abrechnungs- und Zugriffsmodell

Anforderungsnummer	**Stakeholder**

AF5_01	Betreiber

Anforderungsbezeichnung

Mitgliedsbeitragfinanzierung für die Datenbanknutzung

Anforderungsbeschreibung

Die Datenbank soll ein Modell zur Mitgliedsbeitragfinanzierung implementieren. Es wird empfohlen, bei diesem Modell zwischen den Varianten zum Abrufen einzelner Szenarien mittels einer „Pay per Dataset“ Möglichkeit und einer Möglichkeit zur „Paketierung“ unterschieden werden. Bei der Paketierung soll gegebenenfalls zwischen verschiedenen Anwenderrollen (z.B. reiner Datennutzer oder zusätzlich Datenlieferant) und Stakeholdern (z.B. Nutzung im öffentlichen oder gewerblichen Interesse) unterschieden werden.

Weiterhin wird empfohlen, eine Gewährung von Gutschriften im Gegenzug für die Lieferung oder Veredelung von Daten in Betracht zu ziehen.

Optional kann auch ein Modell mit konstanter Mitgliedfinanzierung in Betracht gezogen werden.

Interessenten soll zudem ein Testzugang zur Datenbank ermöglicht werden. Dieser soll einen beschränkten Zugriff auf die Szenariodaten ermöglichen, bei dem zwar die Suchfunktion der Datenbank zur Verfügung steht, die gefundenen Szenariodaten jedoch nicht abrufbar und exportierbar sind.

Anforderungsnummer	**Stakeholder**
AF5_02	Betreiber

Anforderungsbezeichnung

Anwender- und Rechtemanagement

Anforderungsbeschreibung

Die Datenbank soll Funktionen zum Anwender- und Rechtemanagement implementieren.

Hierbei sollen Rollen–spezifische Zugriffsrechte auf Datenbankfunktionen und die gespeicherten Szenariodaten berücksichtigt werden. Es soll möglich sein, den Anwenderstatus (z.B. gesperrter, eingeschränkter, voller Zugriff) zu verwalten.

Es soll weiterhin die Möglichkeit bereitgestellt werden, Nutzer-spezifische Berechtigungen anhand des gewählten Bezahlmodells zu verwalten.

Im Anwendermangement soll hinterlegt werden, ob ein Anwender die aktuellen allgemeinen Geschäfts- und Nutzungsbedingungen akzeptiert hat.

Anforderungsnummer	**Stakeholder**
AF5_03	Betreiber

Anforderungsbezeichnung
Anlegen neuer Anwender
Anforderungsbeschreibung
Dem Betreiber soll es ermöglicht werden, neue Anwender in der Datenbank anzulegen. Bei der Anlage sollen mindestens nachfolgend genannte Parameter berücksichtigt werden: • Eindeutige Anwenderkennung • Name, Vorname • Eindeutige Mailadresse • Passwort • Firmen-/Organisationsdaten • Kontakt- und Adressdaten • Anwenderrolle und rollen-abhängige Zugriffsrechte auf Daten und Funktionen • Nur bei Nutzer notwendig: Auswählen des gewünschten Bezahlmodells („Pay per Dataset“, „Paketierungs-Modell“ oder Testzugang)

Anforderungsnummer	**Stakeholder**
AF5_04	Betreiber
Anforderungsbezeichnung	
Administratives Bearbeiten von Anwenderdaten	
Anforderungsbeschreibung	
Dem Betreiber soll es ermöglicht werden, die gespeicherten Anwenderdaten nach dem Anlegen zu bearbeiten.	

Anforderungsnummer	**Stakeholder**
AF5_05	Betreiber
Anforderungsbezeichnung	
Deaktivieren von Datenbankanwendern	
Anforderungsbeschreibung	
Dem Betreiber soll es ermöglicht werden, Anwender der Datenbank nach dem Anlegen zu deaktivieren. Ein deaktivierter Anwender soll der Zugriff auf die Szenariodaten eingeschränkt werden. Das Anwender-Profil mit individuellen Einstellungen und den definierten Suchfiltern soll für eine mögliche Reaktivierung erhalten bleiben.	

Anforderungsnummer	**Stakeholder**
AF5_06	Betreiber
Anforderungsbezeichnung	
Reaktiveren von Datenbankanwendern	
Anforderungsbeschreibung	
Dem Betreiber soll es ermöglicht werden, deaktivierte Datenbankanwender zu reaktiveren.	

Anforderungsnummer	**Stakeholder**
AF5_07	Betreiber
Anforderungsbezeichnung	
Löschen von Datenbanknutzern	
Anforderungsbeschreibung	
Dem Betreiber soll es ermöglicht werden, angelegte Datenbankanwender zu löschen. Gelöschte Nutzer soll der Zugriff auf die Datenbank entzogen werden. Weiterhin sollen personenbezogene Daten des Anwenders gelöscht werden.	

Anforderungsnummer	**Stakeholder**
AF5_08	Nutzer, Datenlieferant
Anforderungsbezeichnung	
Als neuer Nutzer oder Datenlieferant registrieren	
Anforderungsbeschreibung	
Einem Nutzer oder Datenlieferant soll es ermöglicht werden, sich für den Zugriff auf die Datenbank zu registrieren. Bei der Anwenderregistrierung sollen mindestens die Parameter aus AF5_03 berücksichtigt werden. Beim ersten Anmelden an die Datenbank soll der Nutzer oder Datenlieferant die allgemeinen Geschäfts- und Nutzungsbedingungen einsehen können und zur Akzeptierung aufgefordert werden. Die Registrierung soll als privater und öffentlicher Nutzer mit Auswahl des gewünschten Bezahlmodells ermöglicht werden.	

Anforderungsnummer	**Stakeholder**

AF5_09	Nutzer, Datenlieferant, Veredeler, Auditor
Anforderungsbezeichnung Anwenderdaten bearbeiten	
Anforderungsbeschreibung Dem Anwender soll es ermöglicht werden, sein individuelles Anwenderprofil und die darin hinterlegten Daten einzusehen, zu ändern oder zu löschen. Ein Nutzer soll sein gewähltes Bezahlmodell ändern, pausieren oder stornieren können. Dem Anwender soll eine Beendigung als Datenbankanwender ermöglicht werden.	

Anforderungsnummer AF5_10	**Stakeholder** Betreiber
Anforderungsbezeichnung Anwendersupport	
Anforderungsbeschreibung Der Betreiber soll einen Anwendersupport betreiben. Dieser soll registrierten und potentiellen Anwendern eine Kontaktmöglichkeit und Ansprechpartner zur Beantwortung von Fragen und zur Problemlösung bereitstellen. Der Anwendersupport könnte über ein Kontaktformular, eine Mailadresse oder Telefonnummer realisiert werden.	