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

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

von

Alexander Klinge, Mathilde Krampitz
IKEM – Institut für Klimaschutz, Energie und Mobilität e.V., Berlin

Heiko Ehrich
TÜV NORD Mobilität GmbH & Co. KG, Institut für Fahrzeugtechnik und Mobilität, Essen

Björn Siemon
consulting4drive GmbH, Berlin

Christopher Wiegand
dSPACE digital signal processing and control engineering GmbH, Paderborn

unter Mitwirkung von:

Marcus Lassowski (consulting4drive GmbH)

Jann-Eve Stavesand (dSPACE digital signal processing and control engineering GmbH)

Andre Simon (TÜV NORD Mobilität GmbH & Co. KG)

Berichte der Bundesanstalt
für Straßenwesen
Fahrzeugtechnik Heft F 156

bast
Bundesanstalt für
Straßenwesen

Die Bundesanstalt für Straßenwesen veröffentlicht ihre Arbeits- und Forschungsergebnisse in der Schriftenreihe Berichte der Bundesanstalt für Straßenwesen. Die Reihe besteht aus folgenden Unterreihen:

A - Allgemeines
B - Brücken- und Ingenieurbau
F - Fahrzeugtechnik
M - Mensch und Sicherheit
S - Straßenbau
V - Verkehrstechnik

Es wird darauf hingewiesen, dass die unter dem Namen der Verfasser veröffentlichten Berichte nicht in jedem Fall die Ansicht des Herausgebers wiedergeben.

Die Hefte der Schriftenreihe Berichte der Bundesanstalt für Straßenwesen können direkt bei der Carl Ed. Schunemann KG, Zweite Schlachtpforte 7, D-28195 Bremen, Telefon: (04 21) 3 69 03 - 53, bezogen werden.

Seit 2015 stehen die Berichte der Bundesanstalt für Straßenwesen (BASt) als kostenfreier Download im elektronischen BASt-Archiv ELBA zur Verfügung.
https://bast.opus.hbz-nrw.de

Impressum

Bericht zum Forschungsprojekt 82.0719
Entwicklung eines Konzepts und Lastenheftes für eine ‚Szenariendatenbank' zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen

Fachbetreuung:
Claus Pastor

Referat:
Automatisiertes Fahren

Herausgeber:
Bundesanstalt für Straßenwesen
Brüderstraße 53, D-51427 Bergisch Gladbach
Telefon: (0 22 04) 43 - 0

Redaktion:
Stabsstelle Presse und Kommunikation

Gestaltungskonzept:
MedienMélange:Kommunikation

Druck und Verlag:
Fachverlag NW in der Carl Ed. Schünemann KG
Zweite Schlachtpforte 7, D-28195 Bremen
Telefon: (04 21) 3 69 03 - 53 | Telefax: (04 21) 3 69 03 - 48
www.schuenemann-verlag.de

ISSN 0943-9307 | ISBN 978-3-95606-793-8 | https://doi.org/10.60850/bericht-f156

Bergisch Gladbach, Oktober 2024

Kurzfassung - Abstract

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

Der vorliegende Bericht gibt einen Einblick in die verschiedenen Dimensionen der Konzeptionierung und Lastenheftentwicklung einer kooperativen Datenbank als Austausch- und Distributionsplattform für Simulationsszenarien zur Bewertung der Sicherheitswirkung autonomer Fahrfunktionen. Die Ausarbeitung gliedert sich in die Teilbereiche rechtswissenschaftlicher, wirtschaftswissenschaftlicher und technischer Rahmen- und Umsetzungsbedingungen einer nutzenmaximierenden Szenariendatenbank.

Hierfür wurden zunächst, im Wege einer Vorabanalyse der technischen Rahmenarchitektur, grundlegende Anforderungen bezüglich der Integration weiterer relevanter Datenbanken über eine Ontologie und Möglichkeiten der Standardisierung der Datenformate angeleitet.

Neben der Integration wurde die Modularisierung der unterschiedlichen Datenbanken/ Datasets untersucht, um eine möglichst hohe Testabdeckung und damit eine Sicherheitsaussage für eine Fahrfunktion erreichen zu können. Die Modularisierung in Bezug auf die einzuspeisenden Daten ist ein wichtiger Teilaspekt der Rahmenarchitektur, um zum einen zu gewährleisten, dass rechtliche Rahmenbedingungen adressiert werden und zum anderen, dass in der Umsetzung ein Höchstmaß an Flexibilität gegeben ist. Auch die Untersuchung unterschiedlicher Nutzerzugänge in Bezug auf Rechtemanagement und Suchanfragen in Bezug auf eine Operational Design Domain (ODD), aber auch hinsichtlich anderer nutzerspezifischer Anfragen stellt einen wichtigen Teil der Betrachtung dar. Durch eine aufbauende technische Validierung wurden verschiedene Aspekte hinsichtlich der Generierung und der damit verbunden Einspeisung von Szenarien sowie der Filterung abgelegter Szenarien untersucht, um abschließend explizite technische Umsetzungsempfehlungen abzuleiten.

Simultan konnten durch eine weitgreifende Marktanalyse die Schlüsselstakeholder einer kooperativen Szenariendatenbank identifiziert und jeweils nutzerspezifische Partizipationsanreize und -hürden abgeleitet werden. Anschließend wurden die Anreize im Zusammenhang mit den Hürden durch eine Stakeholderbefragung evaluiert und aufbauend durch Leitfadeninterviews in den Kontext zu bereits existierenden Szenariendatenbanken gesetzt. Aus den Ergebnissen wurden explizite Partizipationsanforderungen zur Rollenbesetzung im Betreibermodell für die jeweiligen Stakeholdergruppen abgeleitet und in Bezug eines erfolgsversprechenden Finanzierungsmodells ergänzt. Hierbei wurde berücksichtigt, welche Finanzierungsoptionen für die einzelnen Stakeholder von Relevanz sind und gleichzeitig eine Unterteilung in initiale Finanzierung und in Betriebsfinanzierung unternommen.

Die Analyse des Rechtsrahmens setzt an der Erörterung der rechtlichen Bedeutsamkeit der Datenbank an, untersucht Aspekte des Datenzugangs und -weiterverwendung und widmet sich schwerpunktmäßig datenschutzrechtlichen Anforderungen, insbesondere bedeutsamen Rechtfertigungsgründen sowie den Besonderheiten und Anforderungen mit Blick auf die Privilegierung von Forschungsdaten. Auch werden mögliche Rechtsformen untersucht. Schließlich wird auch die Bedeutsamkeit it-sicherheitsrechtlicher Vorgaben erläutert. Aufbauend auf die rechtliche Analyse werden praktische Handlungs-

vorgaben abgeleitet und Regulierungspotenzial aufgezeigt.

Die vorab in den drei Teilbereichen erarbeiteten Forschungsergebnisse wurden einem konsolidierten Review unterzogen und in einen Anforderungskatalog überführt. Hierzu wurden ausgehend von den Anwendungsszenarien und den Nutzerbedürfnissen rechtliche, wirtschaftliche und technische Anforderungen spezifiziert, die bei der Realisierung der Szenariendatenbank Berücksichtigung finden sollten.

Der Bericht kommt zu den zentralen Folgerungen:

- Es besteht die Notwendigkeit einer Zuschussfinanzierung zwecks Verteilung der Investitionsrisiken auf mehrere Parteien (Hauptlast auf der öffentlichen Hand) und Verringerung der Einstiegshürden für zukünftige Share-/Stakeholder
- Die zu besetzende Rollen sind Datenlieferant, Veredler, Betreiber, Auditor, Nutzer
- Die jeweiligen Motivatoren der einzelnen Rollen müssen klar adressiert und in der Betreibermodellstruktur verankert werden
- Die Ausgestaltung als kommerzielle oder nicht-kommerzielle Datenbank hat Einfluss auf die Betreibermodellstruktur und Rollenbesetzung (Privat / Öffentlich)
- IT-Sicherheit und Datenschutz sind von Anfang an mitzudenken
- Als Rechtsform kommt aus Haftungsgründen insbesondere die (gemeinnützige) GmbH in Betracht.
- Eine Anbindung existierender Datasets oder Scenario Libraries ist zweckmäßig
- Die Integration umfassender Suchoptionen ist sinnvoll
- Die Möglichkeit des Einspeisens von unterschiedlichen Arten von Szenarien (Rohdaten-Szenarien [Annotiert und Anonymisiert], OpenX-Szenarien, logische Szenarien, konkrete Szenarien, funktionale Szenarien, abstrakte Szenarien) ist zu gewährleisten
- Ein Bewertungsschema für Szenarien, welches den Wert und die Wichtigkeit jedes einzelnen Szenarios, wiedergibt und dies in den Kontext der Library und der ODD zieht ist zweckmäßig

Development of a concept and specifications for a scenario database for evaluating the safety effects of highly automated driving functions

This report provides an insight into the various dimensions of the conceptualization and development of a specification sheet for a cooperative database which is intended to underpin the creation of an exchange and distribution platform, which will in turn be used to generate simulation scenarios to evaluate the safety impact of autonomous driving functions. The narrative is divided into sections describing the legal, economic and technical framework and the conditions that need to be in place to ensure maximum benefit for the scenario database.

This involved the production of a preliminary study of the fundamental technical architecture which analyzed basic requirements for the integration of further relevant databases by means of an ontology as well as possibilities for the standardization of data formats.

In addition to this integration, the various databases/datasets were also examined in terms of modularity so as to achieve the highest possible test coverage and thus a reliable safety statement for a driving function. The modularization is an important aspect of the basic architecture for two reasons: first, to ensure that key legal conditions are addressed and, second, to enable maximum flexibility in the implementation. Another important part was an analysis of user access rights in terms of rights management and search queries related to an Operational Design Domain (ODD), as well as other user-specific queries. A technical validation was undertaken regarding a range of topics related to the generation and the associated feeding of scenarios as well as the filtering of stored scenarios to derive explicit recommendations for technical implementation.

In parallel, a far-reaching market analysis identified the key stakeholders of a cooperative scenario database and derived user-specific participation incentives and obstacles. The incentives and obstacles were evaluated by means of a stakeholder survey and then placed in the context of already existing scenario databases via interviews. The results were used to derive explicit participation requirements for the roles in the operator model for the respective stakeholder groups and further define them against a promising financing model. This analysis took into account the financing options relevant for individual stakeholders, while conceptualizing a subdivision into initial financing and operational financing.

The analysis of the legal framework starts with a discussion of the legal significance of the database, and examines topics related to data access and reuse. It goes on to focus on data protection requirements, in particular the various significant grounds for justification, as well as the special issues and requirements related to the privileging of research data. The different possible legal forms are examined next, and the significance of IT security requirements is explained after that. The legal analysis then serves to derive practical guidelines for action and identify regulatory possibilities.

The results of the research carried out in the three sections were subjected to a consolidated review and converted into a catalog of requirements. This was based on a specification of legal, economic and technical requirements on the basis of the application scenarios and user needs, which were taken into account in the realization of the scenario database.

The main conclusions of the report were the following:

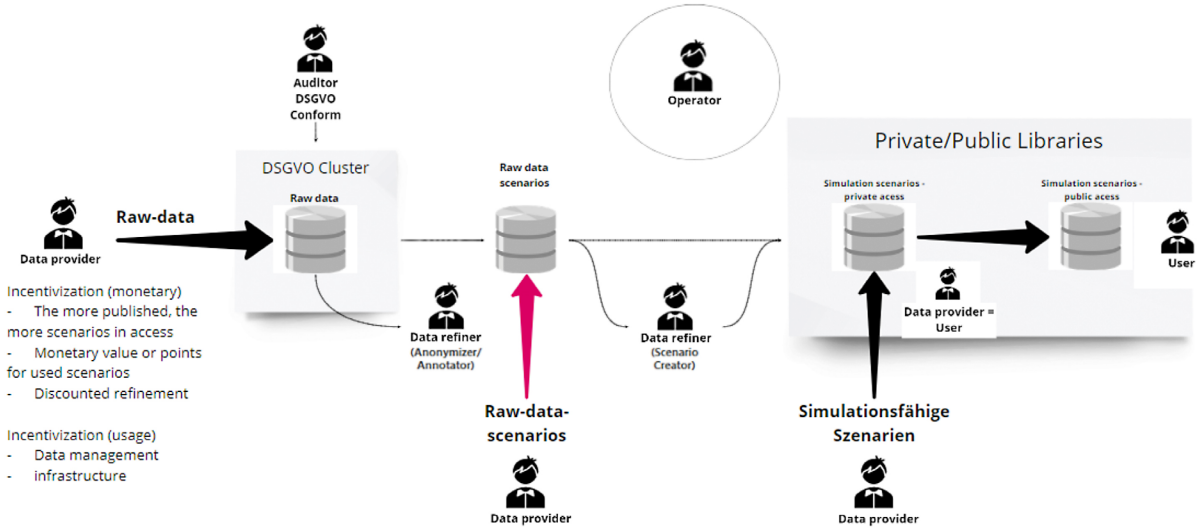
- There is a need for grant funding to spread investment risks across multiple parties (the primary burden should be on the public sector) and reduce initial hurdles for future share- and stakeholders
- The key roles which need to be filled for the relevant processes are data provider, refiner, operator, auditor, user
- The incentives of each role must be clearly addressed and embedded in the structure of the operator model
- The choice of whether a given database is commercial or not is relevant for the operator model structure and role assignment (the choice of private or public, for instance)
- IT security and data protection must be considered from the outset
- Liability considerations mean that the limited liability company (gGmbH) – whether non-profit or not – is the best choice of legal form

- It is advisable to ensure a connection to existing datasets or scenario libraries
- It is highly recommended to include comprehensive search options
- It must be possible to work with different types of scenarios (raw data scenarios [annotated and anonymized], OpenX scenarios, logical scenarios, concrete scenarios, functional scenarios, abstract scenarios)
- There should be an evaluation scheme for scenarios that reflects the value and importance of each scenario and puts this into the context of the library and the ODD

Summary

Development of a concept and specifications for a scenario database for evaluating the safety effects of highly automated driving functions

This short summary report looks into the various dimensions of the conceptualization and development of a specification sheet underlying a cooperative database. The report is divided into sections covering the legal, economic and technical framework and the conditions required to implement a utility-maximizing scenario database. The general concept is summarized in the following graphic.



Economic environment

To analyze the market architecture of a scenario database, the relevant stakeholders were identified and assigned to public, private or private-public categories. This categorization made it possible to identify the most important players and their operational interests and user concerns. These served as a basis for the structure of the role model, the underlying differentiated use case and the compilation of the legal, economic and technical requirements for the individual roles.

To ensure a successful operation of the scenario database, a use case scenario with five roles (data supplier, data refiner, auditor, operator and user) was developed. These roles acted as follows:

- If sufficient incentives were given, the data supplier contributed to the supply of the data required for the creation of the scenarios.
- The data refiner labeled/anonymized the available data sets to enable the implementation of the simulation scenarios.
- In addition to ensuring smooth technical operation (hosting, user administration, license management, software release maintenance, backup), the operator was responsible for the final selection and the establishment of scenarios. In addition to the necessary skills for handling annotated data, the operator had to enable the creation of test environments and the analysis of test data.

- The auditor checked the scenarios for their GDPR conformity or their quality and could act independently of the operator.
- Depending on the stakeholder cluster, users of the database could then use the available simulation scenarios to test the safety of autonomous driving functions, expand technical competence or identify infrastructure requirements.

A stakeholder could take on more than one role – operator and data refiner, for instance, or data provider and user. In any case, the casting of the roles depends on relevant participation stimuli or obstacles.

An extensive expert survey of 42 participants from various stakeholder groups evaluated incentives and obstacles related to database participation and used them to derive possible roles in the hypothetical operation. A constructive workshop with 24 participants subsequently allowed the results to be validated and adapted and the derived financing and operator model proposals to be analyzed together with industry experts. The results of the survey and the constructive workshop can be summarized in the following categories:

- The stakeholders that are most likely to fill the core operating roles (data refiner, operator or auditor) are:
  - Refiner: private or public-private institutions (AI companies, technology start-ups)
  - Operator: private sector (tool manufacturers, IT infrastructure companies)
  - Auditor: private or public-private institutions (federal authority, technical service), with the verification of the conformity of the anonymized data with GDPR carried out by a supervisory authority
  - Users: all clusters; with sufficient incentives, users may simultaneously act as data providers.
- The financing and operator models proposed for cost-covering operation are:
  - For the initial setup of the database (CAPEX): grant financing
  - For the financing of running costs (OPEX): a combination of constant membership fees and packaging (other payment possibilities include pay-per-dataset)
  - For later operation: commercialization of content, for example through simulations that link different scenarios, as well as refinement/linking of raw data
  - For the creation of incentives for data delivery: a remuneration system based on point credits which can be used to acquire new data or scenarios
  - The system can be modular, with the option to book further services (e.g., integrated anonymization)

A comparison with established scenario databases was carried out via interviews with the operators of the databases ENVITED marketplace (by the association Automotive Solution Center for Simulation) and SafetyPool (by Deepen AI and WMG University of Warwick). This focused on role distributions, value propositions, key resources and financing mechanisms. A range of similarities were found, such as the acceptance of all common file formats, the publication of simulation-capable scenarios by the respective data providers, or the goal of offering a variety of simulation scenarios for sale/exchange.

While the SafetyPool database pursues an international orientation and provides incentives through free access and the use of a points system, ENVITED marketplace restricts access to stakeholders with expertise in AD/ADAS systems and is distinguished by its association structure. Compared to the core functionalities of these existing databases,

the use case is characterized by numerous additional functionalities from the user's point of view. These include:

- Generation of a quantitative basis for legislative changes, in particular the – possibly necessary – regulatory improvement, legal control and the derivation of road safety measures
- Provision of basic elements required to expand technical competences
- Identification of the needs in infrastructure, technical services, AI systems, tools and other business models (R&D)
- Protection for the manufacturers of newly developed driving functions
- Access to IT infrastructure and simplified data management
- Differentiation (through flexible packaging of the use case) of user access and thus equal appeal to different stakeholder groups
- GDPR compliance

Ultimately, the use case created additional benefits and set clear incentives for the different stakeholder groups. The results of the economic analysis were constantly sychronised with the technical design, making it possible to derive a technically feasible and economically efficient application.

Technical framework architecture

The different use cases that are to be supported by a given database are the starting point of the basic technical architecture. There is special need for R&D scenarios in software-in-the-loop, hardware-in-the-loop, data reprocessing use cases and real drives on a proving ground for highly automated driving; these contribute to the ability to release licensed automated driving functions. It should be noted that various databases (e.g. Safetypool, ENVITED marketplace, the MUSICC database or the GIDAS database), as well as various datasets (e.g. NuScenes or ApolloScapes), are already available on the market. There are also services which provide scenarios for dedicated platforms. However, none of these databases, datasets or services meets all the requirements relevant to the mentioned use cases or is by itself sufficient for the protection of highly automated driving functions. Given that a large number of scenarios are required to make a reliable safety statement about automated driving functions, and since the use cases regarding such driving functions are highly detailed and manufacturer-specific, the database must contain an in-depth search functionality. This functionality must do justice to the corresponding applications. In addition to the relevant legal framework, which does not consider the use of raw personal data to infringe on individual privacy, established standards in the market also place important demands on architecture. The most important ASAM standards, which should be supported by relevant databases, especially in the context of simulation, are:

- ASAM OpenDrive
- ASAM OpenSzenario
- ASAM OpenODD (based on BSI PAS 1883)
- ASAM OpenLabel
- ASAM OpenXOntology

Since the database we are considering is supposed to be collaborative, it is essential that the database is hosted in a cloud. The technical framework architecture can be divided into the following sub-categories:

- Connecting other databases and datasets
  - Modular concept for the integration of different databases
  - Ontological database structure
- Transferring data sets to the collaborative database
  - Modular concept for feeding raw data
  - Feeding in raw data (GDPR server)
  - Feeding in anonymized and annotated scenarios
  - Feeding in simulation scenarios
  - Feeding in functional and abstract scenarios
- User access
  - Configurable dashboards for evaluating metadata
  - Definition of an ODD (with predefined taxonomy)
  - Search queries based on an ODD
  - Simple searches independent of ODD
  - Search queries that also search the descriptions in the metadata
  - Integration of scenarios into the scenario data base exclusively for private sector use
  - Possibility of feeding into/publishing in the collaborative database (see above)
- Metadata
  - Format based on one or more selected ODD taxonomy
  - Extension options by the user (additional tags/descriptions)
  - Description of scenario contents (e.g. ODD) and omissions (e.g. no 3D assets, no pedestrians).
  - Understanding where the relevant data comes from and how it is created (e.g. based on expert knowledge, measurements of a real trip or the PCM of the Gidas database)
  - Rating scheme – how important is a given scenario in the context of the database but also in the context of the ODD defined by the user.
- Rights management
  - Datasets or additional databases are not necessarily accessible to everyone, therefore appropriate licensing is implemented
  - Private area for own data and analysis
- Billing service

Legal framework

The analysis of the legal framework starts with the discussion of the legal benefits of the database. From the point of view of manufacturers and developers, the scenario database has legal relevance, in particular when it comes to the creation of a safety concept for the approval of automated driving functions and compliance with the relevant requirements in terms of liability, product safety, etc. Furthermore, the information provided in the

scenario database is important for the legal control related to the approval of automated driving functions as well as the promotion of different forms of deregulated self-regulation, such as the development of area-specific standards.

Next, the analysis states the reasons for justifying the processing of personal data that are relevant to data protection law – consent, the balancing of interests and the collection of car owner data due to the new legal justification basis in § 1 g StVG – as well as the special features and requirements related to the privileging of research data.

Finally, the analysis discusses the possible legal forms of database operation – for liability considerations, it considers the registered association and the GmbH (or UG). It goes on to investigate the incidence effect that is possibly due to tax advantages and advantageous in terms of research data, as well as being associated with image advantages associated with a meaningful classification as a "non-profit". The last step is an explanation of the importance of IT security regulations. Practical guidelines for action and the regulatory potential linked to the implementation of the database are then derived based on the analysis of the legal environment.

The analysis has the following legal recommendations:

- IT security must be considered from the very start
- The database should not be fed with personal data,
- As little personal data as possible should be transferred to the database. Therefore, non-personal data should be requested from the data suppliers, as so far as sufficient information content for the processing purpose is guaranteed.
- If personal data is nevertheless included in the database, the data processing should be shaped in a way that ensures compliance with the GDPR.
- All processing/information/balancing processes should also be documented comprehensively (to guard against liability risks beyond general accountability).
- The concept of the research project (in particular the question, responsibilities, types of data used, possible calculations, methodology, community benefits and the publication of the essential results) and the adoption of appropriate guarantees in accordance with Article 89 (1) and (2) GDPR should be presented transparently in order to benefit from the data protection privileges of research data.
- In this context, if the database is privately operated, care must be taken to ensure that purely commercial use is separate from research and development; it is advisable to set up an outsourced research database for this purpose. In the case of private financing or private self-interest, a concept must be developed that excludes direct influence on knowledge transfer (e.g., through instructions). In addition, it must be shown that private (e.g., economic) interests do not dominate the research orientation.
- Overall, it is worthwhile to maintain a cooperative exchange with the responsible data protection authority.
- For reasons of liability, the legal forms of either GmbH or registered association should be considered, with GmbH probably being better in the long term. GmbH status has numerous advantages but is only conceivable if the prohibition on profit reduction is compensated by a suitable financing model. Before founding an association or a Limited Liability Company with the privileges granted under § 51 AO, it is advisable to contact the competent financial authorities in good time in order to ensure that the requirements of community law are met.

Inhalt

Der Anhang zum Bericht ist im elektronischen
BASt-Archiv ELBA unter: https://bast.opus.hbz-nrw.de abrufbar.

1 Einleitung

Automatisiertes und autonomes Fahren ist in aller Munde. Mit der Änderung des Straßenverkehrsgesetzes im Jahr 2017 hat der Gesetzgeber auf nationaler Ebene bereits die normativen Weichen für Fahrfunktionen höheren Automatisierungsgrades gestellt. Am 28. Juli 2021 trat das Gesetz zum autonomen Fahren in Kraft. Durch eine zunehmende Automatisierung bis hin zum autonomen Fahren verspricht man sich neben Effizienzgewinnen und einer folgenden Verkehrsminimierung insbesondere, die Zahl der Unfalltoten drastisch zu reduzieren und die Verkehrssicherheit signifikant zu verbessern. Konkrete technische Anforderungen an die seit 2017 zulässigen Fahrfunktionen fehlen. Dies liegt unter anderem daran, dass es bislang wie bereits erwähnt in diesem Zusammenhang an evidenzorientierten Instrumenten für die prospektive und retrospektive Bewertung der Auswirkungen des Einsatzes automatisierter Fahrfunktionen auf die Verkehrssicherheit fehlt. Diese sind aber sowohl für Hersteller und Zulieferer, als auch für die Wissenschaft und regelungsnahe Forschung unbedingt erforderlich, um die industrielle Entwicklung und die entsprechende Regulierung daraufhin abzustimmen und auf diese Weise zeitnah dem sicheren Einsatz solcher Fahrfunktionen im realen Straßenverkehr den Boden zu bereiten. Eine retrospektive Auswertung aussagekräftiger Quelldaten ist geeignet, den zulassungsrechtlichen Regulierungsbedarf zu eruieren und eine zweckmäßige Feinsteuerung anzuleiten. Auch verspricht der auf diese Weise ermittelte Kenntnisgewinn Wahrnehmung, Sensibilisierung und Akzeptanz seitens der Gesellschaft und eine Diskussionsgrundlage anstehender demokratischer Auseinandersetzung zu schaffen. Um die verkehrlichen Auswirkungen beurteilen zu können, bedarf es eines umfassenden Überblicks über die relevanten, konkreten und situativen straßenverkehrlichen Steuerungsabläufe und Steuerungsmechanismen, welche sich aus amtlichen Statistiken nur eingeschränkt entnehmen lassen. Insbesondere fehlt eine gesamtheitliche Informationsgrundlage zur prospektiven und auch retrospektiven Beurteilung der Frage, ob automatisierte Fahrfunktionen, die sich durch eine maschinelle Längs- und/oder Querführung, welche nicht mehr durch einen Menschen initiiert oder überwacht wird, auszeichnen, für den Betrieb im realen Straßenverkehr geeignet sind. Die Informationslage ist bislang durch eine Vielfalt verschiedener singulärer Datenquellen geprägt, die nur einem beschränkten Personenkreis zur Nutzung zur Verfügung stehen, was einer ergänzenden, kumulativen und umfassenden Nutzung entgegensteht.

Projektziel ist vor diesem Hintergrund die konzeptionelle Modellierung einer zentralen Szenariendatenbank als rechtlich zulässige, kollaborative Datenfusion steuerungsrelevanter Verkehrs-, Umwelt und Straßendaten zwecks prospektiver und retrospektiver Ableitung einheitlicher Prüfverfahren hochautomatisierter Fahrfunktionen auf ihre Eignung für den sicheren Einsatz im öffentlichen Straßenverkehr. Dabei lag der Schwerpunkt auf der konzeptionellen Entwicklung einer geeigneten rechtskonformen, technischen Architektur und eines Rollenmodells aus bestehenden Ansätzen. In rechtlicher Hinsicht wurde dabei schwerpunktmäßig analysiert, welche Anforderungen mit Blick auf Datenschutz, Datensicherheit, Datenzugang und Datennutzung an einen zulässigen Datenbankbetrieb zu stellen sind. Im Anschluss einer analytischen Betrachtung der möglichen Marktstruktur, einschließlich der Identifikation potenzieller Nutzer der Szenariendatenbank wurde ein Lastenheft erstellt, welches die Grundlage in der für die Nachfolgeprojekte geplanten Implementierung der Datenbank bildet und die konzeptionellen Anforderungen definiert. Schließlich wurde das entwickelte Konzept einer abschließenden Evaluierung unterzogen und sowohl die praktische Umsetzbarkeit der technischen Architektur, die Anwendbarkeit der Szenariendatenbank als auch die Datengrundlage und Parametrisierung der Prüfszenarien anhand eines repräsentativen Anwendungsfalls bewertet. Somit konnten Hand-

lungsdirektiven zur Modifikation und Optimierung des Lastenhefts vorgenommen werden. Dies implizierte auch Überlegungen, wie mit der Herausforderung zur Beschaffung und Kategorisierung der Daten umgegangen wird und wie, auch aus technischer Sicht, eine rechtssichere Nutzungsarchitektur geschaffen werden kann. Hierbei wurde zudem die Verarbeitung der Daten bezüglich unterschiedlicher Datenformate wie bspw. Sensor-Rohdaten oder Objektlisten mittels Labeln oder Selektieren betrachtet. Neben den im Fahrzeug aufgezeichneten Daten spielte auch der Import von Daten aus anderen externen Quellen wie Infrastrukturaufzeichnungen oder anderen Datenbanken wie bspw. GIDAS eine wichtige Rolle.

2 Vorgehen

Im Auftrag der Bundesanstalt für Straßenwesen widmete sich das IKEM in Kollaboration mit TÜV Nord, dSPACE und consulting4drive der konzeptionellen Modellierung einer Szenariendatenbank mit Blick auf die Sicherheitswirkung hochautomatisierter Fahrfunktionen und der an eine solche zu stellenden Anforderungen. Das Projekt lief zwölf Monate von Dezember 2020 bis einschließlich November 2021. Ausgehend von der Betrachtung gegenwärtiger technischer und organisatorischer Lösungen, erprobter Betreibermodelle, des Rechtsrahmens und für die Entwicklung solcher Datenbanken relevanter Akteure wurden Anforderungen analysiert und eine technische Rahmenarchitektur entworfen. Anschließend wurde komplementär eine Architektur ökonomischer Rahmenbedingungen entwickelt und ein geeignetes Betreiber- und Finanzierungsmodell hergeleitet. Darauf aufbauend wurden Anforderungen zur Implementierung und Einführung der Szenariendatenbank in einem Lastenheft spezifiziert und einer technischen Validierung zugeführt sowie praktische rechtliche, organisatorische und technische Handlungsempfehlungen abgeleitet. Der vorliegende Schlussbericht fasst die Arbeitsergebnisse des Projektverlaufs zusammen.

3 Ergebnisse

3.1 Technische, rechtliche und ökonomische Rahmenarchitektur

Die konzeptionelle Modellierung einer zentralen Szenariendatenbank als rechtlich zulässige, kollaborative Datenfusion steuerungsrelevanter Verkehrs-, Umwelt und Straßendaten erforderte eine eingehende Analyse der technischen Rahmenarchitektur, der rechtlichen Anforderungen und der Marktarchitektur unter Identifikation potenzieller Stakeholder.

3.1.1 Analyse der technischen Rahmenarchitektur

Im Folgenden werden, ausgehend von der Entwicklung von Fahrerassistenzsystemen oder Fahrfunktionen für automatisiertes Fahren, die unterschiedlichen Formen von Szenarien dargelegt. Des Weiteren wird ein Bild entworfen, welches aufzeigt, wie Szenarien erzeugt und genutzt werden, um dann Ableitungen für eine technische Rahmenarchitektur darzustellen. Dadurch wird sich ein grober Überblick über aktuelle Bibliotheken oder Datasets ergeben.

Der Kern bei der Entwicklung und Absicherung von Fahrerassistenzfunktionen oder Funktionen für das automatisierte Fahren ist eine verlässliche Absicherungsstrategie des Software-Stacks der zu implementierenden Fahrfunktion. Entsprechend müssen Tests auf unterschiedlichen Ebenen (Perception, Data Fusion, Localization, Motion Planing, etc.) durchgeführt werden. Es müssen für jede dedizierte Ebene Szenarien in diese Software-Komponente eingespeist werden, um sie validieren zu können. Im Absicherungsprozess werden dazu eine Vielzahl von Szenarien benötigt. Es lassen sich unterschiedliche Abstraktionen von Szenarien unterscheiden:

- Funktionales Szenario (Functional Scenario):
  Die Darstellung von funktionalen Szenarien basiert auf einer sprachlichen Beschreibung. Funktionale Szenarien stellen Betriebsszenarien des Entwicklungsgegenstands auf semantischer Ebene dar. Die Entitäten und Beziehungen zwischen den Entitäten der Anwendungsdomäne werden in sprachlich gefassten Szenarien ausgedrückt. Die Szenarien sind widerspruchsfrei. Das Vokabular der funktionalen Szenarien ist spezifisch für den Anwendungsfall und die Anwendungsdomäne und kann unterschiedliche Detailtiefe aufweisen.
- Logisches Szenario (Logical Scenario):
  Logische Szenarien stellen eine Detaillierung der funktionalen Szenarien im physikalischen Zustandsraum dar. Somit lassen sich funktionale Szenarien in Parameter der Entitäten (absolute Parameter) und Parameter der Beziehungen (relative Parameter) überführen. Logische Szenarien stellen Betriebsszenarien durch Entitäten und Beziehungen dieser Entitäten mithilfe von Parameterbereichen im Zustandsraum dar. Für die einzelnen Parameterbereiche können optional statistische Verteilungen angegeben werden. Zusätzlich können optional die Beziehungen der Parameterbereiche zueinander, mithilfe von Korrelationen oder numerischen Bedingungen modelliert werden. Logische Szenarien enthalten eine formale Beschreibung von Szenarien.
- Konkretes Szenario (Concrete Scenario):
  Konkrete Szenarien beschreiben die Entitäten und Beziehungen der Entitäten mithilfe von eindeutigen Parametern im Zustandsraum. Jedes logische Szenario kann durch Konkretisierung der Parameterbereiche zu jeweils einem festen Wert in ein konkretes

Szenario überführt werden. Konkrete Szenarien stellen Betriebsszenarien eindeutig durch Entitäten und Beziehungen dieser Entitäten mithilfe von festen Werten im Zustandsraum dar.

Neben den unterschiedlichen Abstraktionsebenen sind auch die folgenden Begrifflichkeiten wichtig:

- Rohdaten-Szenario:
  Als Rohdaten-Szenario werden die gelabelten Rohdaten oder die generierten Objektlisten einer Messfahrt bezeichnet. Rohdaten bezeichnen hier die Bilddaten einer Kamera, die Punktewolke eines Lidar-Sensors oder die Detection-Liste eines Radar-Sensors, wobei auch GPS-Informationen oder die aufgenommenen Fahrzeugbusdaten inkl. der Objektlisten ein Teil der Daten sein können.
- Simulations-Szenario:
  Das Simulationsszenario ist eine Repräsentanz eines konkreten oder logischen Szenarios innerhalb einer Simulationsumgebung. Ein solches Simulationsszenario könnte dann beispielsweise aus einer OpenScenario-, OpenDrive-Beschreibung sowie einer Beschreibung der 3D-Welt bestehen.
- Replay-Szenario:
  Ein Replay-Szenario ist ein Szenario, welches exakt die aufgezeichnete Trajektorie abfährt. Es kann sich dabei um ein Rohdaten-Szenario handeln oder um ein konkretes Szenario (Simulations-Szenario). Das Replay-Szenario stellt dabei ein spezielles konkretes Szenario dar.

All diese unterschiedlichen Szenarien-Typen sind im Absicherungsprozess von Bedeutung. Ein funktionales Szenario wird in der Regel von entsprechenden Experten geschrieben, um dann entweder in realen Testfahrten auf einem Testgelände instanziiert zu werden, oder es wird in ein Simulations-Szenario für eine dedizierte Simulations- und Testplattform überführt. Im letzteren Fall entstehen im Wesentlichen logische und konkrete Szenarien. Logische Szenarien sind für das szenariobasierte Testen entscheidend, da sie es ermöglichen, auch schon früh im Entwicklungsprozess die benötigten Parametervariationen (z. B. Geschwindigkeit des Ego-Fahrzeugs, Variation der Wetterbedingungen oder des Verkehrs) durchzuführen und damit auch gemäß SOTIF die bekannten und auch unbekannten Risiken zu identifizieren bzw. zu minimieren. Soll die Implementierung des Motion Planings getestet werden, so werden i. d. R. Simulations-Szenarien benötigt, die keine qualitativ hochwertige 3D-Umgebung beinhalten muss, vielmehr ist es ausreichend, dass die im Szenario definierten Objekte, Positionen etc. vorliegen, um die benötigten Objektlisten für den zu testenden Algorithmus zu erzeugen. Wird hingegen die Perzeption geprüft, so sind zum einen hochwertige 3D-Szenarien erforderlich, die es ermöglichen, eine physikalische Sensorsimulation durchzuführen, d. h. eine Simulation der Sensoren (z. B. Radar, Lidar, Kamera oder Ultraschall) in Interaktion mit einer möglichst realistischen 3D-Welt unter Berücksichtigung von Ausbreitungseigenschaften und auch Materialeigenschaften der unterschiedlichen Objekte, zur Erzeugung von möglichst genauen Sensorrohdaten, Punktwolken, Detektionslisten oder Target-Listen. Weiter werden hier auch Rohdaten-Szenarien (hier auch Replay-Szenarien) verwendet und sind für Data-Replay-, Data-Reprocessing-Anwendungen aber auch für das Training einer KI entscheidend. Für die Validierung der Simulationsmodelle oder der Simulation werden Szenarien benötigt, die die Realität möglichst gut abbilden. Entsprechend müssen diese Szenarien mit Hilfe von Referenzsensorik aufgenommen, dann annotiert, und dann in ein Simulations-Szenario mit einer hochwertigen 3D-Simulation überführt werden.

Es existieren für die unterschiedlichen Anwendungsfälle diverse DataSets/Bibliotheken (NuScenes, PandaSet, AppolloScapes, Berkelay DeepDrive, Landsmarks, Astyx Dataset, Waymo Open Dataset, etc.), jedoch unterscheiden diese sich erheblich. Einige DataSets enthalten ausschließlich Bilder oder Frames (wie der Landmarks Datensatz), manche haben neben Kamera-Daten auch Lidar-Daten (wie der NuScenes-Datensatz oder Pandaset) und wieder andere Datasets oder Bibliotheken sind auf Simulationsszenarien beschränkt (z. B. Safety Pool oder ADScene), liefern jedoch keine detaillierte 3D-Umgebung. Jede Bibliothek oder jeder Datensatz kann aber wertvoll im Absicherungsprozess sein.

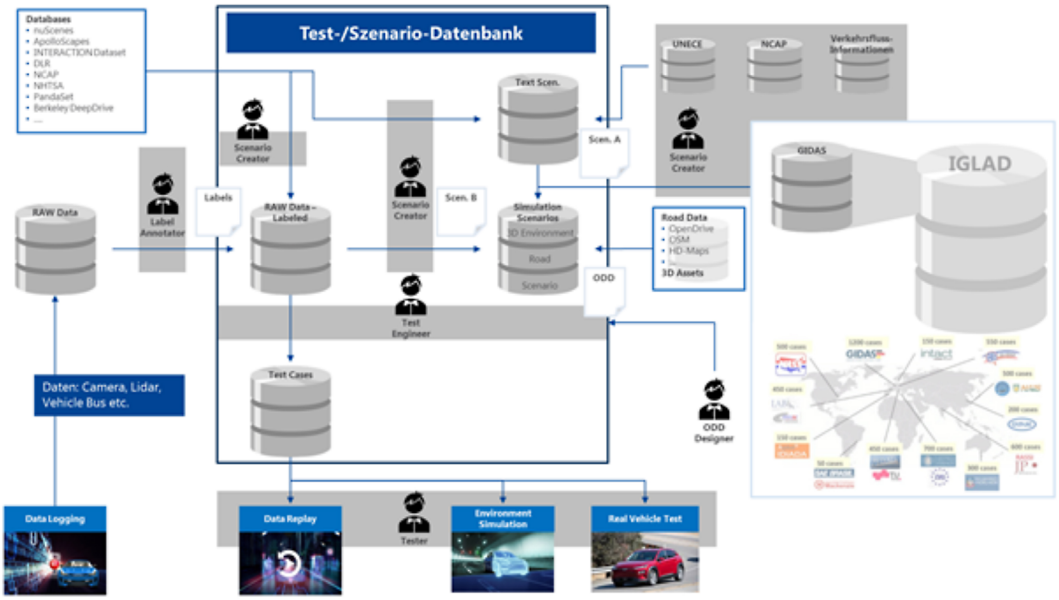


Bild 1: Schematische Darstellung der technischen Personas im Datenbankbetrieb (Quelle: Eigene Darstellung)

Innerhalb des Absicherungs- und Entwicklungsprozesses einer Fahrerassistenzfunktion oder einer Funktion für das automatisierte Fahren, können verschiedene Personas identifiziert werden, die sich gemäß des Rollenmodell in Kapitel 3.2 aufeinander abbilden lassen. Die folgende Tabelle beschreibt zum einen die Funktion der dedizierten Personas und zum anderen stellt sie den Bezug zu dem Rollenmodell aus Kapitel 3.2 her. Ein Kernproblem einer zentralen Test-/Szenariendatenbank stellt die Unterstützung einer Vielzahl verschiedener Datenformate dar, die durch die unterschiedlichen Personas genutzt werden können. Beginnend mit den diversen Unfalldatenbanken, die bereits existieren, aufgezeichneten Daten aus dem realen Fahrzeug, Verkehrsdaten aus Induktionsschleifen oder extrahiert von Kameradaten sowie verschiedenen Initiativen, die ihrerseits Datenbanken aufgebaut haben bzw. aufbauen (z. B. NuScenes Dataset, VOIESUR Database, Udrive Database, MOOVE Database, MUSICC Database, etc.), ergeben sich eine Vielzahl von Importmöglichkeiten. Eine Kernaufgabe muss es daher sein, die unterschiedlichen Use Cases der verschiedenen Rollen/Personas zu unterstützen (vgl. Bild 1).

Rolle	Persona	Beschreibung
Veredler	Label Annotator	• Verantwortet das Labeln bzw. Annotieren der Daten • Identifiziert und klassifiziert Objekte in Szenen und reichert die Daten mit diesen Informationen an • Erhält Daten und (Objekt-)Listen über die zu labelnden Inhalte vom Kunden • Verwendet (halbautomatisch) Labeling-Tools • Erstellt und validiert hochgenaue, maschinenlesbare Labels für: ○ maschinelles Lernen ○ Ground Truth für XiL ○ Erstellung von Szenariodatenbanken
Veredler	Scenario Creator	• Stellt Szenarios auf Basis der annotierten Daten inklusive strukturierter Beschreibungen bereit • Identifiziert die notwendigen Informationen für die Szenariobeschreibung • Erstellt Szenariobeschreibungen ○ textuell oder ○ in technischen Formaten (z. B. XML) oder ○ grafisch
Nutzer/ Veredler	Test Engineer	• Spezifiziert, implementiert und führt Tests aus • Arbeitet mit vorgegebenen Szenarien, die gemäß einer Standard-Ontologie definiert sind • Parametriert Szenarien, definiert und plant Testfälle, richtet die Testumgebung ein, analysiert Testdaten • Verantwortlich für Auswertung und Reporting
Nutzer	ODD Designer	• Spezifiziert mit der ODD [Operational Design Domain] die Systemarchitektur und (ADAS/AD)-Funktionalitäten • Definiert Betriebs- und Umgebungsbedingungen für ADAS/AD-Funktionen • Ableitung und Identifizierung von Szenarien aus der ODD basierend auf Systemarchitektur und -Features • Verantwortlich für den Datenaustausch zwischen den verschiedenen Stakeholdern (Hersteller, Regulierungsbehörden, Tier-1-Lieferanten)
Nutzer/ Veredler	Development Engineer	• Entwickelt Sensor-Setup und Software-Algorithmen für ADAS/AD-Funktionen gemäß ODD • Kennt die relevanten Parameter sowie deren Wertebereiche der ODD Funktionen, die während des automatisierten Fahrens auftreten können • Kennt die relevanten Szenarien, mit denen das automatisierte Fahrsystem konfrontiert werden könnte, und führt Anforderungen auf diese Eingangsdaten zurückführen • Überwacht anhand von Kriterien die Einhaltung der ODD und implementiert Erkennungs- und Reaktionsfunktionen im Fall der Nichteinhaltung • Prüft Tests, Daten und Szenarien gegen die ODD-Beschreibung
Nutzer/ Veredler	Model Creator	• Erstellt die Fahrzeug-, Umgebungs- und Sensormodelle/Sensorfusionsmodelle • Erstellt Modelle, die bei der Simulation für die Szenarioausführung eingebunden werden
Nutzer	Tool Developer	• Entwickelt Werkzeuge oder ganze Tool-Suiten für • Datenerfassung und Dateneinspeisung • Simulation (z. B. Fahrdynamik, Umgebungen) • Testen und Verifizieren von Komponenten und Systemen • Szenariogenerierung • Simulation mit Ground-Truth-Daten, die einen großen Satz von (kritischen) Szenarien für Tests von ADAS/AD-Funktionstests bereitstellen • Die Tools unterstützen standardisierter Formate für Labels (z. B. OpenLABEL) und Szenariobeschreibungen (z. B. OpenSCENARIO)

Tab. 1: Technische Ausdifferenzierung der Rollen und Personas im Datenbankbetrieb

Rolle	Persona	Beschreibung
Nutzer	Safety Engineer	• Leitet (halbautomatisch) aus der formalen ODD-Definition einen Situationskatalog zur Gefahrenerkennung ab • Zeigt die Metrik der Abdeckung die betrachteten Szenarien in Bezug auf die gesamte ODD auf • Schätzt das verbleibende Risiko von Gefahrenszenarien ab, die nicht vom Sicherheitskonzept und Validierungsansatz abgedeckt werden • Identifiziert Szenarios, die ein ungewolltes Verlassen der ODD aus einer formalen Definition der Grenzen der ODD ermöglichen, um diese Situationen mit geeigneten Erkennungs- und Reaktionsmechanismen zu behandeln. • Identifiziert Bereiche oder Teilbereiche der ODD, bei denen Fehler zu Gefährdungen führen könnten und klassifiziert ADAS/AD-Funktionen oder welches Verhalten in jeder von ihnen einen akzeptabel sicheren Betrieb gewährleisten.

Tab. 1: Technische Ausdifferenzierung der Rollen und Personas im Datenbankbetrieb (Fortsetzung)

Es ergeben sich je nach Anwendungsfall (Software-in-the-loop, Hardware-in-the-Loop, Data Reprocessing zur Absicherung der Perzeption, Motion Planing, etc.) unterschiedliche Anforderungen an die Daten/Szenarien. Um unterschiedliche Datenquellen gemeinsam und ergänzend nutzen zu können, lassen sich im Wesentlichen zwei Strategien identifizieren:

- Umwandlung der einzelnen Entitäten der Datenquellen in ein einheitliches Format einer neuen Szenariendatenbank
- Nutzung der unveränderten Datenquellen mit den zu Verfügung gestellten Metadaten

Bevor die Strategien detaillierter erläutert werden, müssen vorab einige Begrifflichkeiten und Konzepte näher dargestellt werden. Die Begriffe und die entsprechenden Konzepte von Taxonomie und Ontologie sind klar zu differenzieren, da beide Begriffe im Zuge der Wissensmodellierung wichtige Bausteine sind und zentral zum Verständnis des Datenbankkonzeptes genutzt werden. Die Taxonomie ist ein Klassifizierungsschema, in dem Objekte nach festgelegten Kriterien eingeordnet werden. In der Regel stellen sich Taxonomien als monohierarchische Strukturen da, die ein kontrolliertes Vokabular, d. h. eine Sammlung von Bezeichnungen, die eindeutig Begriffen zugeordnet sind, beinhalten. Das bedeutet, dass jeder Klasse auch nur eine Oberklasse zugeordnet ist. Genau diese Form der Taxonomie wurde beispielsweise in dem Standard BSI PAS 1883 für ODDs entwickelt. Im Gegensatz zur Taxonomie stellt die Ontologie neben einer auch hierarchisch angeordneten Taxonomie Querbezüge zu anderen Klassen her. Eine Ontologie stellt also ein Netzwerk aus Informationen mit logischen Relationen dar und ist eine formal geordnete Darstellung von Mengen und Begriffen. Sie bringt zusätzlich Regeln zu Schlussfolgerungen und zur Gewähr-

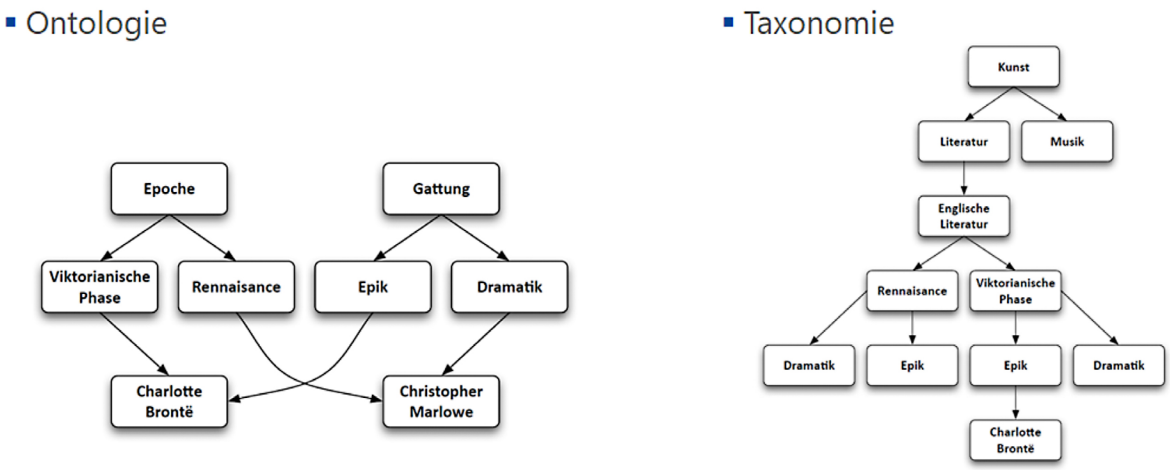


Bild 2: Unterschied zwischen Ontologie und Taxonomie (Quelle: Eigene Darstellung)

leistung ihrer Gültigkeit mit. Einfach lässt sich der Unterschied zwischen einer Ontologie und einer Taxonomie in Bild 2 erkennen.

Eine Ontologie wird dazu genutzt, bestehendes Wissen zu modellieren, in bestehendem Wissen zu suchen und auch Wissen zu generieren. Betrachtet man die ASAM OpenXOntology Standardisierungsinitiative, so kann festgestellt werden, dass dort die unterschiedlichen Aspekte aus OpenDrive, OpenScenario, OpenLabel und OpenODD verknüpft werden (vgl. Bild 3). Beispielsweise wird in OpenODD die Taxonomie aus dem Standard BSI PAS 1883 verwendet und weiterentwickelt und in den Kontext einer Ontologie gesetzt (Stichwort: Terminologieharmonisierung). Dabei wird aus der initial monohierarchischen ODD Taxonomie im ersten Schritt eine polyhierarchische Taxonomie und im zweiten Schritt eine über Relationen vernetzte Abbildung des Wissens – es entsteht eine Ontologie auf Basis gegebener Taxonomien.

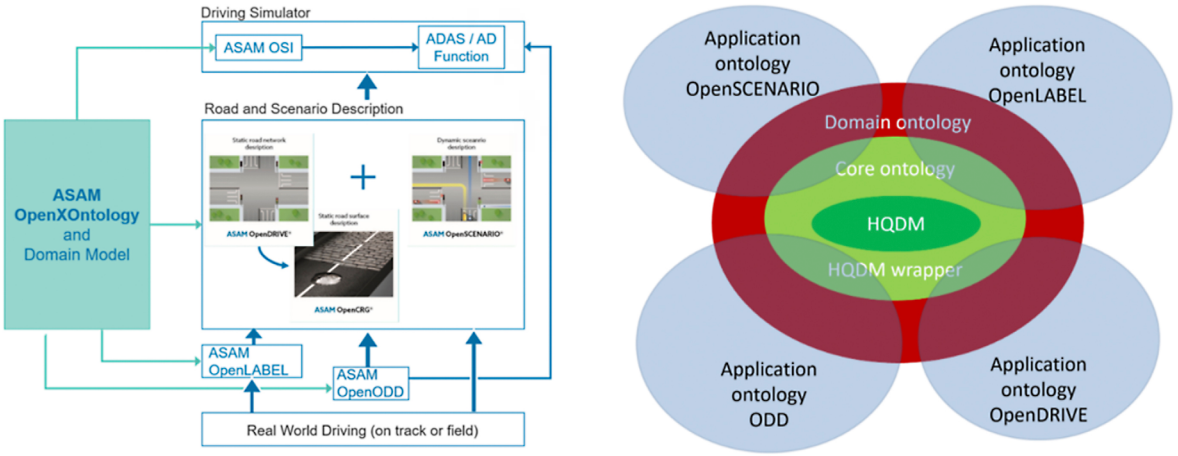


Bild 3: ASAM OpenXOntology und die Zusammenhänge zu OpenODD, OpenLabel, OpenDrive und OpenScenario (Quelle: https://www.asam.net, zuletzt abgerufen am 04.11.2022)

Umwandlung der einzelnen Entitäten der Datenquellen in ein einheitliches Format einer neuen Szenariendatenbank (Native Datenbank):

Bei dieser Strategie sind die entsprechenden Szenarien zu identifizieren und in das definierte Format zu konvertieren. Dieser Konvertierungsvorgang müsste dann regelmäßig durchgeführt werden, um kontinuierlich und retroperspektivisch Aussagen zu automatisierten Steuerungsvorgängen zu treffen. Bei der Konvertierung in das entsprechende Format (z. B. OpenScenario, OpenDrive) sind dann die zugehörigen Metadaten hinzuzufügen, die sich zum einen aus den Metadaten der Datenquelle speisen und/oder zusätzlich durch Expertenwissen angereichert werden, aber dann auch gemäß einer einheitlichen Taxonomie innerhalb der neuen Datenbank verschlagwortet sind. Die Verschlagwortung sollte durch gängige Taxonomien (SAE J3016, BSI PAS 1883, NHTC, OpenODD, OpenLabel etc.) erfolgen, um in der neuen Szenariendatenbank umfassende Suchanfragen formulieren zu können. Neben gängigen Begriffen, die durch die ODD gegeben sind, müssen zusätzlich Metadaten den Szenarien angehängt werden. Das beinhaltet u. a. die Einordnung des Manövers (z. B. Cut-in, Cut-out, etc.), die Datenquelle (Herkunft, Datum, Ort), die Version des Formates (z. B. OpenDrive 1.4 und OpenScenario 1.0), die Einordnung, ob es sich um ein funktionales, logisches oder konkretes Szenario handelt und auch die Information, ob dieses Szenario aus Messdaten oder mit Expertenwissen erstellt wurde bzw. ob es ein Rohdaten-Szenario ist. Die grundsätzlichen Suchanfragen können dann gemäß einer einfachen relationalen Datenbank realisiert werden, wobei bei einer Änderung der Taxonomie natürlich ein Update der Datenbank erforderlich wird. Entsprechend kann hier eine Ontologie verwendet werden, um die jeweilige relationale Datenbank (d. h. die neue Szenariendatenbank) zu adressieren. Dies hätte den Vorteil, dass eine Suchanfrage gemäß der Ontologie weitere logische Rückschlüsse zulässt, auch wenn einzelne Einträge in der Datenbank eine andere Taxonomie verwenden.

Nutzung der unveränderten Datenquellen mit den zu Verfügung gestellten Metadaten:

Da die unterschiedlichen Datenbanken oder Datenquellen auch regelmäßig aktualisiert werden, ist es sinnvoll, direkt diese Datenbanken nutzen zu können (vgl. Bild 4). Dabei stellt die Ontologie ein zentrales Element innerhalb des Datenmanagements dar. Die Ontologie ermöglicht es in Kombination mit einer Mapping-Schicht, die die Ontologie mit der relationalen Datenbank verbindet, logische Zusammenhänge schon bei einfachen Suchanfragen zu nutzen, um damit eine bessere und komfortablere Suche in den Datenbanken zu gewährleisten. Die Mapping-Schicht bildet dabei die Verbindungschicht zwischen den Metadaten der angebundenen relationalen Datenbank und der Ontologie. Die Ontologie kann im Wesentlichen als Wissensmodellierung rund um das Thema automatisiertes Fahren begriffen werden. Durch eine Ontologie und die entsprechende Anbindung verschiedener Datenbanken können die Informationen der Datenbanken gemeinsam und ergänzend untersucht werden. Daraus lassen sich dann auch Rückschlüsse ziehen, welche Szenarien für eine bestimmte ODD sinnvoll sind. Sobald entsprechende Szenarien identifiziert wurden (durch die Suchanfrage mit Hilfe der Ontologie), können diese dann entsprechend in das passende Format für den Use Case konvertiert werden. Die Verschlagwortung der umgewandelten Szenarien sollten jedoch ähnlich wie in der vorherigen Option durchgeführt werden.

Neben der Anbindung der Datenbank sind die User-Interfaces ein wichtiger Teil, um die Filtereigenschaften einzustellen und eine Abdeckung bzgl. der ODD gut zu visualisieren. Dabei muss hier natürlich berücksichtigt werden, dass je nach Nutzer (Stakeholder) unterschiedliche Zugänge erforderlich sind. Neben dem Datenmanagement ist auch ein

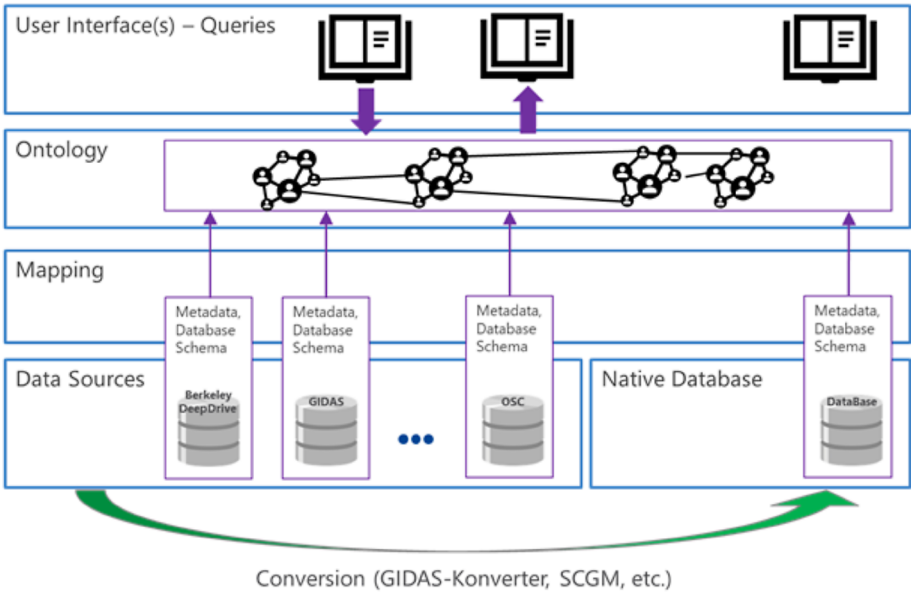


Bild 4: Schematische Darstellung einer kollaborativen Datenbank (Quelle: Eigene Darstellung)

Berechtigungsmanagement erforderlich, da bei einer Anbindung verschiedener Datenbanken nicht zwingend jeder Nutzer auf alle Daten zugreifen kann bzw. darf. Im Wesentlichen sollten alle Nutzer auf die Native Datenbank zugreifen können. Des Weiteren möchten Stakeholder z. B. OEMs auch anteilig nicht alle Szenarien publizieren. Daher sollte es für die Nutzer auch private Bereiche geben, um die eigene Datenbank anzubinden. Idealerweise muss es, wenn es eine Incentivierung für beispielsweise OEMs und Tier1-Zulieferer geben soll, auch ein entsprechendes Abrechnungsmanagement geben (Dies hängt stark von dem Betreiber- und Finanzierungsmodell ab). Dabei sollte jeder Nutzer, der in die Native Database einzahlt, auch incentiviert werden. Insgesamt stellt das Finanzierungs- und Partnermodell (vgl. Herleitung Betreiber- und Finanzierungsmodelle) entscheidende Rahmenbedingungen für die Nutzung und somit an auch an die Rahmenarchitektur.

3.1.2 Analyse der Marktarchitektur

Als vorgelagerte Aufgabe und als Basis der technischen Ausarbeitung sowie folglich auch als Grundlage der Anforderungen im entwickelten Lastenheft bedarf es einer umfangreichen Marktanalyse zur Identifikation der wichtigsten Interessensgruppen und möglichen Partizipanten im Szenariendatenbankbetrieb. Hierfür werden im Folgenden zunächst die wichtigsten Stakeholder aus allen Sektoren identifiziert, kategorisiert und gemappt. Aufbauend werden die jeweiligen Nutzeninteressen herausgearbeitet und anschließend zwei bereits existierende Datenbanken mit dem Fokus auf die Kooperation im Bereich des Austauschs prüfungsrelevanter Simulationsszenarien genauer beleuchtet. Ziel ist die Identifikation, der für einen erfolgreichen Datenbankbetrieb relevanten Stakeholder und deren Nutzerbedürfnis, welches bisher noch nicht durch existierende Lösungen abgedeckt ist oder durch erschwerte Zugangsmöglichkeiten minimiert wird.

Stakeholdermapping

Als erster Schritt der Marktanalyse konnten durch die Erstauswertung existierender Initiativen und Projekte sowie anhand einer breiten Sekundärrecherche die relevanten möglichen Stakeholder mit diversem Nutzerinteresse an einer Simulationsszenariendatenbank

zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen identifiziert werden. Die Interessensgruppen sind in allen Sektoren von Öffentlich bis Privat mit einem Fokus auf die Automatisierung und Vernetzung im Straßenverkehr angesiedelt. Die initiale umfangreiche Stakeholderliste wurde durch Einbezug der projektinternen Expertise bewertet und in relevante Über- und Unterkategorien aufgeteilt.

Aus der ersten Kategorisierung wurden wiederum die Akteure im hypothetischen Szenariendatenbankbetrieb mit dem höchsten bewerteten Nutzerinteresse in den Bereichen Maßnahmenentwicklung und Standardisierung, Zugang zu kuratierten Fahrszenarien für die technische Entwicklung, Weiterentwicklung szenarienbasierter Testtools sowie Wissenszugewinn in der datenbasierten Begleitforschung identifiziert.

Neben der grafischen Aufarbeitung (vgl. Bild 5) wurden aus der vorangegangenen Analyse für alle mit hoher Relevanz bewertete Stakeholder der wahrgenommene Nutzen durch die Partizipation detailliert aufgeschlüsselt (vgl. Tabelle 2). Ersichtlich hierbei wird die Diversität der einzelnen Nutzerinteressen, welche durch eine Datenbank abgedeckt werden sollten. Diese Diversität bedingt zunächst die nötige Zugangsdifferenzierung, hat aber auch Einfluss auf die möglichen Konstellationen in einem Betreibermodell. Hierzu wird im nächsten Schritt ein Rollenmodell für einen erfolgreichen Datenbankbetrieb entworfen (vgl. Rollenmodell). Dabei wird speziell auf spezifische Einsatzszenarien der verschiedenen Rollen als auch auf die Kernanforderungen zur Rollenbesetzung durch die identifizierten Stakeholder eingegangen.

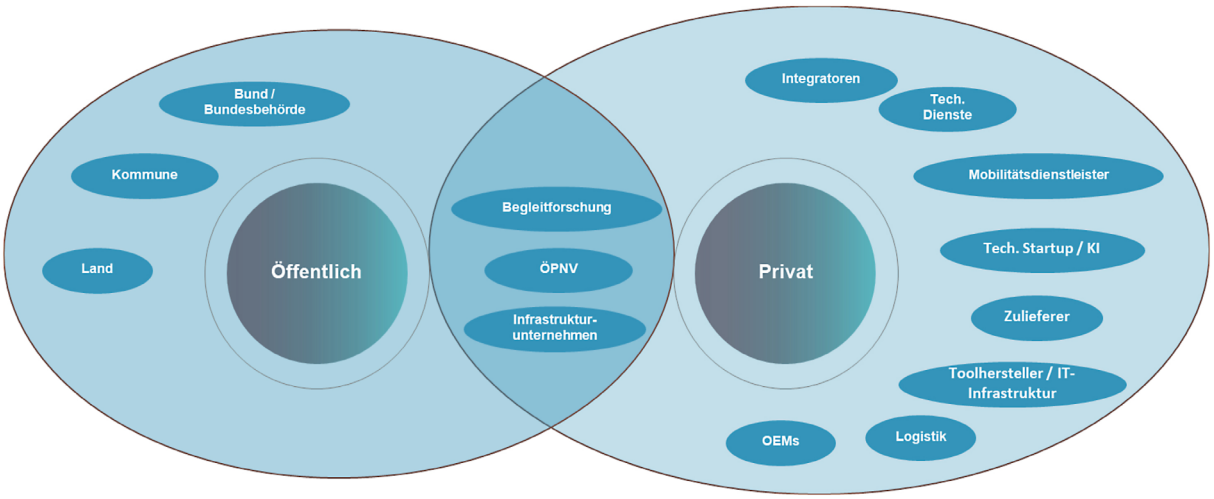


Bild 5: Darstellung des Stakeholdermappings (Quelle: Eigene Darstellung)

Stakeholder	Sektor	Nutzerinteressen für die Szenariendatenbank
Bund (z. B. Verkehrsministerium, BASt, BAuA, KBA)	Öffentlich	Im Rahmen der Gesetzgebung, Typgenehmigung und Marktüberwachung von autonomen Fahrzeugen können verschiedene Bundesbehörden die Informationen der Datenbank nutzen. Für relevante Vorfälle mit autonomen Fahrzeugen können Szenarien erstellt und in die Datenbank eingespeist werden.
Bundesländer	Öffentlich	Im Rahmen der Verkehrssicherungspflicht können Bundesländer und Kommunen die Datenbank zur Planung, Eröffnung und Überprüfung von automatisiertem Fahren nutzen. Informationen der Datenbank können im Kontext zur Erhöhung und Sicherstellung der Verkehrssicherheit und der Verkehrseffizienz verwendet werden.
Kommune	Öffentlich	
Bahn und ÖPNV	Öffentlich/ Privat	Die Bahn und der ÖPNV können die Informationen der Datenbank nutzen, um Innovationen zur Effizienzsteigerung und Kostenreduzierung des Dienstangebotes zu entwickeln oder die Informationen im Zulassungsprozess zu nutzen.
Infrastrukturunternehmen	Öffentlich/ Privat	Infrastrukturunternehmen können durch Auswertungen der zur Verfügung stehenden Datensätze weiteren Infrastruktur- und Anpassungsbedarf identifizieren.
Forschung	Öffentlich/ Privat	Forschungstreibende können die Datenbank zur Validierung ihrer Forschungsergebnisse und als Informationsquelle für neue Forschungen im Bereich Automated Driving oder Fahrerassistenzsystem nutzen.
Tech Startups/KI	Privat	Startups im Bereich der Künstlichen-Intelligenz-Entwicklung können die Szenarien zur Verbesserung der Simulation durch Realdaten nutzen
Toolhersteller/IT-Infrastruktur	Privat	Toolhersteller und IT-Infrastrukturunternehmen können die Informationen zur Weiterentwicklung der Testtool-Automatisierung, Prozessoptimierung und Erweiterung des Geschäftsfeldes nutzen.
Mobilitätsdienstleister	Privat	Mobilitätsdienstleister können die Informationen der Datenbank nutzen, um neue Dienstangebote zu entwickeln und zuzulassen.
Logistikunternehmen	Privat	Logistikunternehmer können die Informationen der Datenbank nutzen, um autonome Lieferfunktionen zu entwickeln und zuzulassen. Daten aus der Datenbank können auch zur Effizienzsteigerung und Erhöhung der Fahrersicherheit genutzt werden.
Technische Dienste	Privat	Im Rahmen der Homologation führen die Technischen Dienste Prüfungen zur System-Genehmigung und Fahrzeugtypgenehmigung durch. Die Prüfung von automatisierten Fahrzeugfunktionen deckt dabei eine Überprüfung des beim Hersteller entwickelten Sicherheitsmanagements und Herstellerdokumentation sowie praktische Prüfungen an den Produkten ab. Informationen der Datenbank können zur Identifikation relevanter Szenario-Parameter herangezogen werden, die in den Prüfungen des Sicherheits- und Validierungskonzepts des Herstellers als auch in eigenen Stichproben-basierten praktischen Prüfszenarien berücksichtigt werden. Im Rahmen der periodisch technischen Überwachung führen die Prüfstellen Überprüfung an Fahrzeugen im Feld durch.
OEMs	Privat	Im Zuge der Entwicklung und Validierung neuer Soft- und Hardware können OEMs und Zulieferer die Informationen der Datenbank zur Identifikation relevanter Szenario-Parameter heranziehen.
Zulieferer	Privat	
Integrator	Privat	Integratoren profitieren durch einen einheitlichen Katalog an Szenarien zur Entwicklung im Bereich Automated Driving und Fahrerassistenzsysteme.

Tab. 2: Nutzerinteresse auf Stakeholderbasis

Experteninterviews: Datenbankbetreiber

Als Teil der Branchenanalyse und als Ergebnis des ersten Stakeholderworkshops konnten weitere Datenbanken mit ähnlichem Fokus auf Nutzergruppen und Zielbild identifiziert werden. Zur tiefen Analyse bereits existierender Lösungsansätze im Bereich der Austauschplattformen für Simulationsszenarien, wurden mit zwei Betreibern der Datenbanken jeweils einstündige Experteninterviews vereinbart und durchgeführt. Bei den bereits existierenden Datenbanken handelt es sich zum einen um SafetyPool, betrieben durch Deepen

AI und WMG, University of Warwick und zum anderen um den ENVITED Marketplace, betrieben durch den eingetragenen Verein Automotive Solution Center for Simulation.

In den Experteninterviews lag der Fokus auf der Analyse der Rollenverteilungen, Wertversprechen, Schlüsselressourcen und Finanzierungsmechanismen der bereits etablierter Szenariendatenbanken. In Tabelle 3 sind die Ergebnisse der Interviews mit SafetyPool und ENVITED übersichtlich zusammengefasst.

	Interviewergebnisse	
	ENVITED	**SafetyPool**
Grundidee	Marktplatz für Vereinsmitglieder zum gebündelten Verkauf und Sammlung von HD-Kartendaten und bereits aufbereiteten Szenarien	Internationaler Datenpool für Simulationsszenarien basierend auf einem Austausch über ein Punktesystem (einstellen:/auslesen – für die Veröffentlichung eigener Szenarien wird ein erweiterter Zugriff auf weitere Szenarien gewährt)
Rollenmodell		
Datenlieferanten	Alle Vereinsmitglieder (Mitgliedsbeitrag) haben die Möglichkeit Szenariendaten in allen gängigen Formaten entweder privat oder öffentlich (zum Verkauf) auf der Datenbank abzulegen. Bisher kann jede Institution, welche eine Expertise in AD/ADAS nachweisen kann, Mitglied werden	Momentan noch kostenloser Zugang und keine Restriktion für Mitglieder (Offen für alle Stakeholdergruppen). Alle Zugangsberechtigten können Szenarien (ODR; OSC) öffentlich oder privat ablegen. Für ein „verkauftes“ Szenario erhält man Punkte, für den „Einkauf“ müssen Punkte bezahlt werden.
Incentivierung	Günstigerer Zugang zu einer Vielzahl an Szenarien. Kostenausgleich durch die Möglichkeit zum Datenverkauf	Das Einspeisen von Szenarien basiert auf einem Punktesystem. Wissen wird gegen Punkte eingespeist, sodass es billiger ist, auf den Inhalt der Datenbank zuzugreifen, sobald selbst Daten geliefert wurden.
Veredler	Die Datensätze werden nach dem Upload nicht nachbearbeitet. Die Anonymisierung und Rohdatenaufbereitung bzw. Szenarienerstellung liegt in der Verantwortung des Datenlieferanten	Bisher ist keine Veredlung der Datensätze als integraler Bestandteil der Datenbank angedacht. Es werden nur bereits erstellte Szenarien zum Tausch angeboten. Deepen AI übernimmt nach unserer Einschätzung mit vorhandener Expertise die Rohdatenaufbereitung vorab. Die gelabelten Rohdaten werden auch von Deepen AI als Szenarien auf die Datenbank geladen.
Betreiber	Automotive Solution Center for Simulation (asc(s)): Übernahme des gesamten Kernbetriebs als Verein mit Fokus auf die Integration der Kompetenzen von Automobil- und Zulieferindustrie, Soft- und Hardwareherstellern, Ingenieurdienstleistern und Forschungseinrichtungen.	Deepen AI und Warwick University: Übernahme des gesamten Kernbetriebs als Spinn-Off Initiative des World Economic Forums und mit Unterstützung durch Drittmittelfinanzierung.
Auditor	Eine Auditierung der Datensätze ist nicht vorgesehen. Der Qualitätsstandart wird über die Rückverfolgung aller gespeicherten daten erreicht (Volle Traceability in einem noch zu entwickelndem Ökosystem)	Eine Auditierung der Datensätze ist nicht vorgesehen. Viele Szenarien wurden von Deepen AI aufbereitet. Für externe Szenarien ist der Prozess der Qualitätssicherung uns nicht bekannt
Nutzer	ENVITED Vereinsmitglieder. Nutzung für Simulation und ODD-Definition	Alle Zugangsberechtigten. Nutzung für ODD-Definition und Prüfung der ODD-relevanten Szenarien, sowie Integration von Policy Makers.
Incentivierung	Günstigerer Zugang zu einer Vielzahl an Szenarien und Möglichkeit zum Datenmanagement	Internationale Abdeckung relevanter Stakeholder. Vielzahl an Szenarien. Labeler als Betreiber.

Tab. 3: Interviewergebnisse – etablierte Szenariendatenbanken anderer Betreiber

	Interviewergebnisse	
	ENVITED	**SafetyPool**
Geschäftsmodell		
Finanzierung	Mitgliedsbeiträge der Vereinsstruktur von asc(s und Transaktionsgebühr die für den Verkauf/Einkauf von Szenarien/Daten anfällt´. Bisher ist der Betrieb nicht gewinnbringend. Es gibt noch keinen Grundstock an öffentlich zugänglichen Szenarien	Finanziert durch die WMW (Universtiy of Warwick), die britische Regierung und Deepen AI. Die Teilnahme ist derzeit kostenlos. Inklusive Teilnahme. Keine monetäre Transaktion zur Teilnahme erforderlich.
Wertschöpfung	Momentan defizitärer Betrieb. Skalierung zu hoher Varietät an Szenarien ermöglicht Kostendeckung und strategischen Marktvorteil sowie eine Schlüsselrolle in der Standardisierung.	Momentan keine öffentlich zugänglichen Szenarien und damit keine Wertschöpfung. Bisher reine Ausgaben. Geplante Skalierung zu international größter Szenariendatenbank mit Unterstützung des World Economic Forums und unter Einbezug der internationalen Auto-Motive-Community
Wertversprechen	Vergünstigter Zugang zu einer Vielzahl simulationsrelevanter Daten	Zeitersparnis und Sicherheitsvalidierung von AD/ADAS Systemen

Tab. 3: Interviewergebnisse – etablierte Szenariendatenbanken anderer Betreiber (Fortsetzung)

Beide Datenbanken decken bereits in der konzeptionellen und praktischen Ausarbeitung ein breites Nutzerinteresse der oben identifizierten Stakeholder ab. Zwar bieten bisher keine der beiden Lösungen effektiv öffentlich geteilte Szenarien zum Tausch oder Verkauf an, jedoch wird ersichtlich, dass das Zielbild einer möglichen Austauschplattform für simulationsfähige Szenarien teilweise durch bereits existierende Lösungen abgedeckt ist. Zusätzlich lässt sich ableiten, dass bisher nicht alle der oben genannten Nutzerbedürfnisse vollumfänglich bedient werden.

Probleme könnten langfristig durch national geltende aber international nicht vollumfänglich umgesetzte Datenschutzverordnungen entstehen. Durch eine Vereinsstruktur auf deutscher Ebene auf der anderen Seite wird der Fokus auf eine kleinere Nutzergruppe im OEM-nahen Bereich gelegt, während Nutzerinteressen der Forschung oder anderen Akteuren mit einem nicht-kommerziellen Interesse schwereren Zugang zu frei verfügbaren Datensätzen haben. Eine detaillierte Analyse der Nutzerinteressenabdeckung durch bereits existierende Lösungen und der Zusatznutzen einer neuen Szenariendatenbank wird in Anreizevaluation und Geschäfts- und Betreibermodellvorschläge unter Inbezugnahme des entwickelten Use-Cases ausgeführt.

3.1.3 Analyse der rechtlichen Rahmenbedingungen

Unter Einbindung des Konsortiums und der Ergebnisse der zwei Stakeholderworkshops wurde der rechtliche Nutzen der Datenbank und rechtliche Fragestellungen in den relevanten Rechtsgebieten (Datenschutz, Datensicherheit, Datenzugang, Datennutzung) diskutiert und anschließend umfangreich gutachterlich und in einem Rechtsgutachten aufbereitet. Zudem wurde ausblickhaft auch die europäische und nationale Datenstrategie betrachtet und bewertet. Die umfassende Analyse der rechtlichen Rahmenbedingungen befindet sich im angehängten Rechtsgutachten (Anhang A2).

Rechtliche Bedeutsamkeit der Szenariendatenbank

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.

Wechselwirkung zwischen Fahrzeugzulassungsrecht und der Szenariendatenbank

Zwischen der Fahrzeugzulassung 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 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 automatisierter Fahrfunktionen

Automatisiertes Fahren wird vom gegenwärtigen Rechtsrahmen nur zum Teil erfasst.

Die Szenariendatenbank könnte im Rahmen der Zulässigkeit automatisierter Fahrfunktionen nach dem StVG als Sicherheitsnachweis im Rahmen der Zulassung bedeutsam werden, und den Absicherungsprozess erheblich vereinfachen und erleichtern. Der automatisierungsbedingte Verantwortungswechsel vom Menschen 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.

Datenspeicherungs- und Übermittlungspflichten im StVG mit Blick auf automatisierte Fahrfunktionen

Im StVG, konkret in § 63 a, 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 Fahrzeugführer und bei systemseitigen Aufforderungen zur Übernahme der Fahrzeugsteuerung oder technischen Störungen des Systems geregelt, vgl. § 63 a Abs. 1 StVG. Nicht geregelt, sondern gemäß § 63 b S. 1 Nr. 1 StVG an den Verordnungsgeber delegiert, wurden der Ort sowie die Art und Weise der Datenspeicherung.

Feinsteuerung mit Blick auf geltendes Recht

Der geltende Rechtsrahmen ist mit Blick auf automatisierte Fahrfunktionen schwerfällig und zum Teil lückenhaft, unter anderem aufgrund des Fehlens ausreichender Informationen. Die Szenariendatenbank könnte als Informationsgrundlage dienen und helfen Gesetzeslücken auszufüllen und passende Vorschriften für die Besonderheiten automatisierter Systeme zu entwickeln.

Regelungsvorhaben zum autonomen Fahren im Lichte der Szenariendatenbank

Das Gesetz zum autonomen Fahren hat im Jahr 2021 Datenspeicherungs- und Übermittlungspflichten an öffentliche Stellen eingeführt.

Mit Blick auf diese Regelung könnte der Szenariendatenbank eine zentrale Rolle im Rahmen der Typprüfung auf Grundlage des neu kreierten Regelzulassungsverfahrens zu-

kommen. Die Szenariendatenbank könnte als Informationsgrundlage zur Erstellung des erforderlichen Sicherheitskonzepts herangezogen werden.

Datenerhebungs- und Übermittlungspflichten

Daneben könnten aufgrund der neuen Regelungen die zulässige Erhebung von Herstellerdaten und damit die zulässige Fusion wichtiger sicherheitsrelevanter Informationen ermöglicht werden.

Das neue Gesetz sieht halterseitige Datenspeicherungs- und Übermittlungspflichten an das Kraftfahrtbundesamt und die für die Genehmigung der Betriebsbereiche zuständigen Landesbehörden in beträchtlichem Umfang vor, vgl. § 1 g StVG. Außerdem wird das Kraftfahrtbundesamt gemäß § 1 g Abs. 5 S. 1 StVG ermächtigt, die Daten, soweit der Personenbezug aufgehoben wird „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 zu machen (und durch jene zu vorbenannten Zwecken verwendet zu werden), vgl. § 1 g Abs. 5 S. 2 StVG. Insoweit besteht ein Anspruch von Forschungseinrichtungen auf ermessensfehlerfreie Entscheidung[1] 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 Abs. 1 DSGVO.

Datenschutzrecht

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).

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

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.[2]

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.[3]

---

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

2 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.

3 Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen" Version 1.1 2020, S. 89.

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. Die Möglichkeit des Personenbezugs besteht bei allen durch die OEMS 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.[4]

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.

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 ausgeführter 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 Erhebung von personenbezogenen Daten als auch 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.[5] 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. 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. Dies wird je nach Verantwortlichem unterschiedlich beantwortet, entscheidend ist das „mobilisierte Zusatzwissen“ der einzelnen Verantwortlichen. Bei der Bewertung sind die, während der Speicherdauer erwartbaren, technischen Möglichkeiten zu berücksichtigen. Solange die Person re-identifiziert werden

---

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

5 Ernst in Paal, Boris/Pauly, Daniel, DS-GVO BDSG, Art.4 DSGVO, 3. Auflage, 2021, Rn. 49.

kann, liegt lediglich Pseudonymisierung vor, die DSGVO bleibt anwendbar. Die Anonymisierung stellt insoweit ein Mehr zur Pseudonymisierung dar. Echte Anonymisierung ist, auf Grund des Anstiegs von Rechenleistung und Speicherkapazitäten, welche die Verknüpfung von Daten vereinfachen, in der Praxis kaum noch zu bewerkstelligen. Die in dem Zusammenhang häufig generierte bloße „faktische Anonymität" führt dazu, dass die DSGVO anwendbar bleibt, 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 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. Stärken und Schwächen möglicher Techniken hat die Art.29-Datenschutzarbeitsgemeinschaft in einer Stellungnahme zusammengefasst.

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. Praktisch verbleibt aufgrund der einzelfallabhängigen Anforderungen immer ein gewisses Restrisiko.

Relevante Rechtfertigungstatbestände mit Blick auf die in die Datenbank eingespeisten Forschungsdaten

Die Verarbeitung personenbezogener Daten ist regelmäßig unzulässig und nur ausnahmsweise dann rechtmäßig, wenn einer der in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbestände greift. Relevante Rechtfertigungsgründe mit Blick auf die Szenariendatenbank sind die Einwilligung, die Erforderlichkeit zur Vertragserfüllung und die Interessenabwägung.

Freiwillige, informierte und bestimmte Einwilligung gemäß Art. 6 Abs. 1, S. 1, lit. a DSGVO

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.[6] Die Einwilligung ist formfrei gebunden und kann daher auch in elektronischer Form erfolgen.[7] Wegen der Nachweispflicht des Verwenders gem. Art. 7 Abs. 1 DSGVO ist allerdings die Speicherung der Einwilligung zweckmäßig. Darüber hinaus muss die Einwilligung freiwillig erteilt werden.[8] 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 Einwilli-

---

6 BeckOK DatenschutzR/Albers/Veit, 31. Ed 1.11.2019, Art. 6 DSGVO Rn. 24.
7 Kotter „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?", 2019, S. 33.
8 Metzger „Digitale Mobilität – Verträge über Nutzerdaten", GRUR 2019, 129 (131).

gungserklärung erfassen können.[9] 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.[10] 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[11] 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, vielgestaltige Mobilitätsverträge zwischen einer Vielzahl von Vertragsparteien auffächert, ist eine unterschiedliche datenschutzrechtliche Beurteilung erforderlich.[12]

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[13], teilweise aber auch integriert in den Kaufvertrag[14]) und Vertragspartner (z. B. Drittanbieter), welche neben die klassischen Vertragsschwerpunkte (Kauf, Miete Leasing etc.) und Vertragspartner (Hersteller, Händler, Käufer bzw. Leasingnehmer, Mieter usw.) treten. [15]

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.[16]

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.[17] Zwar kann die Einwilligung stellvertretend erteilt

---

9 Kotter „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?“ 2019, S. 33.

10 Lüdemann „Connected Cars - Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück“, ZD 2015, 247 (253).

11 Steege, „Ist die DSGVO zeitgemäß für das autonome Fahren? Datenschutzrechtliche Aspekte der Entwicklung, Erprobung und Nutzung automatisierter und autonomer Fahrzeuge“, MMR 2019, 509 (511).

12 Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 60 f.

13 „Mercedes-Me“ (Mercedes Benz) und „On-Star“ (Opel), vgl. Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62.

14 z. B. „BMW-Connected-Drive-Vertrag“, vgl. Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62 f.

15 Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel,/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 60 ff.

16 Brink/Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 83.

17 Brink/Herfelder, “Einwilligung und Vertragsdatenverarbeitung“ “ in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 84.

werden, dies setzt aber die Kenntnis des Vertretenen voraus, was mit Blick auf sämtliche zukünftige Nutzer nicht durchführbar ist.[18]

Denkbar erscheint es, die Einwilligung für den in Anspruch genommenen Service vor jedem Fahrtantritt durch den jeweiligen Nutzer einzuholen,[19] oder für die verschiedenen Fahrzeugnutzer (die anders als der Fahrzeugerwerber nicht vertraglich einwilligen können) Fahrprofile im Fahrzeug anzulegen, deren persönliche Einstellungen jederzeit durch die Nutzer geändert werden können[20].

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 (schutzwürdige) Vertrauen geweckt wurde, dass die Datenverarbeitung nur im Rahmen der Einwilligung erfolgt.[21] Aus diesem Grund ist ein Hinweis sinnvoll, dass die Daten auch nach Wegfallen der Einwilligung auf anderer Grundlage verarbeitet werden können.[22]

Erforderlichkeit der Verarbeitung für die Erfüllung eines Vertrags, mit der betroffenen Person gemäß Art. 6 Abs. 1 S. 1 lit. b DSGVO

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.[23] Welche Datenverarbeitungen als erforderlich anzusehen sind, ist im konkreten Fall im Rahmen einer umfassenden Interessenabwägung zu ermitteln.[24]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.[25] Dies ist etwa der Fall, wenn die Datenverarbeitung als solche erst die Fahrfunktion ermöglicht.[26] Anders verhält es sich mit Blick auf Datenverarbeitungen, welche zusätzliche personenbezogene Daten zwecks Personalisierung von Leistungen generieren wollen.[27] Handelt es sich um sensible Daten, so ist eine Rechtfertigung der Verarbeitung gemäß Art. 6 Abs. 1 lit. b DSGVO ausgeschlossen.[28] Als

---

18 Brink/Herfelder, "Einwilligung und Vertragsdatenverarbeitung" " in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 84.

19 Brink/Herfelder, "Einwilligung und Vertragsdatenverarbeitung" " in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 85.

20 Brink/Herfelder, "Einwilligung und Vertragsdatenverarbeitung" " in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 86.

21 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz", 2. Auflage 2020, S. 28.

22 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz", 2. Auflage 2020, S. 28.

23 Brink/Herfelder, "Einwilligung und Vertragsdatenverarbeitung" " in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 77.

24 BeckOK DatenschutzR/Albers/Veit, 31. Ed 1.11.2019, Art. 6 DSGVO Rn. 32.

25 Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto" in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62 f.

26 Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto" in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 64.

27 Buchner „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto" in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 73.

28 Art. 9 Nr. 1 DSGVO.

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.

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

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.[29] Denkbare berechtigte Interessen sind zum einen die gemeinschaftsnützliche Erhöhung der Verkehrssicherheit[30] 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.[31] 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.

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.[32] Schließlich bestehen auch bereichsspezifische Vorgaben für Forschungsdaten, die den allgemeinen Regeln unter Umständen als speziellere Regeln vorgehen,[33] 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.[34] 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 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.[35] Diese Garantien sollen gewährleisten, dass technische und organisatorische

---

29 Albers/Veit, BeckOK, Datenschutzrecht, Art. 6 DSGVO Rn. 52.

30 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).

31 Spindler in Schuster/Spindler, Recht der elektronischen Medien, 4. Auflage 2019, Art. 6 DSGVO Rn. 13.

32 Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen“ Version 1.1 2020, S. 89.

33 Ebenda.

34 Bundesministerium für Gesundheit „Wissenschaftliches Gutachten „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen“ Version 1.1 2020, S. 89.

35 Roßnagel „Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (159).

Maßnahmen (z. B. die Pseudonymisierung[36] oder Anonymisierung[37]) 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“[38] versteht, zurückgegriffen werden.[39]

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.

Die datenschutzrechtliche Besserstellung gegenüber zu sonstigen Zwecken erhobenen Daten greift daher nur, wenn die Forschung, der gemeinschaftsnützlichen zweckgebundenen Suche nach der Wahrheit dient.[40] Datenschutzrechtliche Privilegierungen greifen zudem nur für unabhängige Forschung,[41] da nur dann der Erkenntnisgewinn zum Wohle der Allgemeinheit im Zentrum steht und entsprechende Beschränkungen zu rechtfertigen vermag.[42] 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.[43]

Auch die Verfolgung politischer Interessen darf den freien wissenschaftlichen Erkenntnisprozess zu Gemeinwohlzwecken, nicht dominieren.

Weiterhin schließt die fehlende wissenschaftliche Methodik die Privilegierung aus.[44] 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.[45]

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 ab-

---

36 Vgl. Art. 89 Abs. 1, S. 3 DSGVO.
37 Vgl. Art. 89 Abs. 1, S. 4 DSGVO.
38 BVerfGE 35, 79.
39 Rossnagel „Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (158).
40 Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20.).
41 Krohm in Gola/Heckmann, 13. Aufl. 2019, § 27 BDSG Rn. 14.
42 Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (19).
43 Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (19 f.).
44 Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20.).
45 Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20.).

hängt, insbesondere davon, welche personenbezogenen Daten verarbeitet werden und wer an dem Prozess beteiligt ist.[46]

Denkbare Maßnahmen, welche als gesetzliche Gebote Niederschlag gefunden haben,[47] 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).[48]

Einzelne Privilegierungen

Einschränkungen bzw. Ausnahmen von Betroffenenrechten bestehen etwa mit Blick auf die Zweckbindung für die Weiterverarbeitung für Forschungszwecke, [49] für die Speicherbegrenzung[50], den Bestimmtheitsgrundsatz für die Einwilligung,[51] das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten,[52], die Informations-[53] und Löschpflicht[54].[55]

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,[56] da sich Forschungsfragen- und -ziele nicht immer konkret im Vorhinein erfassen lassen.[57] 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.[58]

Privilegierung der Zweckbindung

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 ermög-

---

46 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 23.
47 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 19.
48 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 23.
49 Vgl. Art. 5 Abs. 1, lit. b DSGVO.
50 Vgl. Art. 5 Abs. 1, lit. e DSGVO.
51 Erwägungsgrund 33 DSGVO.
52 Art. 9 Abs. 2, lit. j DSGVO.
53 Art. 14 Abs. 5, lit. b DSGVO.
54 Art. 17 Abs. 3, lit. d DSGVO.
55 Roßnagel „Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (159).
56 Erwägungsgrund 33 S. 1 DSGVO.
57 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 21.
58 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.

licht aber nicht, dass sich der Verantwortliche für die Forschungsnutzung auf die Rechtsgrundlage des Primärzwecks berufen könnte,[59] vielmehr ist eine eigenständige Rechtfertigung der Sekundärverarbeitung zu Forschungszwecken erforderlich.

Eingeschränktes Widerspruchsrecht bei Verarbeitungen von Forschungsdaten gemäß Art. 21 Abs. 6 DSGVO

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 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 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[60].

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,[61] 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[62]. Davon hat der nationale Gesetzgeber in § 27 Abs. 2 S. 1 BDSG Gebrauch gemacht.[63]

Haftung für Datenschutzverstöße

Die haftungsrechtliche Verantwortlichkeit weist der DSGVO-Compliance einen besonderen Stellenwert zu. Die Haftung für Datenschutzverstöße folgt neben allgemeinem Vertrags- und

---

59 Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (21).
60 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 25.
61 Rossnagel „Datenschutz in der Forschung Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen”, ZD 2019, 157 (159).
62 Vgl. Art. 89 Abs. 2 DSGVO.
63 Krohm in Gola/Heckmann, 13. Aufl. 2019, BDSG § 27 Rn. 6.

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.[64]

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[65]. Die Exkulpationsmöglichkeit gem. Art. 82 Abs. 3 gilt nicht beim Handeln eigener Mitarbeiter.[66] Auch eine ordnungsgemäße Überwachung seiner Mitarbeiter vermag den Verantwortlichen nicht zu befreien, eine Exkulpationsmöglichkeit, welche der Regelung in § 831 BGB entspricht, fehlt.[67] Ein vertraglicher Haftungsausschluss des Art. 82 DSGVO kommt selbst bei leichter Fahrlässigkeit nicht in Betracht.[68] Selbst die Einhaltung zertifizierter und genehmigte Verhaltensregeln vermögen die Haftung nicht auszuschließen,[69] wohl aber zu reduzieren.

Das Einschalten eines Auftragsverarbeiters gemäß Art. 28 DSGVO als „verlängerter Arm des Verantwortlichen"[70] verlagert eine etwaige Schadensersatzpflicht gesamtschuldnerisch[71], entsprechend dem Verantwortungsanteil,[72] auf mehrere Pflichtige. Die Delegierung von datenschutzrechtlichen Pflichten an den Auftragsverarbeiter vermag allerdings keine Enthaftung herbeizuführen. Vielmehr bleiben neben der Begründung neuer Pflichten bei dem Übernehmer[73] gewisse Überwachungspflichten bestehen,[74] deren Verletzung haftungsbegründend wirkt (bspw. Auswahl geeigneter Mitarbeiter, Organisation und Aufsicht z. B. des Auftragsverarbeitenden,[75] sowie Schulung und Kontrolle).

Datenzugang und -weiterverwendung

Weiterhin ist der Rechtsrahmen des Datenzugangs und -weiterverwendung für die Schaffung der Szenariendatenbank relevant. Zukünftige Betreiber der Szenariendatenbank können auf Grundlage etwaiger bestehender Datenzugangs- und -weiterverwendungsansprüche Daten zur Szenarienbildung einsehen und verwerten.

---

64 Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1.Auflage 2019, Art. 82 DSGVO Rn. 22.
65 Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 82 Rn. 23.
66 Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 82 Rn. 23.
67 Wybitul/Haß/Albrecht „Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung", erschienen in NJW 2018, 113 (116).
68 Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1.Auflage 2019, Art. 82 DSGVO Rn. 25.
69 Böhm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1.Auflage 2019, Art. 82 DSGVO Rn. 21.
70 Martini in Paal/Pauly/Martini, DSGVO, BDSG, 3. Aufl. 2021, Art. 28 DSGVO Rn. 2.
71 Vgl. Art. 82 Abs. 4 DSGVO.
72 Vgl. Art. 82 Abs. 5 DSGVO.
73 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).
74 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).
75 Paal „Schadensersatzansprüche bei Datenschutzverstößen - Voraussetzungen und Probleme des Art. 82 DSGVO", MMR 2020, 14 (17)

Hierbei muss zwischen verschiedenen möglichen Akteurskonstellationen unterschieden werden. Etwaige Datenzugangs- und -weiterverwendungsansprüche sind zunächst davon abhängig, ob jeweils private oder öffentliche Anspruchsteller bzw. -gegner vorliegen. Insoweit hat das zukünftige Betreibermodell Auswirkungen auf die Anspruchsmöglichkeiten.

Datenzugangsansprüche privater Akteure ergeben sich gegenüber öffentlichen Stellen über die entsprechenden Gesetze des Bundes oder der Bundesländer, wobei diese jedoch aufgrund gegenläufiger Gründe, etwa dem Schutz personenbezogener Daten, des geistigen Eigentums, von Geschäfts- und Betriebsgeheimnissen, sowie öffentlich Belangen, eingeschränkt sein können.

Gegenüber anderen privaten Akteuren kann der Zugang freiwillig erfolgen oder unter bestimmten Voraussetzungen durch gesetzliche Ansprüche erzwungen werden. [76]

In der Konstellation, dass der Staat Datenzugang von einem privaten Akteur verlangt ist zu sehen, dass dies für gewöhnlich durch Überlassung der Daten durch die Unternehmen auf Grund freiwilliger Vereinbarungen geschieht. [77]

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.

Die Authentizität, Vertraulichkeit und Integrität der verwendeten Datensätze und Verarbeitungsprozesse ist 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.

Ein einheitliches Gesetz, welches sämtliche Aspekte der IT-Sicherheit regelt, gibt es bisher nicht, vielmehr werden in verschiedenen Gesetzen punktuell Regelungen getroffen.

Zentrales Regelwerk ist das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). 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.[78]

---

[76] Harti/Ludin, Recht der Datenzugänge, MMR 2021, 536 (536).
[77] Richter „Zugang des Staates zu Daten der Privatwirtschaft“, ZRP 2020, 245.
[78] Riehm/Meier „Rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit“, MMR 2020, 571 (573).

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 oder Standards fehlen aufgrund der Neuartigkeit der Datenbank.

Rechtsform der Datenbank

Personen- und Kapitalgesellschaften
Im Rahmen der rechtlichen Analyse wurden zudem mögliche Rechtsformen der Szenariendatenbank anhand von verschiedenen Kriterien wie Haftung und Finanzierung erörtert und die Vor- und Nachteile der einzelnen Kapital- und Personengesellschaften gegeneinander abgewogen. Dabei erwiesen sich die Rechtsformen der Gesellschaft bürgerlichen Rechts (GbR), Offenen Handelsgesellschaft (OHG) und Kommanditgesellschaft (KG) als nicht praktikabel, da sie umfangreiche Haftungsansprüche auch in das Privatvermögen der Gesellschafter begründen.

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)
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

Tab. 4: 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
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.[79]	Besonderheiten: Auseinanderfallen der Gesellschafter in persönliche Haftende und Haftungsbeschränkte. Auch diese Rechtsform gilt nur für Kaufleute.	Besonderheiten: Umfangreiche Formalitäten und hohe Gründungskosten[80]	Besonderheiten: Unter bestimmten Voraussetzungen kann eine GmbH auch „gemeinnützig“ sein, mit den entsprechenden Vorteilen (Steuerliche Vergünstigungen, Image etc.)

Tab. 4: Überblick über relevante Kapital- und Personengesellschaften (Fortsetzung)

Verein

Neben den Personen- und Kapitalgesellschaften besteht auch die Möglichkeit, die Datenbank als Verein zu betreiben.

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. Gemäß § 22 BGB erlangt ein Verein, dessen Zweck nicht auf wirtschaftlichen Geschäftsbetrieb gerichtet ist, die Rechtsfähigkeit durch Eintragung in das Vereinsregister. 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.[81] 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. [82] Zur Frage des Nebenzweckprivilegs wird auf das ergänzende rechtswissenschaftliche Gutachten verwiesen.

Des Weiteren wird bei einem Verein danach unterschieden, ob er in das Vereinsregister eingetragen ist oder nicht. 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, welche im Namen des Vereins abgeschlossen werden

[79] Sprau in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 705 Rn. 6.
[80] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, Einf v § 21, Rn. 14.
[81] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 21 Rn. 2 ff.
[82] Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018, § 21 Rn. 2 ff.

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.[83] Für die Szenariendatenbank ist daher die Beteiligung der Bundesanstalt für Straßenwesen als Vertretung der Bundesrepublik Deutschland, die als juristische Person des öffentlichen Rechts beteiligt sein kann nicht ausgeschlossen.

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.[84] Eine Vereinsgründung erfordert, in Abgrenzung zu der Gründung einer GmbH, darüber hinaus kein Stammkapital 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.

GmbH	**Eingetragener Verein**
Komplexere Bilanzierungs- und Buchführungspflichten	Einfache Einnahmen-Überschuss-Abrechnung
Prinzip der Einstimmigkeit, Entscheidungsbefugnisse abhängig von Anteilen langfristig effizienter	Mehrheitsprinzip, Einfache, basisdemokratische Entscheidungsfindung langfristig wenig 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

Tab. 5: Vergleich GmbH/eingetragener Verein

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 sieben 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).[85]

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 sei-

[83] BMJV – Leitfaden zum Vereinsrecht 2016, S. 14.
[84] Schöpflin in BeckOK BGB, 58. Edition 2021, § 21 Rn. 29.
[85] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 51 Rn. 9.

ne 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 Daten auswirkt. Schließlich verspricht sich die Gemeinnützigkeit auch positiv auf datenschutzrechtliche Interessensabwägungen auszuwirken. Nachteilig wirkt sich indes das Gewinnausschüttungsverbot[86] 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.[87]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.[88]

§ 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. [89] 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.[90]

---

86 Helm/Haaf in Beck‘sches Handbuch der GmbH, 6. Auflage 2021, § 24 Rn. 55.
87 Koenig in Koenig, Abgabenordnung, 4. Auflage, 2021 § 52 Rn. 9.
88 Koenig in Koenig, Abgabenordnung, 4. Auflage, 2021 § 52 Rn. 9.
89 BVerfG 1 BvB 2/51, BVerfGE 5, 85 (146 f.)).
90 Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 52 Rn. 29.

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.[91] 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.

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.[92]

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.[93] 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. [94] Demgegenüber würde eine Körperschaft nur mittelbar handeln, wenn sie die gemeinnützigen Zwecke eines anderen Steuerpflichtigen unterstützen würde.

GIDAS-Datenbank

Weiterhin erfolgte ein diesbezüglicher Austausch mit vergleichbaren Forschungsprojekten. Das Forschungsprojekt der GIDAS-Datenbank fußt beispielsweise rechtlich auf einem bilateralen Kooperationsvertrag zwischen der BASt und der Forschungsvereinigung für Automobiltechnik e.V. (FAT). Die einzelnen beteiligten Unternehmen (Hersteller und Zu-

---

[91] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 52 Rn. 36. Dazu auch im Folgenden.
[92] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 55 Rn. 6.
[93] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 56 Rn. 1.
[94] Koenig in Koenig, Abgabenordnung, 4. Auflage 2021, § 57 Rn.2.

lieferer) sind daher nur mittelbar als Zusammenschluss in Gestalt des FAT beteiligt, sodass Haftungsrisiken für sie nicht bestehen. 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[95] indes Rechtsunsicherheit und ist mit großem vertraglichem Aufwand verbunden.

Zudem besteht die Gefahr, dass die Kooperation nach Außen als Einheit auftritt,[96] mit der Folge, dass eine Außen-GbR im Sinne von § 705 BGB vorliegt, für deren Verbindlichkeit die Partner gemäß § 128 HGB analog unbeschränkt haften[97].

Zwischenfazit

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 und einer nicht-kommerziell-orientierten Akteursstruktur im Kernbetrieb aufgefangen wird.

Kartellrechtliche Vorgaben

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.[98] 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.[99]

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).

Im Ergebnis kann offenbleiben, ob die jeweilige Kooperation unter den Kartellbegriff fällt, wenn eine Ausnahme greift. Von dem Verbot wettbewerbsbeschränkender Vereinbarun-

---

95 Eberbach, „Eine Rechtsform für Wissenschaftskooperationen –Ausgangspunkte und Grundlagen“ 02/2018, 51 (66).

96 Geis, · „Forschungskooperationen: Öffentliches oder Zivilrecht? – Positionsbestimmungen und Regelungszuständigkeiten“, 2/2018, 77 (81).

97 Eberbach, „Eine Rechtsform für Wissenschaftskooperationen –Ausgangspunkte und Grundlagen“ 02/2018, 51 (57).

98 Oppermann „Marktrecht“ in Oppermann/Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen“, 2. Auflage 2020 Rn. 48.

99 Mattfeld in Gummert/Weipert, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 1 f.

gen 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.[100]

Eine entsprechende Gruppenfreistellungsverordnung existiert auch für den Forschungsbereich (im Folgenden: GFV-Forschung).[101] Gemäß Art. 2 Abs. 1 GFV-Forschung iVm Art. Abs. 3 AEUV und § 2 Abs. 2 S. 1 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.[102] 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.[103]Das Risiko umfasst auch die Veränderungen von Marktverhältnissen und rechtlichen Einordnungen.[104] In dem Zusammenhang ist auch auf die limitierte Geltungsdauer der GFV-Forschung bis Ende 2022 hinzuweisen. Daher empfiehlt sich eine regelmäßige Überprüfung der Freistellungsvoraussetzungen.

3.2 Rollenmodell

Auf die Ergebnisse aus der Analyse der Marktarchitektur aufbauend wurde ein schematisches Rollenmodell für einen erfolgreichen Datenbankbetrieb zunächst intern abgeleitete und im weiteren Verlauf in zwei Stakeholderworkshops validiert. Den Verlauf der Daten über die fünf als notwendigste identifizierte Rollen, Datenlieferant, Veredler, Betreiber, Auditor und Nutzer, sind in Bild 6 dargestellt. Dabei steht zu Beginn des Rollenmodells der

---

[100] Mattfeld in Gummert/Weipert, Münchener Handbuch des Gesellschaftsrechts, Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 13.

[101] 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).

[102] Erwägungsgrund 6 GFV-Forschung.

[103] Mattfeld in Münchener Handbuch des Gesellschaftsrechts Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 15.

[104] Mattfeld in Münchener Handbuch des Gesellschaftsrechts Bd. 1, 5. Auflage 2019, § 33 Kartelle, zulässige Kooperationsformen Rn. 15.

Datenlieferant, welcher Daten zur Einspeisung in die Szenariendatenbank liefert. Sofern dies Rohdaten mit möglichem Personenbezug, wie beispielsweise Kameradaten, sind, bedarf es einer Anonymisierung und Aufbereitung der Daten zur Szenarienerstellung. Dieser Prozess wird unter der Rolle des Veredlers gesammelt. Der Betreiber sammelt diese verarbeiteten Simulationsszenarien und lässt die DSGVO-Konformität durch einen Auditor sicherstellen. Am Ende des Rollenmodells steht der Nutzer welcher Simulationsszenarien erwirbt. Er kann gleichzeitig auch als Datenlieferant fungieren. Im Folgenden werden die Entwicklung des Rollenmodells sowie resultierende Anforderungen an die einzelnen Rollen näher beleuchtet.

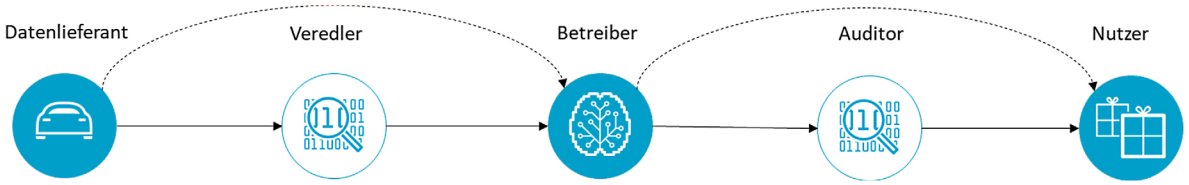


Bild 6: Darstellung des Rollenmodells (Quelle: Eigene Darstellung)

3.2.1 Entwicklung des Rollenmodells

Um die als relevant identifizierten Stakeholder in den Kontext eines möglichen Betreibermodells zu setzen, wird im Folgenden ein Rollenmodell für einen erfolgreichen Datenbankbetrieb entworfen. Hierfür werden zunächst die einzelnen Rollen definiert, die jeweiligen Verantwortungen beschrieben und erste Anforderungen an die jeweiligen Rollen in einem hypothetischen Betrieb definiert (vgl. Tabelle 6).

Auf die erarbeitete Ausdifferenzierung der Rollen aufbauend, wurden im zweiten Schritt detaillierte rollenspezifische Anforderungen auf Basis verschiedener Einsatzszenarien aus

Nutzerrolle	Aufgabe
Datenlieferant	Der Datenlieferant stellt in der Datenbank von ihm aufgenommene bzw. aufbereitete Daten zur Erstellung der Szenarien zur Verfügung. Die Incentivierung des Datenlieferanten sowie die Anforderungen an seine Rolle hängen von seinem Input ab. Drei unterschiedliche Inputs sind hier vorstellbar: Rohdaten/Objektlisten, Rohdaten-Szenarien und Simulationsszenarien.
Veredler	Je nachdem, welche Einsätze/Eingabe in die Datenbank eingehen, ist der Veredler für die Anonymisierung, das Labelling oder die Erstellung der Szenarien zuständig. Die Rolle des Veredlers ermöglicht, die Eingaben in nutzbare Szenarien umzuwandeln.
Betreiber	Der Betreiber stellt sicher, dass die Datenbank korrekt funktioniert. Seine Aufgaben reichen vom Zugriffmanagement und Datamanagement über die Partnerkoordination und Incentivierung bis zum IT-Support der Datenbank. Der Betreiber ist auch für die Konformität in rechtlichen und ethischen Fragenstellungen verantwortlich. Die einzelnen Aufgaben müssen nicht durch einen Stakeholder erledigt werden, sondern können auch vom Betreiber beauftragt werden.
Auditor	Der Auditor bescheinigt, dass die Anonymisierung der Rohdaten im Einklang mit den Rechtsakten und Standards in Bezug auf Datenschutz (z. B. DSGVO) und IT-Sicherheit (z. B. ISO 27001) erfolgt. Auch könnte eine weitere Aufgabe des Auditors die Qualitätsprüfung der Rohdaten, veredelten Daten und der Szenarien sein. Diese ist in der Grundausgestaltung vorerst aber noch nicht vorgesehen.
Nutzer	Der Nutzer ist der Endverbraucher der Simulationsszenarien. Die Interessen der Nutzer sind vielfältig und hängen von der Art des Stakeholders ab, der die Nutzerrolle übernimmt. Für OEMs und Zulieferer, kann die Zulassung autonomer Fahrfunktionen das Interesse sein, während für öffentliche Institutionen die Verbesserung des Verkehrs oder die Bewertung der Verkehrssicherheitsmaßnahmen ein wichtiger Anreiz ist.

Tab. 6: Rollenbeschreibung und Aufgabendefinition

den Ergebnissen der vorrangegangenen Arbeitsschritte abgeleitet, sowie die Incentivierung für die rollenspezifischen Akteure vorab erörtert. Die ausdifferenzierten Rollen sind in den folgenden fünf Abbildungen als Baumdiagramme dargestellt. Die Ergebnisse wurden im Anschluss durch eine Expertenbefragung vertieft, validiert und angepasst. Die validierten Ergebnisse wurden in Bezug zur Anreizevaluation gesetzt und in dem darauf aufbauenden zweiten Stakeholderworkshop mit den Interessensgruppen diskutiert und erweitert (vgl. Anreizevaluation und Geschäfts- und Betreibermodellvorschläge). Der dort detailliert beschriebene Use-Case (vgl. Use-Case-Entwicklung) baut auf die Schlussfolgerungen des folgenden Modells auf und summiert die Erkenntnisse in einem expliziten Anwendungsfall.

3.2.2 Datenlieferant

Der Datenlieferant kann sowohl aus dem öffentlichen, privaten als auch öffentlich-privaten (semi-öffentlichen) Bereich kommen und liefert Daten, welche für die Erstellung von Simulationsszenarien benötigt werden. Es wurden drei Betriebsszenarien zur Einspeisung von Datensätzen durch verschiedene Datenlieferanten identifiziert: Rohdaten (Messdaten aus Kamera, GPS, Lidar, Radar und weitere Aufnahmen des Fahrzeugbusses oder der Infrastruktur), Objektlisten, Rohdaten-Szenarien und simulationsfähige Szenarien (vgl. Bild 7). Die technischen Anforderungen an die Rollen ergeben sich aus den einzuspeisenden Datenformaten. Folglich muss der jeweilige Datenlieferant für die jeweilige Rohdaten- bzw. Szenarienaufbereitung qualifiziert sein.

Zwei Einsatzszenarien der Datenlieferantenrolle sind zu unterscheiden. Zum einen das Szenario, in welchem der Datenlieferant selbst auch Nutzer der Datenbank ist, und zum anderen das Szenario, in welchem der Stakeholder ausschließlich Datenlieferant ist. Beide Fälle unterscheiden sich im Hinblick auf die Incentivierung und die ökonomischen Anforderungen.

Für das zweite Szenario erfolgt die Incentivierung über die Möglichkeit, die zur Verfügung stehenden Datensätze profitabel bzw. zu einem höheren Wert und zusätzlich einfacher zu monetarisieren. Akteure wie Forschungsinstitute, Toolhersteller oder Technologieunternehmen sind als „reine“ Datenlieferanten denkbar. Über einen potenziellen monetären Ausgleich, beispielsweise über einen selbstbestimmten Verkaufspreis, für die Verwendung des eingestellten Szenarios durch andere Nutzer könnten private Akteure aus ihrer Partizipation Vorteile ziehen, indem sie auf diese Weise einen Marktzugang zum Verkauf der ihnen zur Verfügung stehenden Szenarien erhalten. Nicht alle Datenlieferanten ist es erlaubt die zu Verfügung stehenden Datensätze zu monetarisieren, daher ist es wichtig die Datensätze auch kostenfrei zur Verfügung stellen zu können.

Im ersten Szenario, profitiert der Datenlieferant neben der Möglichkeit zur Monetarisierung der ihm zur Verfügung stehenden verwertbaren Datensätze auch durch den Nutzen der IT-Infrastruktur, welche die Vergünstigung der Veredlung bzw. die Datenaufbereitung ermöglicht. Der Zusatznutzen entsteht durch das vereinfachte Datenmanagement und ein angepasstes Nutzerinterface zur ODD-Definition und -Prüfung, sowie die größere Varietät an Szenarien. Eine zusätzliche Incentivierung der Datenlieferung erbringt auch eine mögliche Freigabe der getesteten Fahrfunktion anhand der ODD-relevanten und in der Datenbank verfügbaren Szenarien. In Tabelle 2 und Bild 18 werden die Nutzenunterschiede in Abhängigkeit von der jeweiligen Stakeholdergruppe noch detaillierter dargestellt.

Diverse Akteure könnten sowohl Datenlieferant als auch Nutzer der Datenbank sein. Beispiele wären OEMs und Zulieferer, die selbst bereits Szenariensätze besitzen, aber von der größeren Varietät der Szenarien und Corner-Cases profitieren könnten, um die Sicherheitsprüfung autonomer Fahrfunktionen zu verbessern und zu vereinfachen.

Zudem sind öffentliche Akteure mögliche Datenlieferanten, welche gleichsam als Nutzer auftreten können. Der Zusatznutzen entsteht durch die Möglichkeit, Rohdaten wie Kameraaufnahmen oder Verkehrsdaten einzuspeisen, um entweder durch die Monetarisierung der Datensätze eine externe Dienstleistung zur Auswertung der Daten mit speziellem Fokus (z. B. eine Erhebung des Durchflusses einer Kreuzung anhand einer Drohnenaufnahme) zu vergünstigen oder direkt durch die IT-Infrastruktur, das Datenmanagement und die Veredlung zu profitieren, z. B. um Verkehrssicherheitsmaßnahmen anhand von Simulationsszenarien zu bewerten.

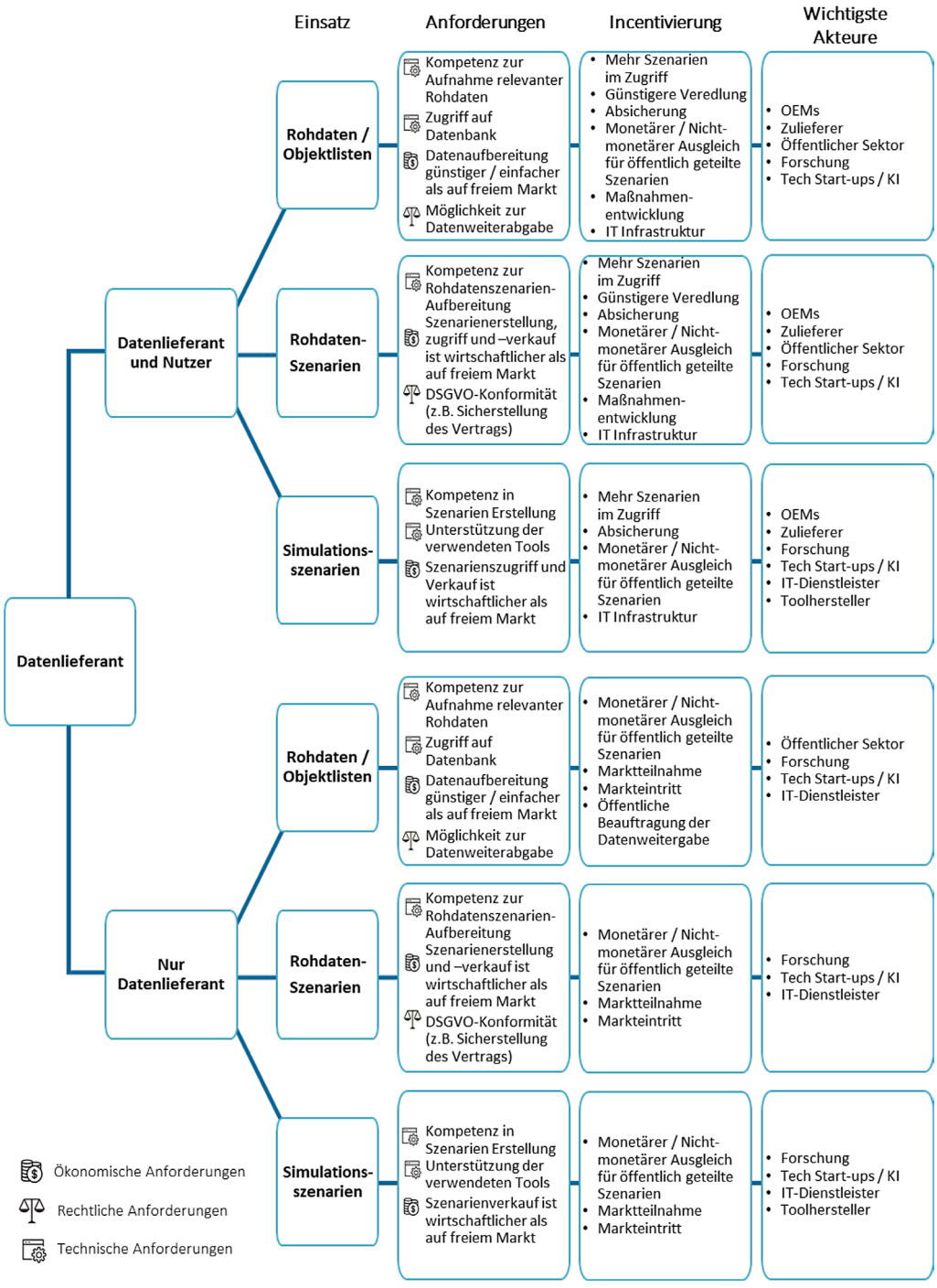


Bild 7: Detaillierte Rollenbeschreibung Datenlieferant (Quelle: Eigene Darstellung)

Synchron zu dem oben genannten Nutzen der Freigabe der Fahrfunktion, durch beispielsweise Produzenten, besteht der Nutzen öffentlicher Akteure, beispielsweise Kommunen, in der Definition der sicherheitsrelevanten zu prüfenden Szenarien, als Informationsgrundlage für eine mögliche Freigabe. Hierdurch könnten die Rahmenbedingungen einer möglichen Freigabe definiert und damit explizite Maßnahmen entwickelt werden.

3.2.3 Veredler

Im Datenbankmodell sind für die Rolle des Veredlers drei mögliche Einsatzszenarien differenzierbar (vgl. Bild 8). Im ersten Schritt müssen Rohdaten anonymisiert und im zweiten Schritt diese zu Rohdatenszenarien aufbereitet werden. Aufbauend werden aus den Rohdatenszenarien simulationsfähige Szenarien erstellt, welche dann privat oder öffentlich auf der Datenbank abgelegt werden können.

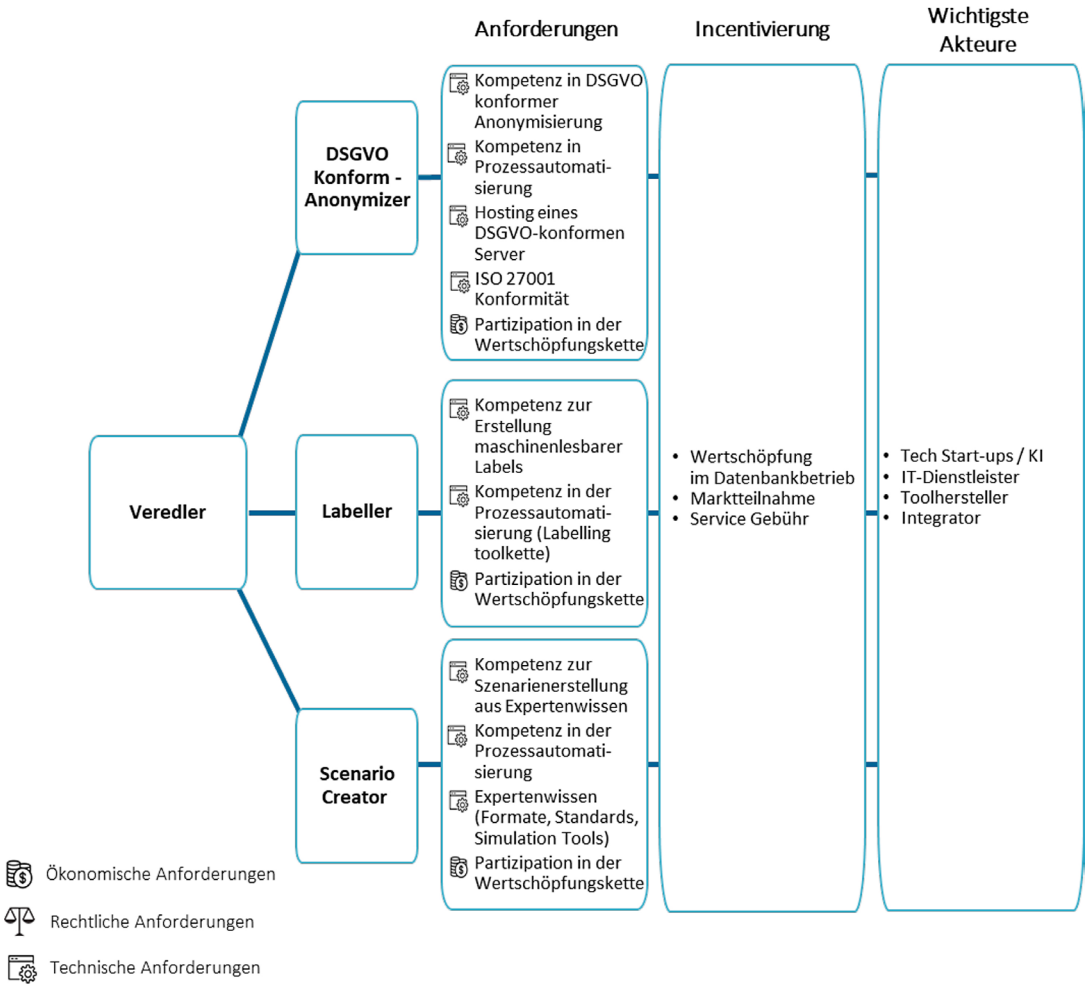


Bild 8: Detaillierte Rollenbeschreibung Veredler (Quelle: Eigene Darstellung)

Im ersten Szenario übernimmt der Veredler die DSGVO-konforme Anonymisierung der vom Datenlieferant eingespeisten Rohdaten. Hierfür ist es erforderlich, dass der Veredler neben den technischen Fähigkeiten zur DSGVO-konformen Anonymisierung von personenbezogenen Rohdaten die passenden Zertifizierungen zur Durchführung von DSGVO-relevanten Audits besitzt. Laut der DSGVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Außerdem muss auf allen Stufen der Lieferkette die Datensicherheit gewährleistet werden. Der Verantwortliche

(in diesem Fall, der Veredler) muss geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

Die Verantwortung der Anonymisierung könnte auch beim Datenlieferanten, oder außerhalb des Kernbetriebs der Datenbank liegen (vgl. Bild 24). Hierdurch ergeben sich klare Vorteile für den Betreiber, jedoch auch eine geringere Incentivierung zur Datenlieferung.

Aufbauend werden in der Veredlung durch die Erstellung maschinenlesbarer Labels Rohdaten in nutzbare Inputs für die Szenarien umgewandelt. Folglich ist eine weitere Anforderung an den Veredler im Einsatzszenario als Ersteller der Rohdatenszenarien die Fähigkeit, diesen Prozess zu automatisieren, um in der langfristigen Perspektive das Kostenminderungspotenzial auszuschöpfen.

Im dritten Einsatzszenario ist der Veredler für die Erstellung der Simulationsszenarien oder auch simulationsfähigen Szenarien verantwortlich. Für diesen Zweck sind Fachkenntnisse und Expertise mit Blick auf Szenarienerstellung und Prozessautomatisierung erforderlich. Wichtig ist, dass der Veredler in der Lage ist, standarisierte simulationsfähige Szenarien aus diversen Dateiformaten zu erstellen.

Im Idealfall führt der Veredler mehr als eine der genannten Funktionen aus und ist Teil oder Partner des Betreibers. Dies würde die Koordination zwischen dem Betrieb und dem Veredler vereinfachen. Die Incentivierung für einen unabhängigen Veredler oder einen Partner des Betreibers besteht im Verdienst einer Servicegebühr und die Möglichkeit am Markt teilzunehmen sowie den dadurch entstehenden strategischen Vorteil auf dem Markt auszubauen.

Die Besetzung der Veredlerrolle durch Tech Start-ups, Toolhersteller oder IT-Infrastrukturunternehmen ist vorstellbar.

3.2.4 Betreiber

Die Schlüsselrolle des Rollenmodells übernimmt der Betreiber (vgl. Bild 9). Dessen Funktionen sind die Teilnehmer der Datenbank zu koordinieren, zu unterstützen und zu incentivieren, sowie sicherzustellen, dass die technischen Aspekte der Datenbank erfolgreich funktionieren. Zusätzlich kommen dem Betreiber die Aufgaben der rechtssicheren Ausgestaltung des Datenbankbetriebs zu. Aus dem Aufgabenumfang in allen Bereichen (Technisch, Rechtlich, Ökonomisch) ist es herauszustellen, dass die Funktionen nicht alle durch einen einzigen Stakeholder bedient werden müssen. Eine Institution oder Partnerschaft übernimmt jedoch die Verantwortung für die Datenbank (Betreiber) und vergibt aus eigener Expertise oder Kapazität nicht erfüllbare Aufgaben in Form von Unteraufträgen oder bestellten Dienstleistungen. Die angesprochenen Kompetenzen sind in der folgenden Grafik zusammengefasst.

In Bezug auf die ökonomische Anforderung an den Betreiber ist es wichtig, dass seine Kosten durch den Geschäftsbetrieb oder Fördermittel gedeckt werden. Aus den Interviews (vgl. Tabelle 3) mit vergleichbaren Szenariendatenbanken (SafetyPool und ENVITED) wurde festgestellt, dass eine anfängliche Kostendeckung unwahrscheinlich ist und folglich zunächst eine öffentliche Zuschussfinanzierung oder weitere Finanzierungsquellen zur Kostendeckung, wie beispielsweise das Angebot von Zusatzleistungen in Bezug auf das Testen, Validieren und Freigeben für einen monetären Ausgleich, notwendig sind.

Die Incentivierung der Besetzung der Betreiberrolle ist vielfältig und hängt stark von der zur Verfügung stehenden Finanzierung der Datenbank-Anfangsphase und der Stakeholder-

struktur (Öffentlich/Privat/Öffentlich-Privat) ab. Anreize zur Rollenbesetzung sind neben dem Beitrag zur Vergrößerung des kooperativ nutzbaren Szenarienbestandes für die Sicherheitsprüfung autonomer Fahrfunktionen und der Beitrag der Datenbank zur Standardisierung der Simulationsszenarien auch monetäre Anreize in der Form von Fördergeldern oder Marktpositionierung. Zweiteres bezieht sich auf die oben angesprochene Möglichkeit, den Partizipierenden Zusatzleistungen im Bereich der Absicherung, Validierung und Freigabe der Fahrfunktion anzubieten.

Die Auswahl der konkreten Akteure, welche die Rolle des Betreibers übernehmen könnten, hängt von dem spezifischen Use-Case der Szenariendatenbank ab. Wenn es sich um den vorgeschlagene Use-Case (Forschungsdatenbank) handelt, könnte eine öffentliche Institution oder auch der technische Dienst als Finanzier oder Vorsitz der Betriebskooperation fungieren. Es gibt auch die Möglichkeit, dass eine Forschungsdatenbank von einer öffentlich-privaten Partnerschaft (ÖPP), in Kooperation mit privatwirtschaftlichen IT-Dienstleistern betrieben wird. In dieser Konstellation wäre ein Mischbetrieb der Szenariendatenbank vorstellbar, in welchem verschiedene Nutzerzugangspakete modular für kommerzielle Nutzer, beispielsweise OEMs oder Zulieferer mit dem kommerziellen Nutzen der ODD-Definition, Prüfung und Freigabe, sowie unkommerzielle Nutzer, beispielsweise Forschungsinstitute oder Kommunen mit dem Ziel der Erfüllung von Forschungsvorhaben bzw. der Definition von Rahmenbedingungen, angeboten werden. Hierdurch könnten die diversen Nutzerinteressen individuell nach den jeweiligen Bedürfnissen abgedeckt werden.

Auch eine rein privatwirtschaftliche Betreiberstruktur ist vorstellbar. Dies erscheint jedoch besonders in der Anfangsphase eher unwahrscheinlich, da der Zusatznutzen zu bereits bestehenden privatwirtschaftlich betriebenen Datenbanken und die resultierenden Einnahmequellen zu gering für ein privatwirtschaftlich tragbares Geschäftsmodell ist. Potenzielle privatwirtschaftliche Betreiber wären beispielsweise IT-Dienstleister oder Toolhersteller.

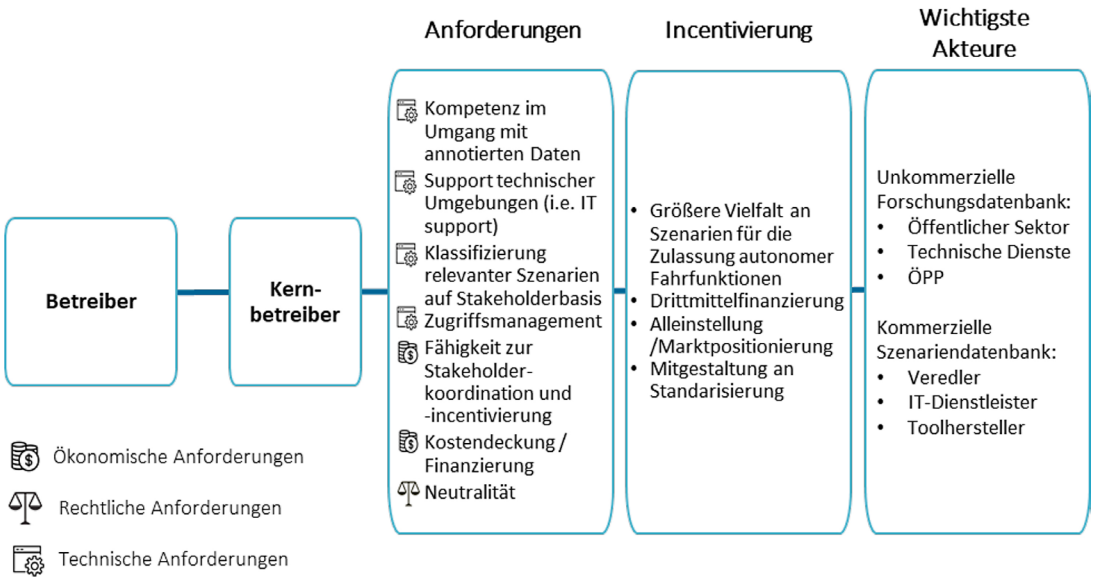


Bild 9: Detaillierte Rollenbeschreibung Betreiber (Quelle: Eigene Darstellung)

3.2.5 Auditor

Aufgabe des Auditors ist es, zu überprüfen, ob die zur Verfügung gestellten (anonymisierten) Rohdaten mit der Datenschutz-Grundverordnung (DSGVO) konform sind (vgl. Bild 10). Hierzu werden regelmäßige Audits durchgeführt, um zu überprüfen, ob die Anonymisierung der Rohdaten im Einklang mit den Rechtsakten und Standards in Bezug auf

Datenschutz (z. B. DSGVO) und IT-Sicherheit (z. B. ISO 27001) erfolgt. Als Anreiz erhält der Auditor für jeden durchgeführten Audit eine Servicegebühr.

Es sind weitere Anforderungen an den Auditor, je nach Betriebsmodell, ableitbar. Es ist vorstellbar einen Auditor zur Qualitätsprüfung der Szenarien einzusetzen. Dadurch können die auf der Datenbank verfügbaren Szenarien im Hinblick auf Aktualität, Corner-Case und weiteren Qualitätsstandards zertifiziert werden. Dies wird besonders bei steigender Homologationsrelevanz jedoch auch bereits für Absicherungsthemen von großer Bedeutung sein.

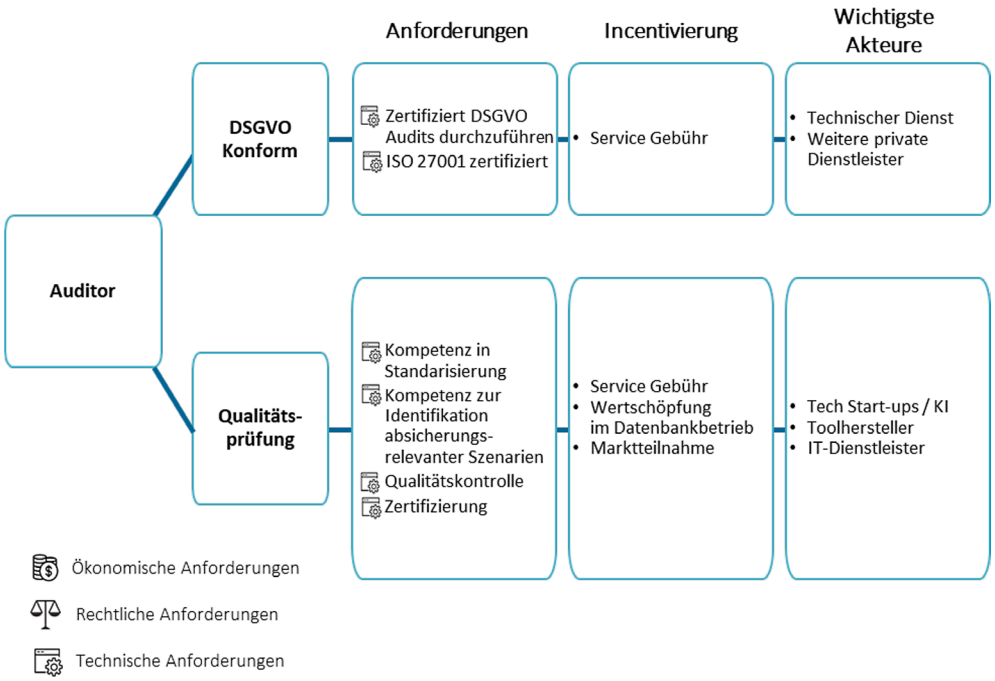


Bild 10: Detaillierte Rollenbeschreibung Auditor (Quelle: Eigene Darstellung)

3.2.6 Nutzer

Die letzte Rolle ist die des Nutzers (vgl. Bild 11). Wie beschrieben, besteht die Möglichkeit, dass der Nutzer auch Daten liefert. Die ökonomische Anforderung an den reinen Nutzer ist folglich die Bereitschaft eine Gebühr für den Zugriff auf die Datenbank und für jedes verwendete Szenario zu entrichten.

Ein Anreiz für die Partizipation an der Datenbank als reiner Nutzer ist das vereinfachte Datenmanagement in der Datenbankinfrastruktur sowie der vereinfachte Zugriff auf eine größere Varietät an Szenarien und Corner Cases. Eine zusätzliche Incentivierung der Datenbanknutzung kann durch die Möglichkeit der Freigabe bzw. der Absicherung von neu entwickelten Fahrfunktionen erreicht werden.

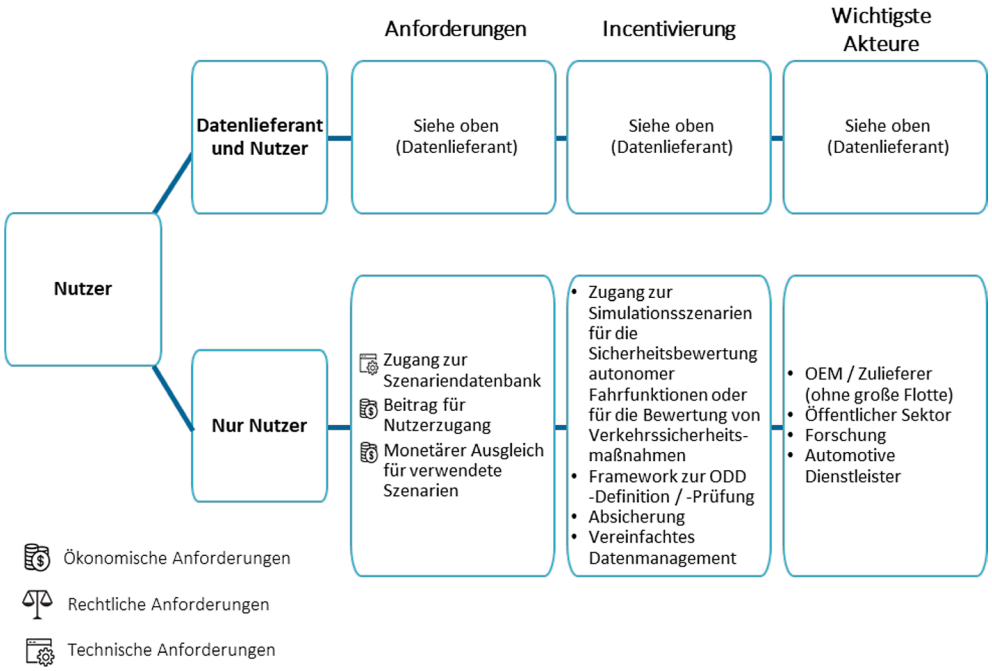


Bild 11: Detaillierte Rollenbeschreibung Nutzer (Quelle: Eigene Darstellung)

3.2.7 Zwischenfazit

Zusammenfassend besteht das Rollenmodell der Szenariendatenbank aus den fünf beschriebenen Rollen: Datenlieferant, Veredler, Auditor, Betreiber und Nutzer. Es besteht die Möglichkeit, dass ein Stakeholder mehr als eine Rolle übernimmt. Vorstellbar ist, dass ein Stakeholder zum Beispiel zugleich die Rolle des Betreibers und Veredlers oder des Datenlieferanten und des Nutzers ausfüllt. Außerdem unterscheiden sich die Rollen des Veredlers und des Datenlieferanten auf Basis des von ihnen angebotenen Inputs sowie des erwarteten Umfangs der Dienstleistungen.

In jedem Fall muss sichergestellt werden, dass die Stakeholder einen Anreiz haben, sich an der Datenbank zu beteiligen und dass die ökonomischen Anforderungen jeder Rolle erfüllt werden. Die bereits angesprochenen Anreize sowie die Rollendifferenzierung bilden die Basis der Anreizevaluation und werden im Abschnitt Anreizevaluation und Geschäfts- und Betreibermodellvorschläge detailliert und differenziert dargestellt.

3.3 Herleitung Betreiber- und Finanzierungsmodelle

Die Herleitung der Finanzierungs- und Betreibermodellvorschläge baut auf der vorrangegangenen Marktanalyse, den Experteninterviews sowie dem abgeleiteten Rollenmodell auf. Zur Ableitung relevanter Finanzierungsmechanismen unter Einbezug der diversen Bedürfnisse von Nutzern mit kommerziellem bis nicht-kommerziellem Partizipationsinteresse wurden erneut die Modelle der drei bereits existierenden, Datenbanken in den Analysefokus genommen (vgl. Tabelle 2).

Der ENVITED Marketplace fordert eine Bezahlung für einzelne Testdaten (Pay per Dataset), SafetyPool ermöglicht eine Monetarisierung in verschiedenen Preissegmenten (Paketierung) und eine weitere nicht durch Experteninterviews abgedeckte existierende Lösung, die Road Safety Data, betrieben durch das Departement for Transport im Vereinigten Königreich Großbritannien und Nordirland, wird vollständig aus staatlichen Mitteln finanziert.

Zusätzlich zu diesen Optionen wurde im Modell dieses Forschungsvorhabens nun noch die Option eines konstanten Mitgliedsbeitrags als Finanzierungsvariante eingeführt. Separiert wurde außerdem die Erstfinanzierung (CAPEX) von den laufenden Kosten (OPEX) betrachtet.

Bei der Grundfinanzierung der Datenbank ist zunächst zu entscheiden, ob eine Zuschussfinanzierung seitens eines oder mehrerer Stakeholder aus dem Betreibermodell möglich ist. Als potenzieller Investor wäre eine öffentliche Institution denkbar. Eine Zuschussfinanzierung garantiert eine finanzielle Grundsicherheit beim Aufbau der Datenbank und sollte daher in Betracht gezogen werden. Ein geringerer Anteil der Mitgliedsfinanzierung beim Aufbau der Datenbank reduziert die Investitionskosten für potenzielle Stakeholder und motiviert zur initialen Investition.

Durch eine Koppelung von staatlicher Zuschussfinanzierung und Mitgliedsfinanzierung kann ein Rahmen gesetzt werden, der die Attraktivität einer Beteiligung für potenzielle Stakeholder steigert. Es stellt sich demnach nun die Frage, in welchem Verhältnis die Zuschussfinanzierung zur Mitgliedsfinanzierung im Gesamtfinanzierungsmodell steht (vgl. Bild 12).

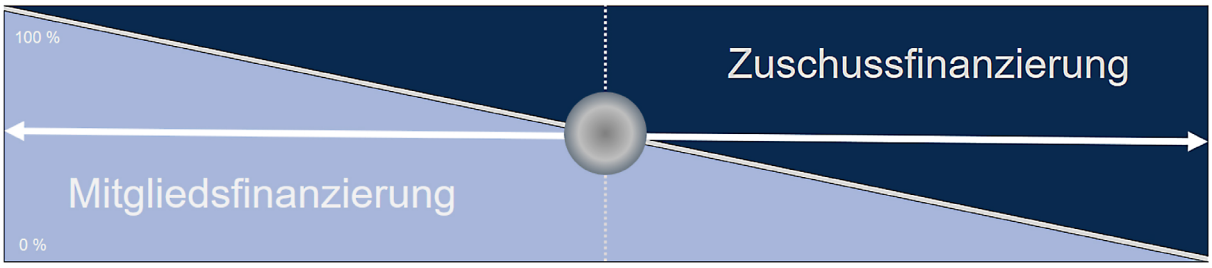


Bild 12: Mitgliedsfinanzierung versus Zuschussfinanzierung beim initialen Aufbau (Quelle: Eigene Darstellung)

Denkbar ist ein Finanzierungskonzept mit einer Verteilung von einer variablen Mitgliedsfinanzierung zu Zuschussfinanzierung (u. a. staatliche Zuschüsse, Förderprogramme). Dabei kann der Zuschussanteil davon abhängen, wie hoch die Zahlungsbereitschaft der jeweiligen Stakeholder (Mitglieder) im Modell ist. Auf Basis derer können die staatlichen Zuschüsse angeboten werden. Das Finanzierungsmodell der Road Safety Data eignet sich als Referenz nicht, da diese ausschließlich durch Zuschüsse finanziert wird.

3.3.1 Geschäftsmodellentwicklung

Nachdem die Best-Practice Ansätze verschiedener Datenbanken zusammengetragen wurden, erfolgte zusätzlich zur Untersuchung der Finanzierung der laufenden Kosten die Anfertigung eines Business Model Canvas (BMC) in Bild 13. Das Modell zentralisiert für das Finanzierungsmodell und die Anreizevaluation das Wertversprechen der Datenbank.

Hierdurch kann zielgerichtet das Finanzierungsmodell mit dem Wertversprechen verknüpft werden, sodass die optimale Zahlungsbereitschaft zum Betrieb der Datenbank für jeden Stakeholder erhalten werden kann. Im Kern enthält der Business Model Canvas neun Kategorien. In diesem Kapitel werden die Themen Wertangebote, Kostenstruktur und Einnahmequellen fokussiert. Die Ergebnisse des BMC führen zu den zwei bzw. drei Ausprägungen zur Finanzierung der laufenden Kosten und sind in Tabelle 7 dargestellt.

Bild 13: Business Model Canvas zur Berücksichtigung der Interessen der Stakeholder (Quelle: Eigene Darstellung)

3.3.2 Workshopergebnisse: Finanzierungsmodell

Ausgehend von der Untersuchung der bereits existierenden Datenbanken und der entwickelten BMC wurden anschließend in dem zweiten Stakeholderworkshop zwei bzw. drei Finanzierungsvarianten für die Mitgliedsfinanzierung der laufenden Kosten vorgestellt und hinsichtlich der Kriterien Attraktivität für Mitglieder, Finanzierungszuverlässigkeit und (wirtschaftliches) Unternehmensrisiko bewertet:

Variante A: Konstante Mitgliedsbeitragsfinanzierung
Bei dieser Variante werden die laufenden Kosten im Rahmen eines Mitgliedsbeitrages an alle Teilnehmer (Stakeholder) der potenziellen Datenbank verteilt.

Variante B: Preisdifferenzierung zur Mitgliedsbeitragsfinanzierung
Bei dieser Variante werden die laufenden Kosten in eine Paketierung (Variante B.2) umgelegt. Denkbar ist eine S/M/L –Variante mit unterschiedlicher Anzahl an Abrufen von möglichen Szenarien. Zusätzlich wird eine Option für eine Nutzung bei Bedarf (Variante B.1, Pay per Dataset) eingeführt. Diese ist eine zusätzliche Einnahmequelle für die Datenbank, sollte aber nicht für die Sicherstellung der Fixkosten genutzt werden, da die Einnahmen nicht zuverlässig bestimmt werden können.

Die beiden Varianten mit ihren beschriebenen Ausprägungen wurden in dem Stakeholder-Workshop 2 zur Diskussion gestellt. Die wichtigsten Ergebnisse der Diskussion wurden in der nachfolgenden Tabelle 7 zusammengefasst.

	Variante A: Mitgliedsbeitrag konstant	**Variante B.1: Mitgliedsbeitrag Pay per Dataset**	**Variante B.2: Mitgliedsbeitrag Paketierung**
Attraktivität für Mitglieder	+ Attraktivität für Betreiber + Kosten gut prognostizierbar	+ Attraktivität für Teilnehmer mit geringer Partizipation + Motivation zur Bereitstellung wertvoller Daten	+ Attraktivität für die Nutzer hoch, da Diversität in Paketen abgebildet werden kann
Finanzierungszuverlässigkeit	+ Balance zw. Stakeholdern notwendig	+ Kostendeckung grundsätzlich notwendig, hier schwer umsetzbar + Einnahmen und Ausgaben schwer auszugleichen	+ Geringeres bis mittleres Risiko, da kalkulierbar
Unternehmensrisiko (wirtschaftlich)	+ Nutzen schwer kalkulierbar, damit Teilnahme als Teilhaber fraglich	+ Nutzer bzw. deren Prognose schwer absehbar	+ Keine Nennungen

Tab. 7: Finanzierungsvariantenvergleich der Mitgliedbeiträge

Aus der Diskussion der Teilnehmer ergab sich, dass nicht nur eine Variante allein zu favorisieren ist. Im Sinne einer Risikoreduktion für den Betreiber bzw. ein mögliches Betreiberkonsortium ergibt sich als Zielbild eine sinnvolle Kombination der einzelnen Bausteine. Das bedeutet einen Mitgliedsbeitrag von verschiedenen Stakeholdern einzufordern, welche hiermit den vollen Umfang der Datenbank nutzen können (L-Paket, Paketierung). Gleichfalls können kleinere Teilnehmer für einzelne Daten entlohnt werden oder einen Betrag für die entnommenen Daten zahlen (Variante B.1, Pay per Dataset). Für die Pakete S, M, L wird eine Laufzeit von 12 Monaten empfohlen, um zumindest eine kurzfristige Finanzplanung für die Datenbank zu ermöglich. Dabei kann eine Rabattierung gegenüber dem „Pay Per Datatset" gegeben werden.

3.3.3 Zwischenfazit

Berücksichtigt man eine Zuschussfinanzierung bei dem initialen Aufbau der Datenbank (CAPEX) und eine Kombination der Varianten A, B.1 und B.2 bei der Finanzierung der laufenden Kosten (OPEX), ist damit ein Finanzierungsmodell skizziert, das zumindest einen kostendeckenden Betrieb sicherstellen kann. Die Ausgestaltung der Paketierung im Detail ist in Tabelle 7 dargestellt.

Im späteren Betrieb der Szenariendatenbank bestehen weitere Optionen zur Kommerzialisierung von Inhalten. Anzuführen ist die Vergütung für die Nutzung von Simulationen, für die Verknüpfung von verschiedenen Szenarien sowie die Veredelung/Verknüpfung von Rohdaten. Gleichzeitig kann auch ein Anreiz geschaffen werden, um Daten zu teilen: Hierbei ist ein Vergütungssystem durch Punktegutschriften denkbar. Dieses kann auch von den Akteuren genutzt werden, um neue Daten bzw. Szenarien zu erhalten.

Betriebsfinanzierung		Anmerkung	Testversion (14 Tage)	S	M	L	Alternativ: PAY PER DATASET	SHAREHOLDER
Zugriffsrechte	Lesen		x	x	x	x		x
	Schreiben		x		x	x		x
	Admin							x
Daten (Integration)								x
	Rohdaten	Punktegutschrift	/	x	x	x	/	x
	Veredelte Daten	Punktegutschrift	/	x	x	x	/	x
	Szenarien	Punktegutschrift	/	x	x	x	/	x
Daten (Nutzung)	Rohdaten			x	x	x	(x)	x
	Veredelte Daten				x	x	(x)	x
	Auswahl Szenarien	Vorgesetzte Filter	x		x	x	(x)	x
	Alle Szenarien					x	(x)	x
Organisation	Aufrufe (Anzahl)		limitiert	limitiert	limitiert	unendlich		
	Guthaben (Punkte)		/				Punkte für Integration	
	Discount*1			15%	15%	15%		
	Laufzeit (Monate)			12	12	12	Keine	unbegrenzt
Stakeholder	Kommune		*/	OEM	OEM	**OEM**	OEM	**OEM**
	Datenlieferant			Zulieferer	Zulieferer	**Zulieferer**	**Zulieferer**	**Zulieferer**
	Veredler			**Forschung**	Forschung	Forschung	**Forschung**	Forschung
	Auditor			Tech Start-ups /KI	Tech Start-ups /KI	Tech Start-ups /KI	**Tech Start-ups /KI**	Tech Start-ups /KI
	Betreiber			IT-Dienstleister	**IT-Dienstleister**	IT-Dienstleister	**IT-Dienstleister**	IT-Dienstleister
	Nutzer			Toolhersteller	**Toolhersteller**	Toolhersteller	**Toolhersteller**	**Toolhersteller**

*1 monatliche Zahlweise, jährliche Zahlweise (15% Discount), 12 Monate Vertragslaufzeit, danach monatliche Kündigungsmöglichkeit

Tab. 8: Paketierung inklusive Testzugang

Die Ausgestaltung dieses System ist in Tabelle 8 dargestellt. Unterschieden wird zwischen der Datenintegration und der Datennutzung. Die Gutschrift für eine Datenintegration kann in eine Nutzung von Rohdaten, veredelten Daten oder auch Szenarien umgewandelt werden. Bei den ausgewählten Szenarien sind entsprechend des Lastenheftes Filter vorgewählt. Dies bedeutet Daten mit u. a. ausgewählten Infrastrukturelementen (Bsp. Kreuzung, Kreuzungssituation) werden zusammengefasst und als Mehrwert angeboten. Neu in diesem finalen Modell ist auch das Angebot einer Probelizenz, um Interessierten einen Einblick in die Datenbank zu verschaffen, ohne deren Modell zu kannibalisieren. Dazu wird nur ein eingeschränkter Zugriff auf die Inhalte gewährt.

3.4 Anreizevaluation und Geschäfts- und Betreibermodellvorschläge

Um das vorab erstellte Rollenmodell, sowie das Betreiber- und Finanzierungsmodell in den Kontext der Nutzersicht und der Incentivierung der Rollenbesetzung zu setzen wird im Folgenden eine Anreizevaluation der Partizipation im Datenbankbetrieb ausgeführt. Aufbauend werden die Ergebnisse aus dem Rollenmodell, der Betriebsarchitektur und dem Betreiber- und Finanzierungsmodell zu einem expliziten umfangreichen Use-Case der zu entwickelnden Datenbank konsolidiert. Schließlich wird eine Analyse der bereits abgedeckten Nutzerbedürfnisse durch bereits existierende Datenbanken durchgeführt. Hierdurch wird in der Anreizevaluation der Geschäfts- und Betreibermodellvorschläge vollumfänglich der Zusatznutzen, die Incentivierung der Akteure, eine explizite Ausgestaltung des Anwendungsfalls sowie bereits durch andere Anbieter abgedeckten Kernfunktionalitäten der zu entwickelnden Szenariendatenbank erörtert.

3.4.1 Expertenbefragung: Rollenmodell und Incentivierung

Zur Vertiefung und Validierung der bisherigen Projektergebnisse sowie zur Integration der Nutzersicht in die Analyseergebnisse wurde eine umfangreiche Expertenbefragung durchgeführt. Der umfangreiche Ergebnisbericht der Umfrage ist als Anhang (A3) dem Schlussbericht beigelegt. Im Folgenden werden die Kernergebnisse der Umfrage in Bezug zu dem vorab erstellten Rollenmodell gesetzt und aufbauend die wahrscheinlichsten Rollenbesetzungen in einem hypothetischen Datenbankbetrieb abgeleitet.

Hierzu wurden die in einem projektinternen Workshop vorab erarbeiteten Anreize und Hemmnisse einer Partizipation an der Szenariendatenbank in Rücksprache mit der Auftraggeberin geschärft und, auf die bereits begonnene interne Evaluation aufbauend, durch ein breites Netzwerk an Experten aus verschiedenen Stakeholdergruppen bewertet.

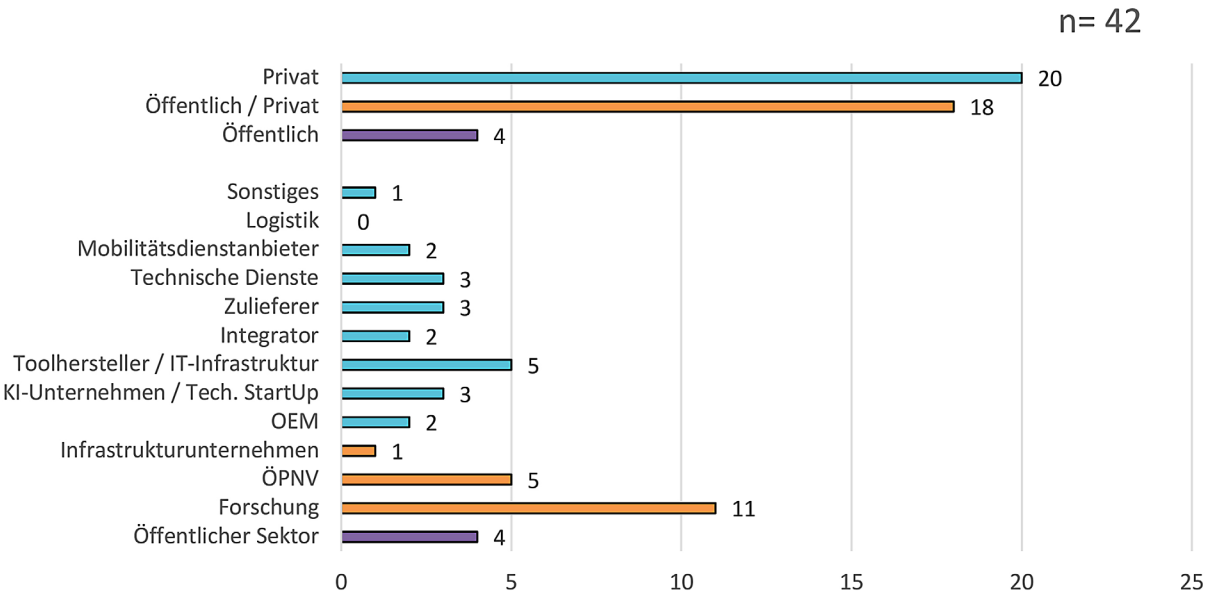


Bild 14: Anzahl der Befragten und ihre Verteilung auf die Stakeholdergruppen bzw. Cluster (Quelle: Eigene Darstellung)

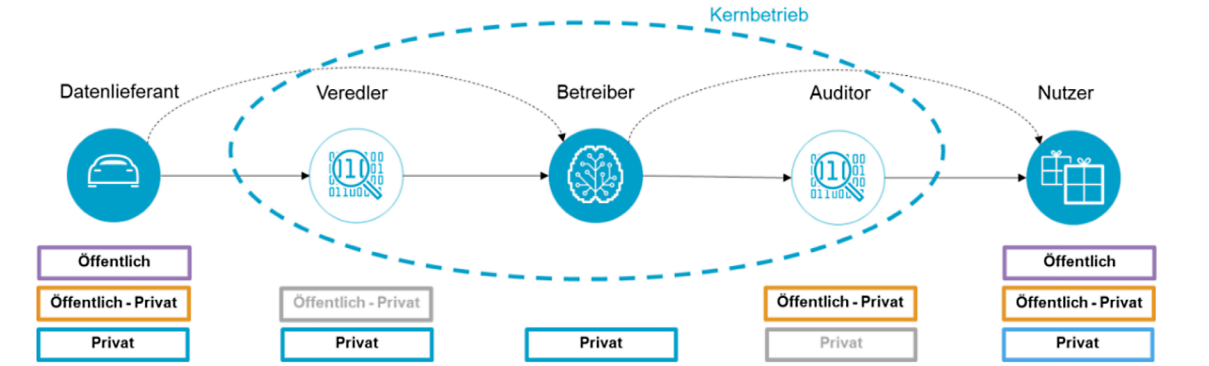
An der Umfrage nahm ein Großteil aus dem privaten und semi-öffentlichen Sektor teil und eine Minderheit aus dem öffentlichen Sektor. Die Teilnahme an der Umfrage ist in Bild 14 detailliert nach Stakeholdergruppe und -cluster aufgeschlüsselt. Das erste Ziel der Befragung war es, das zuvor entwickelte Rollenmodell zunächst zu validieren und im zweiten Schritt die Rollen den einzelnen Stakeholdergruppen zuzuordnen. Hierbei wurde zunächst die Selbstsicht, also die Wahrscheinlichkeit, nach welcher sich ein Stakeholder selbst einer Rolle zuordnen würde, und aufbauend die Fremdsicht, welche Stakeholdergruppe der jeweils Befragten in welcher Rolle sieht, abgefragt. Die Ergebnisse sind zusammenfassend in Bild 15 dargestellt.

Rollenzuschreibungen

Folgend wird im oberen Teil des Bildes die Selbstsicht der Rollenzuschreibung dargestellt. Also mit welcher Wahrscheinlichkeit hat sich welches Cluster (Privat/Öffentlich-Privat/Öffentlich) welcher Rolle zugeteilt (vgl. Bild 15, oberer Teil). Farblich hervorgehoben sind Cluster mit einer höheren Wahrscheinlichkeit und grau unterlegt sind Cluster mit sehr ähnlicher Wahrscheinlichkeit. Für Nutzer und Datenlieferanten sind alle drei

Cluster angegeben, da alle Cluster die Besetzung beider Rollen mit hoher Wahrscheinlichkeit bewertet haben.

Des Weiteren wird die Fremdsicht aufgezeigt, also welche Stakeholdergruppen am häufigsten für die jeweiligen Rollen von den anderen Antwortenden ausgewählt wurden (vgl. Bild 15, untere Tabelle). In der obersten Zeile wird die am häufigsten ausgewählte Gruppe dargestellt. Die Häufigkeit der Auswahl nimmt mit aufsteigender Zeilenzahl ab.



Infrastrukturunternehmen	KI-Unternehmen / Tech. StartUp	Toolhersteller / IT-Infrastruktur	Bund / Bundesbehörde	OEMs
ÖPNV	Forschung	Bund / Bundesbehörde	Technische Dienste	ÖPNV
Logistik	Toolhersteller / IT-Infrastruktur	Integratoren		Zulieferer (Tier1)
OEMs				Mobilitätsdienstanbieter
...				...

Bild 15: Ergebniszusammenfassung Rollenzuschreibungen (Quelle: Eigene Darstellung)

Das aus den Umfrageergebnissen ableitbare wahrscheinlichste Rollenmodell im Kernbetrieb ist die Besetzung der Veredlerrolle durch private bzw. semi-öffentliche Institutionen (Öffentlich-Privat). Die meisten Stakeholder sehen KI-Unternehmen oder Technologie Start-Ups als wahrscheinlichste Besetzung für diese Rolle und somit auch eher den privaten Sektor. Der Datenbankbetrieb wird am wahrscheinlichsten durch den privaten Sektor, und auf Stakeholdergruppenbasis durch Toolhersteller bzw. IT-Infrastruktur Unternehmen, besetzt. Die Auditorrolle wird entweder durch private oder semi-öffentliche Institutionen (Öffentlich-Privat) besetzt. Hier sehen die Befragten mit ähnlicher Anzahl entweder eine Bundesbehörde oder die technischen Dienste in der Verantwortung.

Anreizevaluation

In den folgenden Grafiken (vgl. Bild 16 und Bild 17) werden die Ergebnisse des zweiten Teils der Umfrage präsentiert. Der Fokus lag auf der stakeholderspezifischen Evaluation verschiedener Anreize und Hindernisse der Partizipation. Hieraus können die Möglichkeiten zur Incentivierung der einzelnen Stakeholder für die vorab erarbeitete Rollenbesetzung und folglich die Hebel der Umsetzung für den Datenbankbetrieb abgeleitet werden. In den Grafiken werden die einzelnen mit höchster Priorität wahrgenommenen Anreize und Hürden auf Rollen-, sowie Stakeholdercluster-Ebene dargestellt. Die Farbe des Kastens beschreibt das Cluster und der Inhalt den als höchsten priorisierten Anreiz (rechts), bzw. das höchste priorisierte Hemmnis (links).

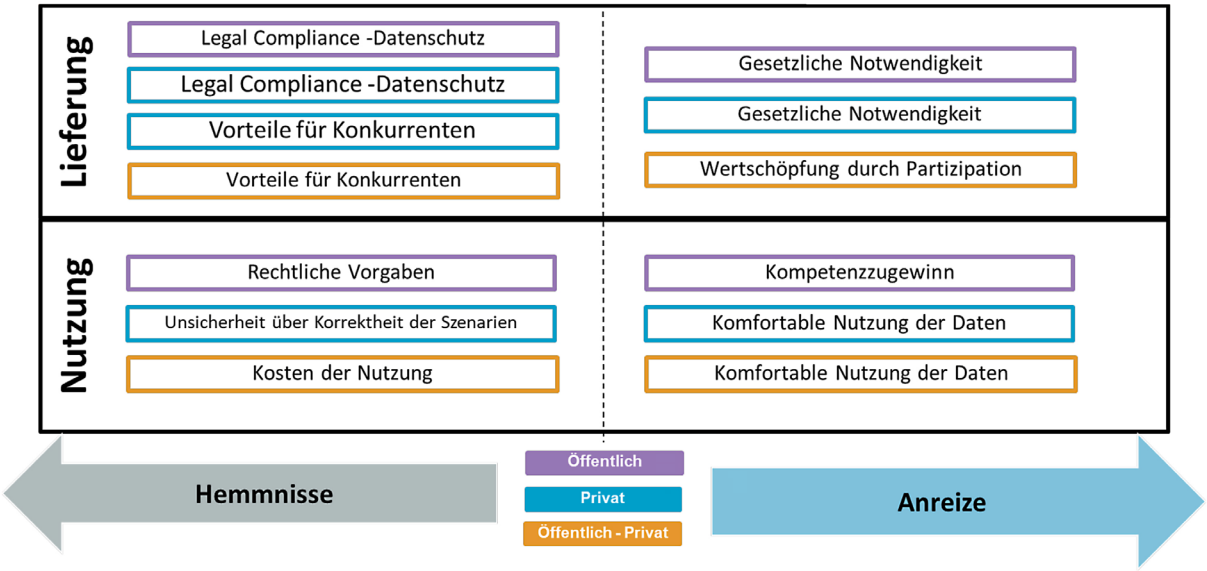


Bild 16: Anreize und Hemmnisse der Datenlieferung und Nutzung (Quelle: Eigene Darstellung)

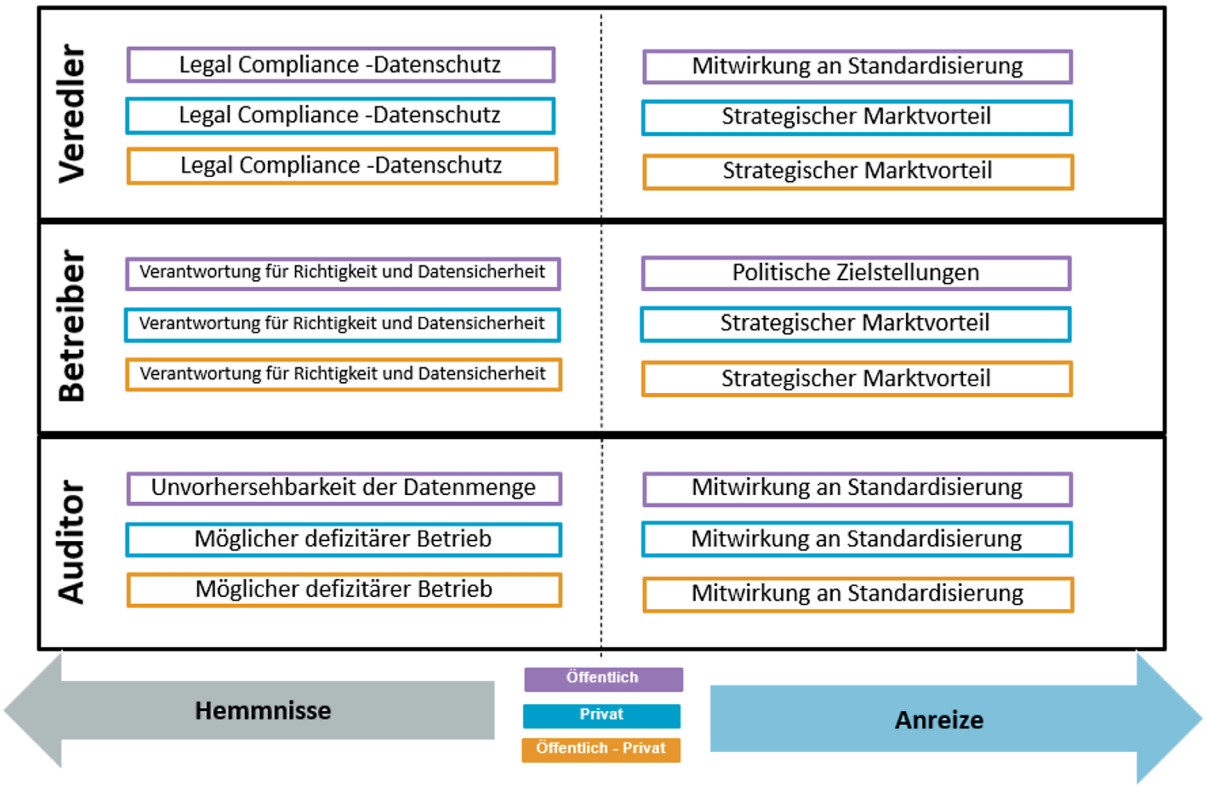


Bild 17: Anreize und Hemmnisse zur Partizipation im Kernbetrieb (Quelle: Eigene Darstellung)

Die Ergebnisse beider Umfrageabschnitte werden detailliert in Tabelle 9 zusammengefasst. Aus den Ergebnissen lassen sich verschiedene Incentivierungsmechanismen für die einzelnen Stakeholder zur Partizipation in den einzelnen Rollen im Kernbetrieb ableiten.

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 das Risiko dar, nach bereits vorgenommener Verede-

lung einen zu kleinen Absatz für die erstellten Szenarien zu erzielen. In diesem Zusammenhang 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 die Einbindung eines externen Gutachters bzw. Auditors 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 sichergestellt 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. Hemmnisse der Datenbanknutzung stellen Kosten der Nutzung, Unsicherheit betreffend der Korrektheit der Szenarien und die Einhaltung rechtlicher Vorgaben dar. Die Kosten der Nutzung könnten in Abhängigkeit der, der Nutzer angehörigen, Stakeholdergruppe angepasst werden. So müssten zum Beispiel OEMs einen höheren Mitgliedsbeitrag entrichten, während der Zugang für gemeinnützige Organisationen unter Umständen kostenlos bzw. kostengünstig angeboten werden könnte. 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 und als Hebel der Umsetzung für die vorab bewertete Rollenbesetzung abgeleitet werden.

Rolle	Cluster	Stakeholderguppe	Anreiz	Hürde
Veredler	Privat	KI-Unternehmen/Tech. Startup	Strategischer Marktvorteil	Legal Compliance -Datenschutz
Betreiber	Privat	Toolhersteller/ IT-Infrastruktur	Strategischer Marktvorteil	Verantwortung für Richtigkeit und Datensicherheit
Auditor	Öffentlich/ Privat	1. Bund/Bundesbehörde 2. Technische Dienste	Mitwirkung an Standardisierung	Möglicher defizitärer Betrieb

Tab. 9: Ergebniszusammenfassung Rollenzuschreibung und Anreiz- bzw. Hemmnis-Evaluation

3.4.2 Use-Case-Entwicklung

Aus den Schlussfolgerungen der Analyse der Marktarchitektur, der Entwicklung des Rollenmodells sowie der Anreizevaluation und Geschäfts- und Betreibermodellvorschläge wurde ein expliziter Anwendungsfall sowie die resultierende Ausgestaltung der zu entwickelnden Szenariendatenbank entworfen. Der Anwendungsfall bezieht folglich die möglichen Rollenverteilungen in einem hypothetischen Szenariendatenbankbetrieb mit ein. Aufbauend wurde der Anwendungsfall in einem Workshop in Kooperation mit Stakeholdern aus dem privaten bis öffentlichen Sektor evaluiert, validiert und an die Diskussion angepasst. Im Folgenden wird der ausgearbeitete Use-Case und das zugrundeliegende Betreibermodell vorgestellt und im nächsten Kapitel mit den Workshopergebnissen gespiegelt.

Zielsetzung der Szenariendatenbank ist es, durch retrospektive, als auch prospektive Daten die Sicherheit von hochautomatisierten Fahrfunktionen mit einer kooperativen Datenbank zu steigern. Hierzu ist eine breite Datenbasis nötig, um bereits ab Start den Nutzen für alle Stakeholder herauszustellen. Im Rahmen des Projektes haben sich das Anreiz- und Betreibermodell als entscheidende Faktoren zur nachhaltigen Umsetzung der Datenbank entwickelt. Um dieser Relevanz Rechnung zu tragen, wurden zunächst relevante Stakeholder identifiziert und kategorisiert. Zur Fokussierung wurden Experteninterviews mit den zwei zuvor genannten bereits existierenden Datenbankbetreibenden im naheliegenden Kontext geführt (vgl. Tabelle 2, Tabelle 3). Aufbauend wurde ein umfangreiches Rollenmodell für einen erfolgreichen Betrieb entworfen und mögliche Rollenbesetzungen durch die vorrangegangene Anreizevaluation herausgearbeitet. Das sich daraus ergebende mögliche Betreibermodell ist in Bild 18 dargestellt.

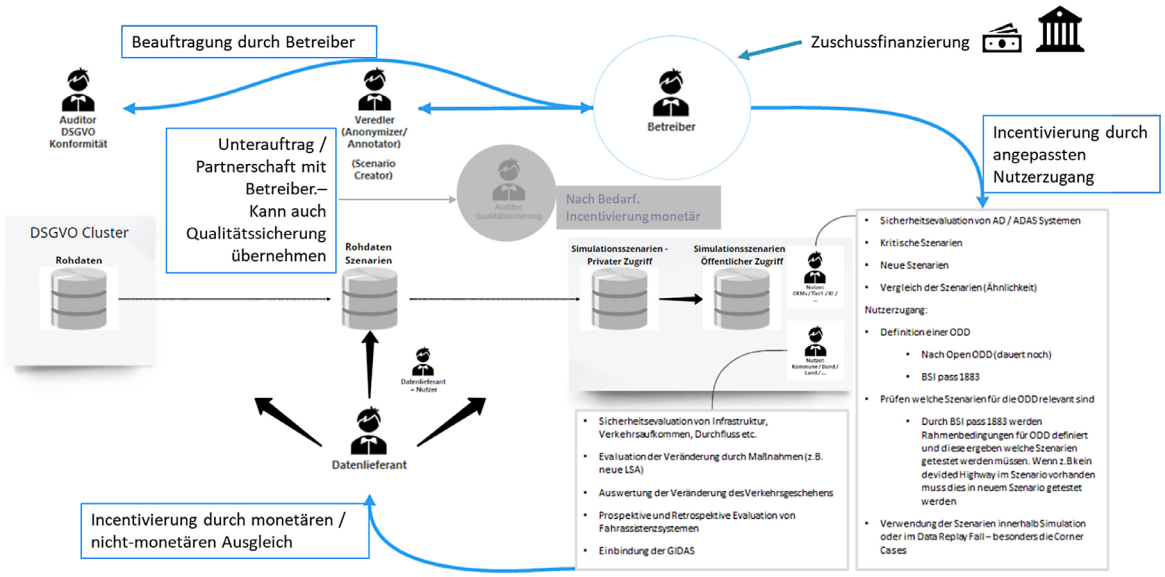


Bild 18: Schematische Darstellung des Betreibermodells (Quelle: Eigene Darstellung)

Es wird ersichtlich, in welchem Verhältnis die einzelnen Rollen im Anwendungsfall der zu entwickelnden Szenariendatenbank stehen. So beauftragt der Betreiber analog zu den Umfrageergebnissen den Auditor, welcher die Aufgabe der DSGVO Konformitätsprüfung für eine mögliche Rohdatenlieferung übernimmt. Der Veredler steht in engem Verhältnis zum Betreiber und kann entweder durch einen Unterauftrag oder als Partner im Betreibermodell integriert werden. Dieser besitzt je nach Rollenbesetzung die Expertise zur Qualitätsprüfung, auf welche im Falle der nötigen Erweiterung in Richtung Qualitätsmanagement zurückgegriffen werden kann. Die Nutzer werden je nach den herausgearbei-

teten Nutzerbedürfnissen zur Partizipation incentiviert, während die Datenlieferung über die genannten monetären und nicht-monetären Anreize motiviert wird.

Es wird dementsprechend auf die Nutzenunterschiede der zwei Hauptnutzergruppen, Akteure mit kommerziellem und nicht-kommerziellem Partizipationsinteresse, eingegangen. Die Abbildung fasst damit die Vorergebnisse der vorherigen Arbeitsschritte zusammen und dient als Grundlage für die folgende Use-Case-Entwicklung.

Bild 19 stellt den auf vorrangegangenen Projektergebnissen aufbauenden Anwendungsfall der zu entwickelnden Szenariendatenbank zusammenfassend dar.

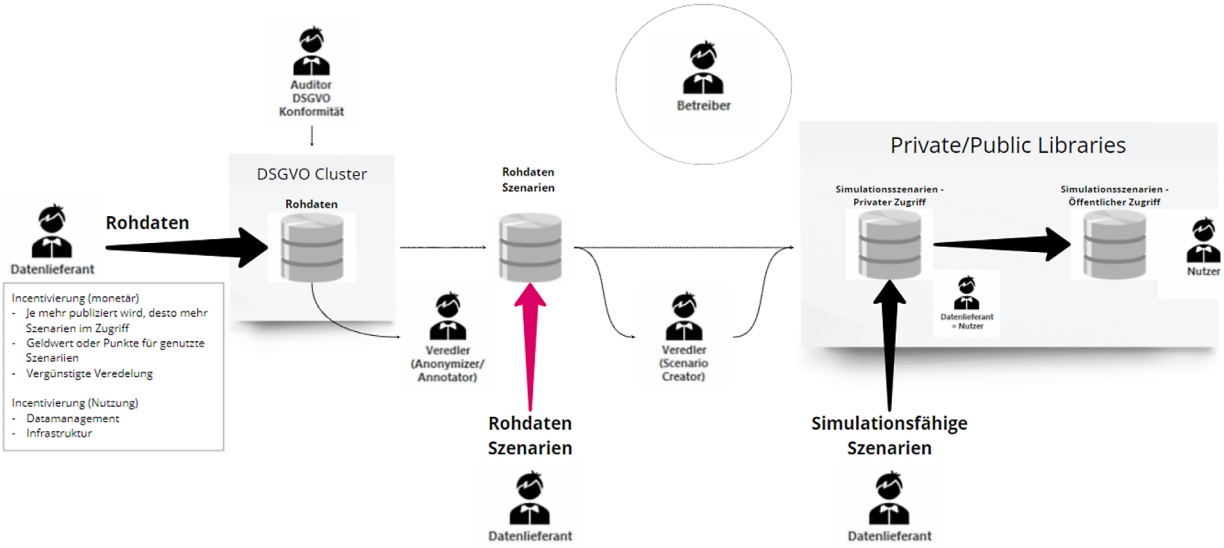


Bild 19: Anwendungsfall der zu entwickelnden Szenariendatenbank (Quelle: Eigene Darstellung)

Wie in der Abbildung beschrieben können durch Datenlieferanten im Use-Case entweder Rohdaten (Messdaten aus Kamera, GPS, Lidar, Radar und weitere Aufnahmen des Fahrzeugbusses oder der Infrastruktur), Objektlisten, Rohdaten-Szenarien und simulationsfähige Szenarien in die Datenbank eingespeist werden. Die Lieferung von Rohdaten-Szenarien (Roter Pfeil) birgt die Verantwortung des Betreibers die gelieferten Daten vor Integration auf eine datenschutzkonforme Anonymisierung zu prüfen, da hier personenbezogene Daten enthalten sein können. Die eingespeisten Szenarien können dann zunächst in einer privaten Bibliothek abgelegt und nach Freigabe durch den Lieferanten schlussendlich für einen öffentlichen Zugriff bereitgestellt werden.

In Anlehnung an die in den Experteninterviews analysierten Rollenverteilungen, Wertversprechen, Schlüsselressourcen und Finanzierungsmechanismen bereits etablierter Szenariendatenbankenbetreiber, konnten die folgenden Schlussfolgerungen für den zu entwickelnden Anwendungsfall herausgearbeitet werden.

Das übergeordnete Ziel ist die Entwicklung einer Forschungsdatenbank mit der Möglichkeit auch Rohdaten einzuspielen. Der Fokus liegt auf der Bewertung der Sicherheit von AD/ADAS und der Integration möglichst vieler Datenlieferanten, beispielsweise auch Datenlieferanten ohne Simulationsexpertise aber zu Verfügung stehender verwendbarere Datensätze, wie Drohnenaufnahmen einer Autobahnauffahrt.

Die Ausgestaltung einer möglichen Datenaufbereitung als integraler Bestandteil der Datenbank ermöglicht die Partizipation einer breiten Nutzergruppe aus den verschiedenen Stakeholderclustern. Hierdurch wird eine größere Varietät an Daten und konsequent

auch eine höhere Anzahl an kritischen Szenarien geschaffen. Der bereits zusammengefasste Nutzen für Nutzer mit kommerziellem Interesse, beispielsweise OEMs und Zulieferer (Tier1), wird durch zur Verfügung stehende kritische und neue Szenarien im Bereich der Sicherheitsevaluation von AD/ADAS Systemen optimiert. Für Nutzer des öffentlichen Sektors mit gemeinnützigem Interesse entsteht der Zusatznutzen durch eine mögliche Sicherheitsevaluation verbauter Infrastruktur, des Verkehrsaufkommens und Verkehrsflusses sowie durch die mögliche Evaluierung neuer Maßnahmen, beispielsweise einer neuen Lichtsignalanlage und die prospektive und retrospektive Bewertung der Veränderung des Verkehrsgeschehens durch Fahrassistenzsysteme (Nutzenmaximierung durch die Anbindung der GIDAS Datenbank).

Aus dem Use-Case ergeben sich nutzergruppenabhängige Wertschöpfungsketten, welche die Partizipation an der Datenbank motivieren. Die abhängige Wertschöpfung stellt daher auch Anforderungen an den Nutzerzugang, welcher durch individualisierbare Filter in der Datenbanksuche an die jeweiligen Zugriffsrechte angepasst werden muss. Die Wertschöpfungsketten sind im Folgenden dargestellt.

Bild 20: Wertschöpfung gemeinnütziger Datenlieferant/Nutzer (Quelle: Eigene Darstellung)

Bild 21: Wertschöpfung kommerzieller Datenlieferant (Quelle: Eigene Darstellung)

Bild 22: Wertschöpfung kommerzieller Nutzer (Quelle: Eigene Darstellung)

Aus den geführten Interviews mit den Datenbankbetreibern sollten sich klare Wertversprechen ergeben: Der „ENVITED Marketplace“ fokussiert den Austausch bzw. Handel von verfügbaren Szenarien. Der „SafetyPool“ zielt auf die schnellere Absicherung von hochautomatisierten Fahrfunktionen durch Austausch von seltenen Szenarien ab. Beide Ergebnisse sind von Relevanz für die Nutzer (OEM), welche Fahrfunktionen für den Endnutzer entwickeln. Für unser Projekt sind OEM als relevante Nutzer der Datenbank Kern-Stakeholder, welche in einem Anreizmodell und damit durch einen Mehrwert zentral angesprochen werden müssen. Zwei Herausforderungen müssen damit gelöst werden: Erstens, die Herstellung eines Finanzierungsmodelles, welches zumindest kostendeckend betrieben wird. Zweitens, die Incentivierung der OEM durch Vorhaltung einer soliden Datengrundlage ab Start der Datenbank.

3.4.3 Workshopergebnisse: Use-Case-Evaluation und wahrgenommener Nutzen

Im Folgenden werden die im zweiten Stakeholderworkshop erörterten Erkenntnisse kurz zusammengefasst und die Einflüsse sowie der weitere Anpassungsbedarf der Projektergebnisse herausgearbeitet.

Zur Überprüfung und Validierung des erarbeiteten Use-Cases (vgl. Bild 19) sowie der erstellten Wertschöpfungsketten für gemeinnützige und kommerzielle Nutzer und Datenlieferanten lag der Fokus der Diskussionsrunde in den Stakeholderworkshops auf dem wahrgenommenen Nutzen zwei differenzierter Varianten des Use-Cases. Zum einen wurde ein in der Szenariendatenbank integrierter auditierender und datenschutzkonformer Server betrachtet, zum anderen kam eine Externalisierung der datenschutzkonformen Anonymisierung auf die Datenlieferanten in Frage (vgl. Bild 23 und Bild 24).

Der wahrgenommene Nutzen wurde hierzu je Nutzercluster (Öffentlich, Öffentlich-Privat, Privat) im Detail differenziert und in Bezug auf die zwei Use-Case Varianten gesetzt. Hierfür wurde zunächst der Nutzen der einzelnen Use-Cases auf Clusterebene abgefragt und anschließend allgemeine Vor- und Nachteile der zwei Varianten herausgearbeitet.

Use-Case DSGVO Cluster als Teil der Szenariendatenbank

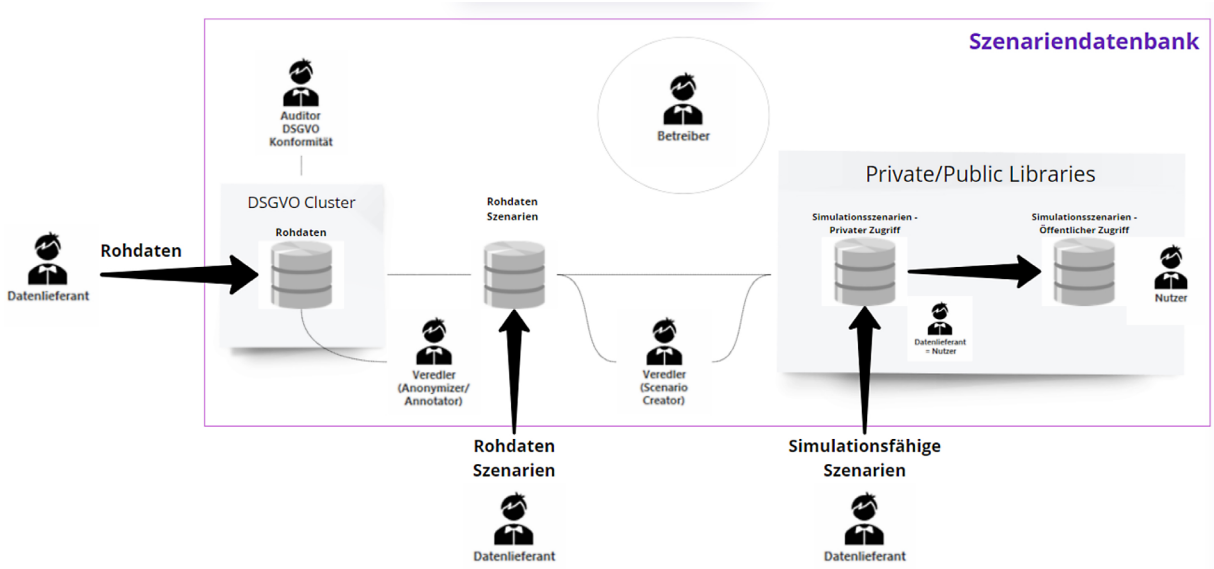


Bild 23: Use-Case Variation 1- DSGVO Cluster als Teil der Szenariendatenbank (Quelle: Eigene Darstellung)

Aus Sicht der öffentlichen Nutzer ergibt sich in Bezug auf die Identifikation neuer Prüfprozesse und Methoden sowie des weiteren Regelungsbedarfs der Nutzen der Partizipation. Weiterer Nutzen wird in der Möglichkeit zur Etablierung von Kontrollmechanismen und Lösungsmöglichkeiten auf einer breiten Datenbasis gesehen. Die Vorteile der Variante 1 bestehen in der einfacheren Internationalisierung der Datenbank durch die Anonymisierung als Teil der Datenbank, da hier verschiedene nationale Ansprüche des Datenschutzes berücksichtigt werden können. Zudem wird ein Vorteil in der breiteren Datenbasis aufgrund niedriger Hürden in der Datenlieferung gesehen.

Öffentlich-Private Akteure sehen großen Nutzen in der Vereinfachung der Zulassungs-, Abnahme- und Standardisierungsprozesse, sowie der Validierung von vorangegangenen Forschungsergebnissen. Eine große Hürde könnten die in der Forschung vorherrschenden Vertraulichkeitsvereinbarungen darstellen, welche (im Einklang mit datenschutzrechtlichen Vorgaben) die Herausgabe nicht anonymisierter Daten untersagen. Vorteile der Variante 1 werden in der einfacheren Abrechnung der Dienstleistungen sowie der größeren Datenvarietät gesehen, während die Verantwortungsverlagerung auf den Betreiber auch einen Nachteil in Bezug auf die Umsetzbarkeit darstellt.

Private Akteure sehen besonderen Nutzen in der Möglichkeit der Prozessautomatisierung der Anonymisierung durch KI-basierte Algorithmen sowie in den sich daraus ergebenen Marktchancen und Kostenminderungspotenzialen. Auch hier werden die geringeren Hürden der Datenlieferung als großer Mehrwert gesehen, da so eigene Tools validiert werden können und die Planungssicherheit der Hersteller steigt. Es wurden keine weiteren Vorteile gegenüber den anderen Clustern erkannt.

Use-Case DSGVO Cluster extern

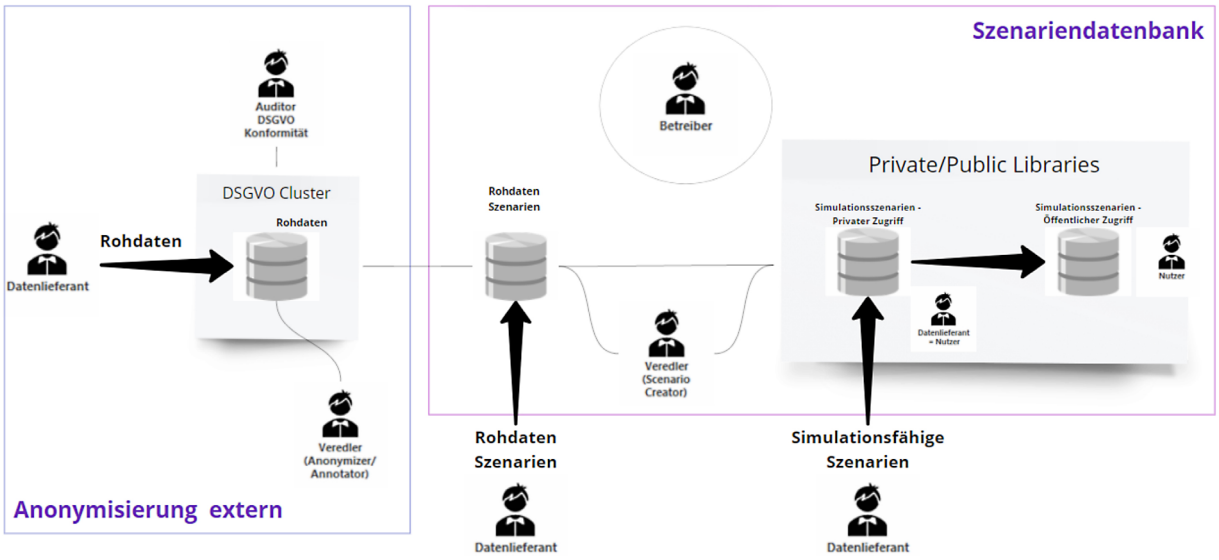


Bild 24: Use-Case Variation 2 - DSGVO Cluster extern (Quelle: Eigene Darstellung)

Die Variante 2 unterscheidet sich durch die Externalisierung der Anonymisierung der Datensätze. Hier müssten also die Datenlieferanten selbst die Anonymisierung vornehmen, welche im Anschluss nur noch durch den Datenbankbetreiber geprüft wird oder im Voraus vertraglich zwischen beiden Parteien (Anonymisierer und Betreiber) geregelt sein muss. Für reine Nutzer der Datenbank ergibt sich also kein Zusatznutzen, aber auch keine Nutzenminderung bei Variante 2. Dies spiegelt sich auch in den Workshopergebnissen wider.

Mit Fokus auf die Vor- und Nachteile der Variante 2 ergibt sich jedoch ein klares Bild der überwiegenden Nachteile. Dies ist erklärbar durch die Verantwortungsverlagerung vom Betreiber zum Datenlieferanten und dem vorrangegangen Projektergebnis, wonach sich die Mehrheit der Stakeholder in zweiter Rolle sieht. Aufgeführte Nachteile der öffentlich-privaten Akteure umfassen die Mehrfachentwicklung der KI-basierten Algorithmen zur Anonymisierung und den Ausschluss aller Datenlieferanten, welche entweder keine Expertise in diesem Bereich haben oder nicht in monetäre Vorleistung gehen können. Öffentliche Akteure sehen die erschwerte Nachvollziehbarkeit der Lieferkette als Problem, während von diesem Cluster auch der einfachere Betrieb der Datenbank als großer Vorteil angeführt wird. Private Akteure sehen Vorteile in der geringeren Hürde der Partizipation für Veredler, da diese in Variante 2 nicht Teil der Datenbank sind und somit ihre mit weniger Pflichten verbundene Dienstleistung ausführen können.

3.4.4 Analyse bestehender Lösungen aus Nutzersicht

Es lässt sich feststellen, dass weltweit unterschiedliche Initiativen und auch schon etablierte Datenbanken existieren. Hinsichtlich der Unfalldatenbanken gibt es neben der GIDAS-Datenbank auf der jeweiligen nationalen Ebene diverse zu nennen. Das IGLAD schließt

dabei eine Klammer um diese. Hier handelt es sich dann aber nicht immer um simulierbare Szenarien. Im ADAS/AD-Bereich lassen sich weitere Datenbanken verschiedenster Art identifizieren (ApolloScape, PandaSet, Waymo Open Dataset, Level 5, NuScenes, etc.). Auch liefern Driving Studies wie UDrive entsprechende Daten, die dann ebenfalls in einer Datenbank genutzt werden könnten. Dies würde immer eine Kooperation mit entsprechender Incentivierung mit sich bringen, um entsprechende Daten in einer Kooperativen Datenbank zu nutzen. Dies ist auch in der ursprünglichen technischen Rahmenarchitektur vermerkt (Vgl. Bild 4).

Die bekanntesten Szenario-Datenbanken sind zum einen die Musicc Database (UK), SafetyPool (UK) und ADScene (Frankreich). Obgleich ADScene laut Roadmap-Planung erst Ende dieses Jahres an den Markt gehen wird, sind die Ähnlichkeiten zu SafetyPool und dem vorliegenden Projekt signifikant:

- Anbindung von Unfalldatenbank (aktuell national beschränkt)
- Einbindung von Stakeholder wie Bund, Land, Kommune
- Partnernetzwerk auch mit OEMs, Tier1 und entsprechenden Geldgebern
- Private & Public Libs
- ODD-basiertes Tagging

Der folgende Abschnitt hat zum Ziel die Kernfunktionalitäten des entwickelten Use-Cases im Vergleich zu bereits existierenden Datenbanken wie SafetyPool und ENVITED zu analysieren. Dafür wurden in Tabelle 10 und Tabelle 11 untersucht, inwiefern Kernfunktionalitäten der interviewten Datenbanken mit denen des Use-Case Szenarios übereinstimmen und welche Vor- und Nachteile sich aus Sicht der Nutzer ergeben würden. Aspekte, die als gleich beurteilt wurden, sind in den Tabellen nicht erneut aufgeführt worden. Dazu zählen unter anderem folgende Bereiche:

- Akzeptanz aller gängigen Dateiformate
- Entscheidung, ob simulationsfähige Szenarien privat oder öffentlich zur Verfügung gestellt werden, erfolgt durch den Datenlieferanten
- Angebot der Simulationsszenarien zum Tausch/Verkauf

Des Weiteren besitzen sowohl ENVITED als auch SafetyPool ähnliche Kernfunktionalitäten wie der Use-Case und visieren eine Vielzahl von Szenarien (insbesondere Corner Cases) und die Nutzung dieser zur ODD-Definition sowie Prüfung an. Der Use-Case besitzt darüber hinaus zusätzliche Kernfunktionalitäten, die die Stakeholdergruppen unterschiedlich ansprechen. Dazu zählen unter anderem:

- Funktion als Datengrundlage für weitere Gesetzgebungen und Ableiten von Verkehrssicherheitsmaßnahmen
- Bereitstellung von Grundlagen zur Ausweitung der technischen Kompetenz
- Identifizierung des Bedarfs von Infrastruktur, technischen Diensten, KI-Systemen, Tools und weiteren Geschäftsmodellen (F&E)
- Absicherung neu entwickelter Fahrfunktionen für Hersteller
- Zugang zur IT-Infrastruktur und vereinfachtes Datenmanagement

Wie aus Tabelle 10 und Tabelle 11 hervorgeht, bestehen insbesondere Unterschiede in der Rechtsform (vgl. Analyse der rechtlichen Rahmenbedingungen), da ENVITED eine Ver-

einsstruktur mit statischem Mitgliedsbeitrag besitzt. Für SafetyPool konnte keine genaue Rechtsform ermittelt werden. Darüber hinaus fordert ENVITED als Mitgliedsvoraussetzung Expertise im AD/ADAS Bereich, wodurch eine deutliche Zugangsbeschränkung erfolgt, während sowohl der Use-Case als auch SafetyPool offen gegenüber allen Stakeholdergruppen sind. In Bezug auf die Veredlung sowie Auditierung verfolgen die interviewten Datenbanken unterschiedliche Ansätze. Aus Nutzersicht profiliert sich der Use-Case dabei vor allem durch die Gewährleistung der DSGVO Konformität und setzt somit einen deutlichen Anreiz zur Nutzung der Szenariendatenbank.

Aus der Analyse der bestehenden Lösungen im Vergleich zum entwickelten Use-Case geht hervor, dass aus Nutzersicht bereits Bedürfnisse durch am Markt existierende Datenbanken abgedeckt sind. Der Use-Case zeichnet sich im Gegensatz zu den schon bestehenden Datenbanken durch den zuvor angesprochenen größeren Umfang an Kernfunktionalitäten aus und bietet dem Nutzer somit einen Zusatznutzen. Außerdem spricht der Use-Case durch seine flexible Paketierungsmöglichkeit und der daraus folgenden Differenzierung

Rolle	**Kernfunktionalität**	**Beschreibung aus Nutzersicht**
Datenlieferant	Mitgliedsbeitrag	+ Kalkulierbarer Vereinsbetrag - gleichbleibende Mitgliedsbeiträge ohne Nutzenabhängigkeit ≠ Mitgliedsbeitrag und zusätzliche Dienstleistung durch Paketierung (kostenloser Zugang für nur Datenlieferanten)
	Mitgliedsvoraussetzung ADAS Kenntnisse	+ Sicherstellung der Expertise, da ausschließliche Teilnahme fachspezifischer Einrichtungen - Ausschluss aller Stakeholder ohne Nachweis von Expertise in AD/ADAS Systemen ≠ Keine Restriktion
Incentivierung	Monetarisierung	≈ Möglichkeit der Monetarisierung von zur Verfügung gestellten simulationsfähigen Szenarien
Veredler	Veredler/Anonymisierung in externem Cluster	- mehr Verantwortung/Kosten ≠ Datenlieferanten- und Nutzungsabhängige Datenveredlung und Anonymisierung
Betreiber	Vereinsstruktur	+ Stakeholderstruktur, Mitbestimmung - gleichbleibende Mitgliedsbeiträge ohne Nutzenabhängigkeit ≠ Vereinsstruktur nicht angestrebt
Auditor	keine Auditierung	+ weniger Kosten - notwendig zur Sicherstellung der DSGVO-Konformität ≠ Sicherstellung DSGVO-Konformität durch externen Auditor
	Qualitätsstandard durch Traceability	+ Geringere Kosten, weniger Verantwortung - Zustimmung zur Nachverfolgung erforderlich ≈ Qualitätssicherung durch Traceability möglich, Qualitätssicherung abhängig von Ausgestaltung
Nutzer	Kernfunktionalität	≈ Nutzung für Simulation und ODD-Definition
Incentivierung	Monetarisierung	+ Vergünstigung und Möglichkeit zum Datenmanagement ≈ Nutzergruppenoptimiertes Datenmanagement
Legende	+ - = ≈ ≠	Vorteil Nachteil Übereinstimmung Ähnlichkeit Unterschied

Tab. 10: Vergleich der Nutzenabdeckung (ENVITED marketplace)

Rolle	Kernfunktionalität	Beschreibung aus Nutzersicht
Datenlieferant	internationale Ausrichtung	≈ Grundsätzlich möglich, aber nicht vorgesehen
	kostenloser Zugang	+ Anreiz durch kostenlosen Zugang ≠ Zugang gegen Mitgliedsbeitrag (außer reine Datenlieferanten)
Incentivierung	Punktesystem	≈ Punktesystem und Möglichkeit zur Monetarisierung
Veredler	Betreiber als Veredler	+ Expertise der Datenaufbereitung - Abhängigkeit ≠ Abhängig von Betreiberstruktur
Betreiber	Kernbetrieb durch Deepen AI	≈ Betreiber wird laut Befragung im privaten Bereich gesehen (beispielsweise Toolhersteller, IT-Infrastruktur)
	Drittmittelfinanzierung	≈ Deckung der Kosten durch Geschäftsbetrieb oder Fördermittel
Auditor	keine Auditierung	+ weniger Kosten - notwendig zur Sicherstellung der DSGVO-Konformität ≠ Sicherstellung DSGVO-Konformität durch externen Auditor
Nutzer	Kernfunktionalität	≈ Nutzung für ODD-Definition, Integration von Policy Makers
Legende	+ - = ≈ ≠	Vorteil Nachteil Übereinstimmung Ähnlichkeit Unterschied

Tab. 11: Vergleich der Nutzenabdeckung (SafetyPool)

der Nutzerzugänge unterschiedliche Stakeholdergruppen an. Die folgende Analyse soll als Entscheidungsgrundlage für Ansätze zur Kooperation, Auslagerung bzw. Einbindung mit bestehenden Datenbanken dienen.

3.4.5 Zwischenfazit

In Bezug auf die Workshopergebnisse setzt der Use-Case vor allem in der Besetzung der Veredler- sowie Auditorrolle verschiedenste Anreize wie die Möglichkeit der Auslagerung oder Finanzierung durch Drittmittel, um unter anderem den Hemmnissen eines möglicherweise defizitären Betriebs entgegenzuwirken. Darüber hinaus wurde deutlich, dass durch die Sicherstellung der DSGVO Konformität und den angebotenen Zusatznutzen der Use-Cases deutliche Anreize geschaffen werden. Mehrfach betont wurde dabei, dass für die Incentivierung privater Akteure in der Betreiberrolle vor allem der strategische Marktvorteil deutlich hervorgehoben werden muss. Der Vergleich der Kernfunktionalitäten zwischen den interviewten Datenbanken und dem Use-Case aus Nutzersicht zeigt auf, dass der Use-Case diese Vorteile durch seine Wertangebote und Schlüsselfunktionen (vgl. Bild 13) bedient.

Aus den beschriebenen Ergebnissen und der Diskussion im Workshop lassen sich allgemeine Schlussfolgerungen ableiten. Gegeben durch die angesprochene Automatisierung des Anonymisierungsprozess könnten dem Auditor weitere Aufgaben zukommen. Neben der Entwicklung des KI-basierten Algorithmus, durch beispielsweise einen Toolentwickler, müsste auch eine Kontrollinstanz die tatsächliche DSGVO-Konformität der anonymisierten Datenformate überprüfen.

Zusätzlich ergab sich aus dem Gesprächsverlauf die Sichtweise der Teilnehmenden, dass sich die zwei Use-Cases nur für Datenlieferanten bzw. den Betreiber unterscheiden und

besonders für reine Nutzer den gleichen Nutzen bieten. Es wäre aus Sicht der Teilnehmenden vorstellbar, ein modulares System zu entwickeln, in welchem beispielsweise der Service der integrierten Anonymisierung direkt über die zu entrichtende Gebühr für den Datenbankzugang abgerechnet wird. Andererseits könnten auch externe Dienstleister mit der Anonymisierung beauftragt werden, um die zu entrichtende Gebühr zu verringern. Es könnten auch alle in der Datenbank angebotenen Dienstleistungen zu einer Grundgebühr modular hinzugebucht werden. Nachteilhaft wäre hierbei der steigende Aufwand durch diverse Vertragsbeziehungen mit den einzelnen Partizipanten der Szenariendatenbank, gegenüber dem Vorteil der Flexibilität.

3.5 Lastenheft für die kooperative Datenbank

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 Grundlage 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 weiterhin den Aufbau einer hinreichenden Datenbasis und die kontinuierliche Weiterentwicklung auf Grundlage des technologischen Fortschritts und der 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 kann.

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 Anwendungsfällen und rollenabhängigen Bedürfnissen an Datengrundlagen, Datenzugängen und Datenbankfunktionen.

Durch die Betrachtung der unterschiedlichen Nutzerinteressen und der 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 zweiten Stakeholder-Workshop wurden 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. Das Lastenheft ist dem finalen Schlussbericht als Anhang (A4) beigelegt.

3.6 Technische Validierung

Ausgehend von den Datenquellen muss sichergestellt werden, dass eine Konvertierung der Ausgangsdaten (Rohdaten in Form von Kamera, Lidar oder andere Formate wie die Pre-Crash-Matrix der GIDAS-Datenbank oder auch Map-Daten) in ein simulierbares Szenario durchgeführt werden kann und dementsprechend korrekte Szenarien für die Datenbank liefert.

- Scenario-Erstellung mit Hilfe der PCM der GIDAS Unfalldatenbank:
  Die Unfalldatenbank GIDAS stellt die sogenannte PCM (Pre-Crash-Matrix) bereit. Diese Daten können dazu verwendet werden, simulierbare Szenarien zu erzeugen. Im Wesentlichen beinhaltet die PCM den Fall (eindeutige ID), die entsprechenden Objekttypen (z. B. Bäume, Straßenmarkierungen, etc.) mit eindeutigen IDs sowie (x,y,z)-Koordinaten der dynamischen Objekte in einem entsprechenden Zeitraster. Die PCM-Daten lassen sich in simulierbare Szenarien überführen und für die Absicherung verwenden (vgl. Bild 25).

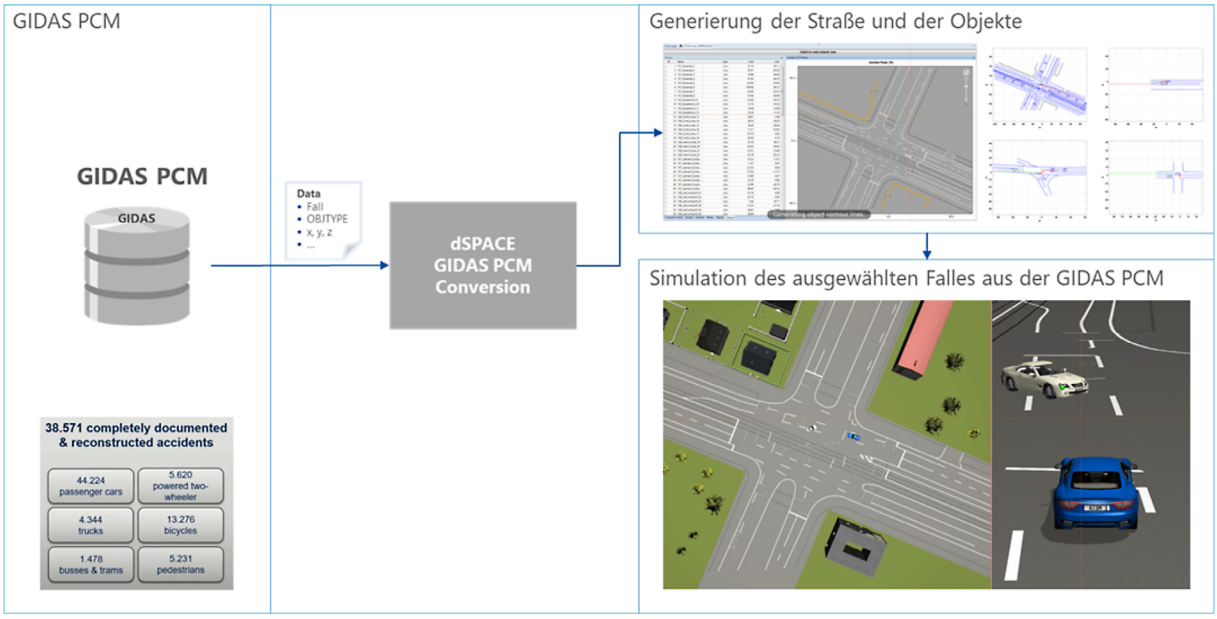


Bild 25: Scenario-Erstellung mit Hilfe der PCM der GIDAS Unfalldatenbank (Quelle: Eigene Darstellung)

- Scenario-Erstellung auf Basis von MAP-Data:
  Für Szenarien ist die Straßeninformation ein essentieller Bestandteil. Die Straßeninformationen werden dann häufig durch (HD-)Maps (z. B. Tom, OSM, oder HERE) bereitgestellt. Diese müssen dann in ein simulationsfähiges Format (z. B. OpenDrive oder proprietäre Formate) überführt werden. In Bild 26 ist exemplarisch die Konvertierung von TomTom-Daten in ein dSPACE Simulationsszenario dargestellt.

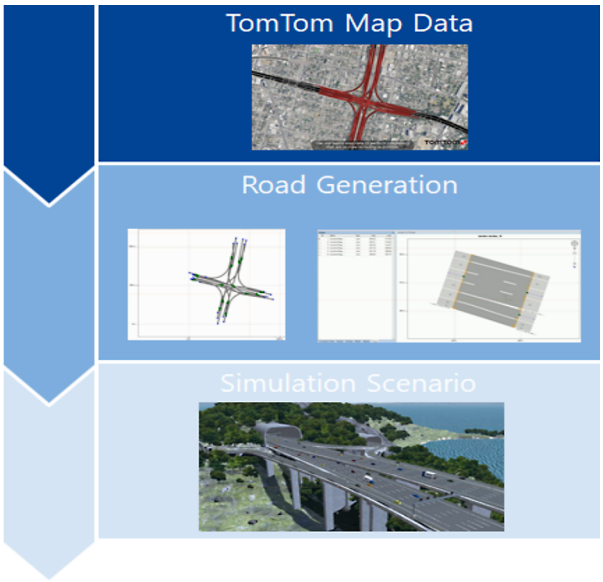


Bild 26: Scenario-Erstellung auf Basis von MAP-Data (Quelle: Eigene Darstellung)

- Scenario-Erstellung basierend auf Rohdaten (Kamera, Lidar und Maps):
  Um sicherzustellen, dass die aufgezeichneten und annotierten Daten auch der Simulation entsprechen, müssen die Daten hinsichtlich der physikalischen Modellierung (der Vehicle Dynamics für das EGO) mitberücksichtigt werden. Dabei dienen die annotierten Daten (die Labels) als die Ground-Truth. Um die Genauigkeit quantifizieren zu können, werden typischerweise Scatter- und Quiver-Plots verwendet, die die Fahrsituation in

(x,y,z) abbilden und dann den Fehler bzgl. der Position darstellen. Ein Beispiel eines Scatter-Plots wird in Bild 27 veranschaulicht.

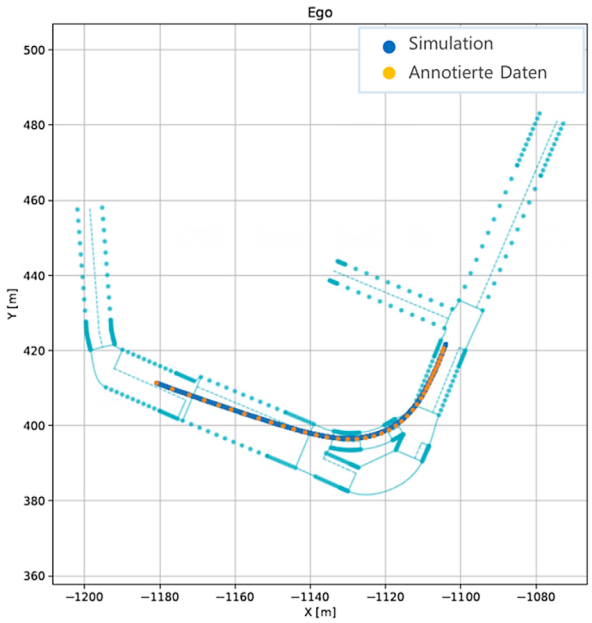


Bild 27: Beispielhafte Darstellung eines Scatter-Plots (Quelle: Eigene Darstellung)

Neben dem Vergleich der Position sind auch Metriken für Geschwindigkeit und Abstand zu den entsprechenden Teilnehmern der Simulation zu prüfen. Unter der Annahme, dass sich die Fahrzeuge und die anderen Verkehrsteilnehmer zum richtigen Zeitpunkt am richtigen Ort befinden, ist davon auszugehen, dass auch der relative Abstand validiert ist. Entsprechend können dann aus den Vergleichen validierte Szenarien in die Datenbank eingespeist werden. In Bild 28 sind exemplarisch zwei Vergleiche von Verkehrssituation gegenübergestellt (Messdaten vs. Simulation).

Bild 28: Exemplarischer Vergleich Messdaten vs. Simulation (Quelle: Eigene Darstellung)

Neben der Konvertierung der Messdaten stellt auch die Organisation der Szenarien einen wichtigen Aspekt der Szenariendatenbank dar. Hierzu müssen die Szenarien mit Metadaten versehen werden können. Idealerweise orientieren sich die Metadaten an einer ODD

Taxonomie (z. B. OpenODD oder BSI PAS 1883). Das Verschlagworten und die Nutzung von Metadaten ist typischerweise ein Teil gängiger Datenbanksprachen wie SQL oder SPARQL. In Bild 29 und Bild 30 ist exemplarisch die Verschlagwortung und die Suchfunktion des dSPACE Toolings SIMPHERA dargestellt.

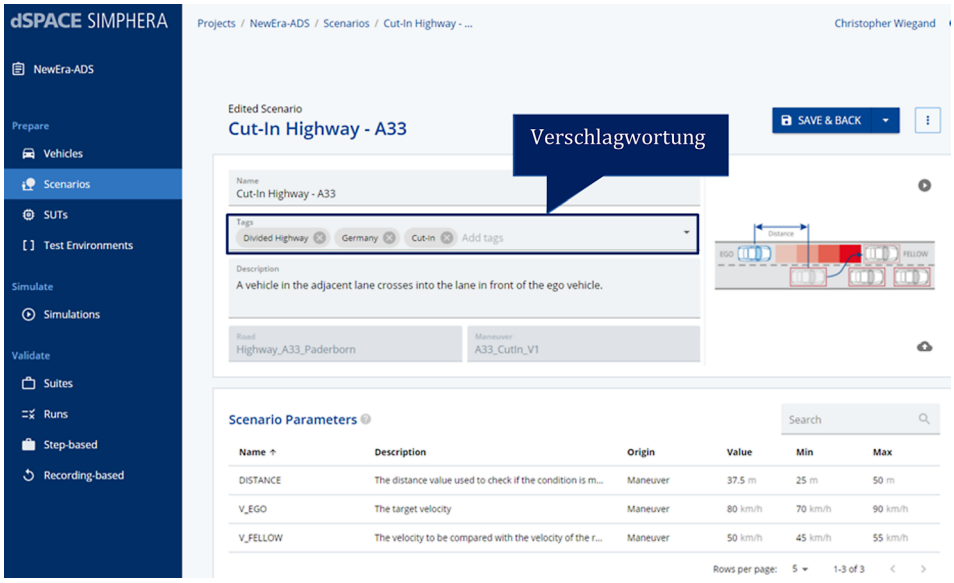


Bild 29: Screenshot 1 von dSPACE Tooling SIMPHERA (Quelle: Eigene Darstellung)

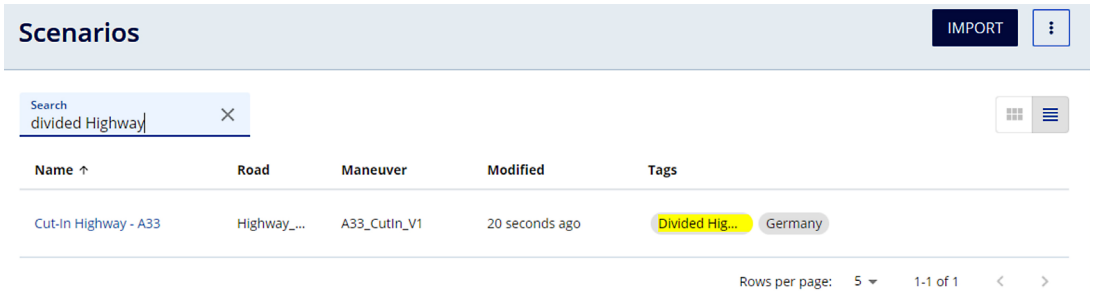


Bild 30: Screenshot 2 von dSPACE Tooling SIMPHERA (Quelle: Eigene Darstellung)

3.7 Ableitung von Handlungsempfehlungen

3.7.1 Rechtliche Handlungsempfehlungen

Im Folgenden werden praktische rechtliche Handlungsempfehlungen dargelegt und auf Grundlage rechtlicher Prüfungen erweitert, um weitere Aspekte (insbesondere denkbare Rechtsformen des Datenbankbetriebs sowie konkrete Anforderungen an die datenschutzrechtliche Einordnung als Forschungsdatenbank) zu berücksichtigen. Diese wurden zudem das beiliegende Rechtsgutachten und das Positionspapier (siehe Anhang A1 und A2) eingearbeitet.

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),[105] 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 zu können und auf diese Weise die finalen Datensätze gegen Manipulationen abzusichern. 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.

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 Gesichtern und Kennzeichen vorzugswürdig.[106] Während Kameradaten auch Verkehrsschilder und Fahrbahnmarkierungen und eine Aufzeichnung von anderen Verkehrsteilnehmern (Fußgängern, Radfahrern) und Fahrzeugen ermöglichen[107] und somit für Verkehrsszenarien wesentliche Informationen enthalten, geben Lidardaten bloße Punktewolken wieder, die die Entfernung zu Gebäuden, Verkehrsteilnehmern usw. in der Fahrumgebung anzeigen[108]. Auf den konkreten Fall bezogen kann der Verarbeitungszwecks, die Szenarienerstellung, mit Lidarinformationen nicht erreicht werden. Auch Radardaten geben lediglich Entfernungswerte zu Umgebungsobjekten wieder[109] 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[110] 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.

---

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

[106] Bundesministerium für Wirtschaft und Energie "Praxishilfe zum Datenschutz in Reallaboren", 2021, S. 19.

[107] Kleinschmidt/Wagner „Technik autonomer Fahrzeuge" in Oppermann/Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020, Rn. 26.

[108] Kleinschmidt/Wagner „Technik autonomer Fahrzeuge" in Oppermann/Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020, Rn. 26.

[109] Kleinschmidt/Wagner „Technik autonomer Fahrzeuge" in Oppermann/Stender-Vorwachs „Autonomes Fahren – technische Grundlagen, Rechtsprobleme, Rechtsfolgen", 2. Auflage 2020, Rn. 26.

[110] Bundesministerium für Wirtschaft und Energie "Praxishilfe zum Datenschutz in Reallaboren", 2021, S. 21.

Es lässt sich auf diese Weise nicht garantieren, dass die Daten in jedem Fall tatsächlich anonym sind, sodass hilfsweise daneben schützende Maßnahmen ergriffen (und dokumentiert) werden sollten, um die Verarbeitung der Daten hilfsweise DSGVO-konform zu gestalten.

3. Hilfsweise (falls dennoch personenbezogene Daten in die 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)nutzer vor Fahrtantritt oder generell im Rahmen der Einstellungen verschiedener Nutzerprofile. 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.[111] Aus diesem Grund ist ein Hinweis sinnvoll, dass die Daten auch nach Wegfallen der Einwilligung auf anderer Grundlage verarbeitet werden können.[112]

   b. Erforderlichkeit zur Vertragserfüllung
   Mit Blick auf neuartige Geschäftsmodelle, die auf den Fahrzeugerwerb oder fahrzeugbezogene Leistungen gerichtet sind, 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.[113] Handelt es sich um sensible Daten, so ist eine Rechtfertigung der Verarbeitung gemäß Art. 6 Abs. 1 lit. b DSGVO ausgeschlossen.[114]

   c. Gesetzlicher Rechtfertigungsgrund in Form der Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO (für private Datenverarbeitende)
   Auf die 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[115], das Einbeziehen zusätzlicher Kontrollmaßnahmen (unabhängige Überwachungsinstanzen),[116] die Einbindung von Datentreuhändern[117] sowie das Vorsehen einer besonders engen Zweckbindung und einer besonders kurzen Verarbeitungsdauer[118].

---

111 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
112 Rat für Sozial- und Wirtschaftsdaten „Handreichung Datenschutz“, 2. Auflage 2020, S. 28.
113 Buchner, „Datengetriebene Geschäftsmodelle rund um das vernetzte Auto“ in Roßnagel/Hornung „Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzen Fahrzeug, 2019, S. 62 ff.
114 Art. 9 Nr. 1 DSGVO.
115 Kotter „Datenschutz beim vernetzten und autonomen Fahren Welche Rahmenbedingungen können sensible Daten schützen?“ 2019, S. 36.
116 Bundesministerium für Wirtschaft und Energie „Praxishilfe zum Datenschutz in Reallaboren”, 2021, S. 26.
117 Schantz in Simitis/Hornung/Spiecker, Datenschutzrecht, 1. Auflage 2019, Art. 6 Abs. 1 DSGVO Rn. 114.
118 Bundesministerium für Wirtschaft und Energie „Praxishilfe zum Datenschutz in Reallaboren”, 2021, S. 26.

4. Sämtliche Verarbeitungs-/Informations-/und Abwägungsprozesse sind zudem umfassend (mit Blick auf Haftungsrisiken über die allgemeine Rechenschaftspflicht hinaus)[119] zu dokumentieren um Betroffenenrechten und Nachweispflichten (beispielsweise zwecks Exkulpation gemäß Art 82 DSGVO)[120] nachkommen zu können. Daneben empfiehlt sich, wenn nicht ohnehin die Verpflichtung greift, die Bestellung eines Datenschutzbeauftragten gemäß Art. 37 Abs. 4 S. 1 DSGVO als zusätzliche Sicherheitsmaßnahme vorzusehen, der dabei hilft die Datenverarbeitenden über datenschutzrechtliche Verpflichtungen zu unterrichten sowie deren Einhaltung zu überwachen, vgl. Art. 39 Abs. 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. Das Konzept des Forschungsvorhabens (insbesondere Fragestellung, Verantwortlichkeiten, herangezogene Datenarten, ggf. Abwägungsgründe, Methodik, Gemeinschaftsnutzen und die Veröffentlichung der wesentlichen Ergebnisse)[121] 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 kommerzielle Nutzung und der Bereich der Forschung und Entwicklung voneinander getrennt sind, sodass sich das Aufziehen einer ausgelagerten Forschungsdatenbank empfiehlt.[122] 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) Interessen 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,[123] datenschutzrechtliche Verhaltensregeln zu entwerfen und der Behörde zur Genehmigung vorzulegen. Vorlageberechtigt sind neben klassischen Vereinen und Verbänden sämtliche freiwillige Zusammenschlüsse, soweit diese eine bestimmte homogene Gruppe vertreten, nicht jedoch einzelne Unternehmen. [124] Genehmigte Verhaltensvorgaben generieren eine gewisse Rechtssicherheit dahingehend, dass die abstrakten Vorschriften der DSGVO eine branchenspezifische Präzisierung und Konkretisierung erfahren.[125] Ab Bestandskraft der Genehmigung ist die Datenschutzbehörde an die genehmigten Regeln bei Auslegung der DSGVO gebunden,[126] mit Blick auf eine gerichtliche Überprüfung ist das genehmig-

---

[119] BeckOK DatenschutzR/Quaas, 36. Ed. 1.5.2021, Art. 82 DSGVO Rn. 19.
[120] BeckOK DatenschutzR/Quaas, 36. Ed. 1.5.2021, Art. 82 DSGVO Rn. 19.
[121] Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (20, 23).
[122] Bundesministerium für Wirtschaft und Energie “Praxishilfe zum Datenschutz in Reallaboren”, 2021 S. 29.
[123] Roßnagel in Simitis, Spiros/Hornung/Spiecker, Indra gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 40 DSGVO Rn. 32.
[124] Ebenda, Rn. 33.
[125] Ebenda, Rn. 1.
[126] Ebenda, Rn. 69.

te Regelwerk indes unverbindlich.[127] 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.[128] Darüber hinaus kann auch über die gesetzlich vorgesehenen Kooperationen mit der Aufsichtsbehörde ein informeller Austausch angestrebt werden.[129]

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.

3.7.2 Regulierungspotenzial mit Blick auf den des nationalen Rechtsrahmen

Neben der Anpassung des gesamten europäischen Datenschutzrechts (insbesondere der DSGVO), was realistisch allenfalls eine mittel- bis langfristige Option darstellt,[130] besteht die kurz- bis mittelfristig realisierbare[131] Möglichkeit innerhalb der den Mitgliedstaaten verbleibenden Regelungsspielräume punktuell nationale Vorgaben zu treffen.[132]

Mit Blick auf die Verarbeitung von Daten, die erforderlich ist, um rechtliche Verpflichtungen 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.[133] Die Anforderungen an die Rechtsgrundlage werden abstrakt

---

[127] Ebenda, Rn. 68.
[128] 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.
[129] Ebenda, S. 51.
[130] Ebenda, S. 56.
[131] 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. 60.
[132] Ebenda, S. 53.
[133] Ebenda, S. 57.

in Art. 6 Abs. 3, S. 2 f. DSGVO definiert. [134] Die Rechtsgrundlage kann neben bundes- oder landesrechtlicher auch satzungsrechtlicher Natur (kommunale Satzungen oder Satzungen anderer juristischer Personen), mangels Außenwirkung nicht aber Verwaltungsvorschrift sein.[135]

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.[136]

Der in Deutschland bestehenden Überregulierung von Forschungsdaten sollte durch gesetzliche Anpassungen begegnet werden, Wertungswidersprüche sind zu beseitigen, bereichsspezifische Datenschutznormen sind zu harmonisieren.[137]

3.7.3 Technische Umsetzungsempfehlungen

Um den unterschiedlichen Arbeitspaketen im Sinne einer kollaborativen Datenbank Rechnung zu tragen, ist eine hochgradig modulare Struktur vorzusehen. Für eine kollaborative Datenbank ist es essentiell sie entsprechend in der Cloud zur Verfügung zu stellen. Weiterführend ist eine Kompatibilität regional (z. B. Alibaba in China, AWS, etc.) zu gewährleisten. Diese modulare Struktur sieht vor, unterschiedliche Datensätze, und Datenbanken kontinuierlich anbinden zu können, ohne die Daten/Szenarien zwingend konvertieren zu müssen (vgl. Bild 4). Weiter muss auch berücksichtigt werden, dass im Falle von Rohdaten und auch Rohdaten-Szenarien rechtliche Aspekte wie Privatheit der Person im Sinne eines DSGVO-Servers Berücksichtigung finden und diese Daten gemäß des Use Cases Training von KI oder der entsprechenden Absicherung auch im Rahmen von Forschungsaktivitäten nutzbar sind. Neben der Abdeckung der in den unterschiedlichen Arbeitspaketen dokumentierten Anwendungsfällen soll diese Modularität auch dazu genutzt werden, eine kontinuierliche Weiterentwicklung zu ermöglichen, und die verschiedenen Aspekte der Architektur effizient und kontinuierlich pflegen und erweitern zu können, bzw. die Möglichkeit zu schaffen, in Phasen Ausbaustufen der kollaborativen Datenbank bereitzustellen.

Neben der Anbindung bereits existierender Datenbanken oder Datensätze ist eine native Datenbank vorgesehen. Jedem Szenario in der nativen Datenbank sind Metadaten zugeordnet, die unter anderem beschreiben welche Aspekte der ODD abgedeckt sind, welches Manöver (z. B. Cut-In oder Cut-Out) ausgeführt wird, woher das Szenario kommt, wie es erstellt wurde (d. h. künstliches Szenario erstellt durch Experten oder ein Szenario erstellt aus Messdaten) und zu welchem Zweck es verwendet werden kann (z. B. ALKS, AEB) oder auch ob eine 3D-Umgebung vorliegt, bzw. für welchen Simulator (z. B. dSPACE SIMPHERA oder CARLA) dieses Szenario erstellt wurde. Neben fest definierten Metadaten, die nur durch den Betreiber verändert werden können, beispielsweise über eine signierte XML-Datei, sollen Metadaten auch durch die Nutzer erweitert werden können, um anwenderspezifische Suchanfragen und Kategorisierungen vornehmen zu können. Tiefergehende Anforderungen an die Metadaten sind im Lastenheft zu finden.

Um Szenarien möglichst einfach finden zu können, ist neben den angesprochenen Metadaten auch eine Ontologie vorgesehen, die es ermöglicht, aus den Suchanfragen Ableitungen zu ziehen, welche Szenarien noch relevant sein können. Dabei erzeugt die Ontologie auf

---

[134] Frenzel in Paal, Boris/Pauly, Daniel, DSGVO und BDSG, 3. Aufl. 2021 Art. 6 DSGVO, Rn. 37.
[135] Ebenda, Rn. 36.
[136] Pauly in Paal, Boris/Pauly, Daniel, DSGVO und BDSG, 3. Aufl. 2021, Art. 89 DSGVO Rn. 13.
[137] Weichert „Die Forschungsprivilegierung in der DSGVO“, ZD 2020, 18 (23).

Basis einer Suchanfrage weitere Queries und durchsucht die angebundene native Datenbank aber auch die angebundenen Datasets/Datenbanken. Damit eine solche erweiterte Suchanfrage für alle angebundenen Datenbanken funktionieren kann, ist eine Mapping-Vorschrift zwischen der Ontologie und jeder angebundenen Datenbank zu implementieren, da sich das Vokabular der einzelnen Datenbanken grundsätzlich unterscheidet.

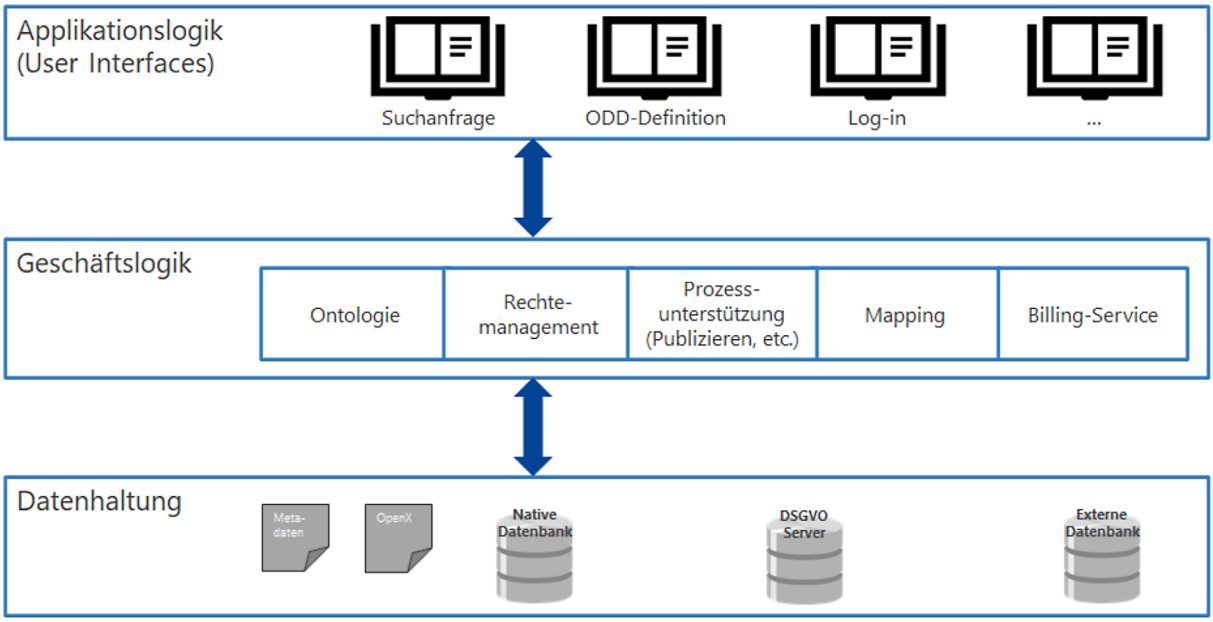


Bild 31: Schematische Darstellung der kollaborativen Datenbank unterteilt in Applikationslogik, Geschäftslogik und Datenhaltung (Quelle: Eigene Darstellung)

Im Kontext der Simulations-Szenarien sind die OpenDrive, OpenCRG und OpenScenario ASAM Standards zu unterstützen, um zu gewährleisten, dass diese Szenarien möglichst plattform-agnostisch genutzt werden können, d. h. dass diese Szenarien in kommerziellen Simulationsumgebungen aber auch in Open Source Umgebungen als Simulationsartefakte mit simuliert werden können und durch Stakeholder wie OEMs, Tier1s oder auch Tech-Unternehmen in der Entwicklung und Absicherung von Fahrerassistenzsystemen oder Systemen für das automatisierte Fahren Verwendung finden.

In den vorhergehenden Absätzen wurden die wesentlichen Aspekte der Datenhaltung und der Anwendungs-/Geschäftslogik eruiert (vgl. Bild 31), wobei dort ein entsprechendes Rechtemanagement sowie der Billing-Service verortet ist. Das Rechtemanagement sieht vor, dass nicht alle Inhalte grundsätzlich für alle zugänglich sind, da zum einen der Zugriff auf Rohdaten sowie der Zugriff auf entsprechende externe Datenbanken gemäß der Berechtigung einzuschränken ist. Die Benutzerschnittstelle, d. h. der Zugang zu den Szenarien ist geprägt durch einfache, aber auch sehr hochwertige Suchfunktionen. Dabei stellt die Benutzerschnittstelle die Definitionen der ODD zur Verfügung, die dann in ein komplexes Query (Suchanfragen die über logische Operatoren miteinander verknüpft sind) umgesetzt wird. Als Basis für die Taxonomie ist BSI PAS 1883 zu verwenden oder vorzugsweise, wenn schon ausdefiniert, ASAM OpenODD. Mit Hilfe der Definition der ODD innerhalb der Benutzerschnittstelle lassen sich so einfach in tabellarischer Form die Szenarien, die für diese definierte ODD infrage kommen, identifizieren und auch anzeigen. Es wird damit ersichtlich, wo schon eine ausreichende Überdeckung vorliegt und wo noch Lücken in der ODD-Abdeckung bestehen. Auch kann zu diesem Zeitpunkt schon identifiziert werden, auf welchen Ebenen (z. B. Perception oder Motion Planning) der Teststrategie noch Inhalte fehlen. Neben den möglichen Suchanfragen und der Erweiterung der Metadaten

ist auch das Hochladen eigener Inhalte ein Mechanismus, der der Benutzerschicht hinzuzufügen ist. Dabei können Inhalte lokal nur für den einzelnen Nutzer sichtbar integriert werden, aber auch entsprechend in die native Datenbank publiziert werden. Es ist jedoch nicht möglich ohne Freigabe durch den Betreiber direkt zu publizieren. Vielmehr wird die Publikation über die Geschäftslogik erfolgen, bei der dann der Betreiber ein Review und eine Einordnung des zu publizierenden Inhaltes vornimmt. Dies ist darin begründet, dass die Qualität bewertet und sichergestellt werden muss. Die grundlegende Architektur wird in Bild 31 dargestellt.

4 Fazit

Schlussfolgernd lässt sich feststellen, dass der Betrieb einer Szenariendatenbank eine entscheidende Rolle zur Prüfung und Bewertung autonomer Fahrfunktionen spielt und einen wichtigen Beitrag zur Verkehrssicherheit leistet. Es lassen sich für eine erfolgreiche Umsetzung verschiedene Handlungsempfehlungen aus ökonomischer, technischer und rechtlicher Sicht ableiten. Die Anwendung des mit dem Lastenheft entwickelten Anforderungskatalogs in Entwicklung, Implementierung und im Betrieb der Szenariendatenbank schafft eine Grundlage zur Berücksichtigung der Empfehlungen.

Aus ökonomischer Sicht wurden die relevanten Stakeholder identifiziert und in die Cluster Privat, Öffentlich und Öffentlich-Privat (Semi-Öffentlich) eingeteilt. Für den Betrieb der Szenariendatenbank wurden aus internen als auch externen Workshops die Kategorien und Vorschläge für das Rollenmodell und die Finanzierung der Datenbank abgeleitet. Die wahrscheinlichste Rollenbesetzung im Kernbetrieb entspricht einer Veredlung der eingespeisten Daten durch private bzw. semi-öffentliche Institutionen (Öffentlich-Privat) (KI-Unternehmen, Technologie Start-ups). Der Datenbankbetrieb erfolgt nach Einschätzung der Teilnahmenden durch den privaten Sektor (Toolhersteller, IT-Infrastruktur-Unternehmen) bzw. wird beauftragt/zuschussfinanziert durch den öffentlichen Sektor. Der Auditor wird am wahrscheinlichsten durch private Prüforganisationen oder öffentliche Institutionen (z. B. Bundesbehörde) gestellt, wobei insbesondere die Überprüfung der DSGVO-Konformität und Informationssicherheit durch akkreditierte Auditoren erfolgen sollte. Der Nutzer, welcher im speziellen Fall gleichzeitig als Datenlieferant agiert, ist unabhängig vom Sektor jedoch abhängig von der jeweiligen Incentivierung und dem Nutzerzugang.

Um in der initialen Aufbauphase der Datenbank einen kostendeckenden Betrieb zu gewährleisten, ist eine Zuschussfinanzierung (CAPEX) notwendig. Die daraufhin folgende Finanzierung der laufenden Kosten (OPEX) erfolgt durch eine Kombination aus konstanten Mitgliedsbeiträgen sowie der Möglichkeit zum Erwerb von Lizenzen (Paketierung S, M, L). Weitere Einnahmemöglichkeiten wären zudem der Erwerb einzelner Datenpakete (Pay per Dataset), sowie die Kommerzialisierung von Inhalten im späteren Betrieb durch beispielsweise die Nutzung von Simulationen zur Verknüpfung von verschiedenen Szenarien sowie die Veredelung/Verknüpfung von Rohdaten. Des Weiteren ist zur Schaffung von Anreizen zur Datenlieferung ein Vergütungssystem vorgesehen, welches mittels Punktegutschriften zum Erwerb neuer Daten bzw. Szenarien genutzt werden kann. Eine weitere Möglichkeit ist die Integration eines modularen Systems, welches die Option anbietet, weitere Dienstleistungen zuzubuchen (bspw. integrierte Anonymisierung).

Die bei Erstellung des Rollenmodells identifizierten diversen Nutzenbedürfnisse fordern eine ausdifferenzierte Zugangsgestaltung, sodass beispielsweise nicht-kommerzielle Gruppen wie Forschungseinrichtungen einen günstigeren bzw. kostenlosen Zugang erhalten können. Durch den Austausch mit bereits existierenden Szenariendatenbanken konnte herausgearbeitet werden, dass diese die identifizierten Nutzerbedürfnisse zwar teilweise, aber nicht vollständig abdecken. Der daraufhin entwickelte Use-Case zielt darauf ab, durch unterschiedliche Incentivierungsmechanismen und Nutzerzugänge für die jeweiligen Stakeholdergruppen diese Bedürfnisse zu adressieren.

Aus technischer Sicht ist eine modulare Architektur im Sinne der Anbindung der nativen Datenbank, der DSGVO-konformen Datenbank für Rohdaten und auch externe Datenbanken zwingend. Dabei ist für die Anbindung der Datenbanken in der Geschäftslogik ein ontologischer Ansatz zu wählen. Die Szenarien sollen zwingend mindestens im ASAM OpenX-Format (d. h. OpenDrive, OpenCRG, OpenScenario) vorliegen, um die Nutzung für

der Szenarien auf unterschiedlichen Simulationsplattformen zu ermöglichen. Hochwertige Metadaten sind jedem Szenario zuzuweisen, um einen erheblichen Mehrwert für Nutzer über hochwertige Suchmechanismen zu liefern. Das Einspeisen von Szenarien sollte durch den Nutzer möglich sein, jedoch ist ein Qualitätsmanagement, welches durch den Betreiber erfolgen muss, nur durch die Geschäftslogik der Datenbank zu unterstützen, da eine vollständige Automatisierung hier als nicht ausreichend angesehen wird. Eine Bewertung der zu publizierenden Szenarien muss zumindest teilweise manuell vorgenommen werden, um die notwendige Qualität aller Teilaspekte (d. h. Qualität der Map-Daten, Trajektorien, hinreichende Verschlagwortung oder Beschreibung, etc.) zu gewährleisten. Im Hinblick auf die technische Validierung können unterschiedlichste Quellen (z. B. GIDAS, NuScenes Dataset, aufgenommene Rohdaten, etc.) als Basis für Szenarien verwendet werden. Hierdurch wird zudem die Berücksichtigung einer breiten Datenbasis im Entwicklungs- und Absicherungsprozess von OEMs oder Tier1s ermöglicht. Somit stellt dieser Aspekt einen wichtigen Teil der Datenbank dar.

Aus rechtlicher Sicht ist zur Umsetzung der Szenariendatenbank entscheidend von Anfang an IT-sicherheitsrelevante Aspekte in die Ausgestaltung zu integrieren. Die Datenbank sollte, soweit es dem relevanten Informationsgehalt nicht abträglich ist, nicht mit personenbezogenen Daten befüllt werden. Falls dennoch personenbezogene Daten in die Datenbank einfließen, muss sichergestellt werden, dass die Datenverarbeitungsprozesse DSGVO-konform ausgestaltet werden. Des Weiteren sind sämtliche Verarbeitungsprozesse umfassend zu dokumentieren.

Das Konzept, die Szenariendatenbank als Forschungsvorhaben aufzubauen und das Ergreifen geeigneter Garantien gemäß Art. 89 Abs. 1 und Abs. 2 DSGVO sollte transparent dargestellt werden, um datenschutzrechtliche Privilegierungen von Forschungsdaten zu erzielen. Wenn die Datenbank privat betrieben wird, ist in dem Zusammenhang darauf zu achten, dass die rein kommerzielle Nutzung und der Bereich der Forschung und Entwicklung voneinander getrennt sind, sodass sich das Aufziehen einer ausgelagerten Forschungsdatenbank empfiehlt. Bei privater Finanzierung oder privaten Eigeninteressen 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) Interessen das Forschungsinteresse nicht dominieren. Zusammenfassend ist es lohnenswert im kooperativen Austausch mit der verantwortlichen Datenschutzbehörde zu stehen.

In Bezug auf die Rechtsform der Szenariendatenbank kommt aus Haftungsgründen entweder die Ausgestaltung als GmbH oder als eingetragener Verein in Frage, 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 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.

Auf Grundlage der verschiedenen Austauschformate während der Projektlaufzeit, lässt sich abschließend folgern, dass einer kooperativen Szenariendatenbank eine große Bedeutung in der zukünftigen Entwicklung und perspektivisch auch in der Homologation autonomer Fahrfunktionen zukommt. Dies lässt sich auch durch die Rückmeldungen der Stakeholder in den Workshops und der Abschlussveranstaltung bestätigen. Das sektorübergreifende Interesse und der hohe Partizipationsgrad lassen auf eine generell gewünschte Beteiligung an einer zu entwickelnden Datenbank schließen.

Literatur

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

Road Safety Data, online verfügbar unter https://data.gov.uk/dataset/cb7ae6f0-4be6-4935-9277-47e5ce24a11f/road-safety-data (zuletzt abgerufen am 04.11.2022).

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

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.

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

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

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

Bundesministerium für Verkehr und digitale Infrastruktur, Eigentumsordnung für Mobilitätsdaten – Eine Studie aus technischer, rechtlicher und ökonomischer Perspektive, 2018.

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

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

Ellenberger in Palandt, Bürgerliches Gesetzbuch, 77. Auflage 2018.

ENVITED marketplace, online verfügbar unter https://envited.market/ (zuletzt abgerufen am 04.11.2022).

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

Gola, Peter/Heckmann, Dirk BDSG, 13. Aufl. 2019.

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

Harti, Andreas/Ludin, Anna „Recht der Datenzugänge", MMR 2021, 536.

Koenig, Abgabenordnung, 4. Auflage 2021.

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

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/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. Aufl. 2021.

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“, 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 „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.

SafetyPool, Online verfügbar unter https://www.safetypool.ai/ (zuletzt abgerufen am 04.11.2022).

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

Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra gen. Döhmann, 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 (zuletzt abgerufen am 04.11.2022).

Steege, Hans, „Ist die DSGVO zeitgemäß für das autonome Fahren? Datenschutzrechtliche Aspekte der Entwicklung, Erprobung und Nutzung automatisierter und autonomer Fahrzeuge“, MMR 2019, 509.

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

Bilder

Tabellen

Alle Tabellen entsprechen eigenen Darstellungen des Projektkonsortiums.

Schriftenreihe

Berichte der Bundesanstalt für Straßenwesen
Unterreihe „Fahrzeugtechnik“

2021

F 136: Kamera-Monitor-Systeme als Fahrerinformationsquelle
Leitner, Oehme, de Silva, Blum, Berberich, Böhm
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 137: Konzept für die Erzeugung eines ISO-konformen UML-Modells und Generierung eines GML-Applikationsschemas für DATEX II zur Verbesserung der Interoperabilität
Lauber, Steiger, Kopka, Lapolla, Freudenstein, Kaltwasser
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 138: Grundlagen zur Kommunikation zwischen automatisierten Kraftfahrzeugen und Verkehrsteilnehmern
Schaarschmidt, Yen, Bosch, Zwicket, Schade, Petzold € 16,50

F 139: Einfluss von Notbremssystemen auf die Entwicklung von Lkw-Auffahrunfällen auf Bundesautobahnen
Straßgütl, Sander € 14,50

F 140: Reibwertprognose als Assistenzsystem
Leschik, Sieron, Gregull, Müller, Trapp, Brandenburg, Haalman, Terpstra
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 141: Methoden für die Bewertung der Mensch-Maschine-Interaktion beim teilautomatisierten Fahren
Schömig, Wiedemann, Julier, Neukum, Wiggerich, Hoffmann € 18,00

F 142: Schräglagenangst
Scherer, Winner, Pleß, Will, Neukum, Stanglmayr, Bäumler, Siebke, Prokop € 14,50

2022

F 143: Unfallverletzungen in Fahrzeugen mit Airbags
Holtz, Heidt, Müller, Johannsen, Jänsch, Hammer, Büchner
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 144: Entwicklung eines Verfahrens zur Generierung eines Safety Performance Indikators aus der Bewertung von Euro NCAP
Bäumer, Hautzinger, Pfeiffer
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 145: Regeneration von Partikelfiltern bei Benzin- und Dieselkraftfahrzeugen
Langwald
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 146: Analysis of options for the creation of safety-related traffic information based on vehicle-generated data
Margalith, Sickenberger, Wohak
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 147: Automatische Notbremssysteme für Motorräder
Merkel, Pleß, Winner, Hammer, Schneider, Will
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 148: Analyse glättebedingter Unfälle von Güterkraftfahrzeugen mit mehr als 12 t zulässigem Gesamtgewicht
Müller, Thüring, Jänsch, Epple, Kretschmer, Gottwald, Oehring, Winkenbach
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 149: Evidenzorientierte Ableitung von sicherheitsrelevanten Grundszenarien für die Fahrdomäne Bundesautobahn
Weber, Eckstein, Tenbrock, König, Bock, Zlocki
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

2023

F 150: Fahrerassistenzsysteme für die Geschwindigkeitsreduzierung bei schlechten Bedingungen
Pohle, Günther, Schütze, Trautmann
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 151: Integration von öffentlichem und privatem Parkraummanagement
Höpping, Jonas, Becker, Krüger, Freudenstein, Krampe, Godschachner, Inninger, Scholz, Hüttner, Grötsch, Stjepanovic
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 152: On-Board-Diagnose (OBD) – Analyse der OBD in Bezug auf zukünftig verfügbare Emissionsdaten für die Periodische Technische Inspektion (PTI)
Hausberger, Matzer, Lipp, Blassnegger, Hametner, Prosenc
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

2024

F 153: Zusammenstellung geeigneter Sicherheitsindikatoren für die Bewertung der Mensch-Maschine-Interaktion von Level 3 Systemen
Yan, Pichen, Schmitz, Sklorz, Baumann
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 153b: Compilation of suitable safety indicators for the evaluation of Human-Machine Interaction of level 3 systems
Yan, Pichen, Schmitz, Sklorz, Baumann
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 154: Systematisierung geeigneter fahrfremder Tätigkeiten für automatisiertes Fahren von schweren Güterkraftfahrzeugen
Flämig, Beck, Hoffmann, Tjaden, Höger, Brandt, Haase, Wolter, Müller, Damer, Hettich, Schnücker
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 155: Handbuch Rollstuhlbeförderung bei Ausschreibungen
Boenke, Deuster
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 156: Entwicklung eines Konzepts und Lastenheftes für eine Szenariendatenbank zur Bewertung der Sicherheitswirkung hochautomatisierter Fahrfunktionen
Klinge, Krampitz, Ehrich, Siemon, Wiegand, Lassowski, Stavesand, Simon
Dieser Bericht liegt nur in digitaler Form vor und kann unter https://bast.opus.hbz-nrw.de/ heruntergeladen werden.

Fachverlag NW in der Carl Ed. Schünemann KG
Zweite Schlachtpforte 7 · 28195 Bremen · Tel.+(0)421/3 69 03-53 · Fax +(0)421/3 69 03-48

Alternativ können Sie alle lieferbaren Titel auch auf unserer Website finden und bestellen.

www.schuenemann-verlag.de

Alle Berichte, die nur in digitaler Form erscheinen, können wir auf Wunsch als »Book on Demand« für Sie herstellen.

ISSN 0943-9307
ISBN 978-3-95606-793-8
https://doi.org/10.60850/bericht-f156

www.bast.de