Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Bundesamt für Strassen
Office fédéral des routes
Ufficio federale delle Strade

Data Governance für Smart Mobility («DAGSAM»)

Gouvernance de données pour la mobilité intelligente («DAGSAM»)

Data governance for smart mobility («DAGSAM»)

Rapp AG
Bernhard Oehry
Jesper Engdahl
Oliver Buschor

Universität Basel
Alfred Früh
Nadja Braun Binder
Robert Schibli

AIT Austrian Institute of Technology
Willibald Krenn
Stephan Krenn
Christoph Schmittner

Forschungsprojekt MB4_20_01B_01 auf Antrag der Arbeitsgruppe Mobilität 4.0 (MB4)

Februar 2023 **1744**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Bundesamt für Strassen
Office fédéral des routes
Ufficio federale delle Strade

Data Governance für Smart Mobility («DAGSAM»)

Gouvernance de données pour la mobilité intelligente («DAGSAM»)

Data governance for smart mobility («DAGSAM»)

Rapp AG
Bernhard Oehry
Jesper Engdahl
Oliver Buschor

Universität Basel
Alfred Früh
Nadja Braun Binder
Robert Schibli

AIT Wien
Willibald Krenn
Stephan Krenn
Christoph Schmittner

Forschungsprojekt MB4_20_01B_01 auf Antrag der Arbeitsgruppe Mobilität 4.0 (MB4)

Februar 2023 **1744**

Impressum

Forschungsstelle und Projektteam

Projektleitung
Bernhard Oehry (Rapp AG)
Projektleitung Stv.
Alfred Früh (Universität Basel)

Mitglieder
Jesper Engdahl (Rapp AG)
Oliver Buschor (Rapp AG)
Nadja Braun Binder (Universität Basel)
Robert Schibli (Universität Basel)
Stephan Krenn (AIT)
Christoph Schmittner (AIT)
Willibald Krenn (AIT)

Begleitkommission

Präsident
Andreas Kronawitter (Kronawitter Innovation)

Mitglieder
Hauke Fehlberg (ASTRA)
Jens Henkner (CertX)
Peter Herzog (SBB SKI)
Thomas Küchler / Marius Schmidt (SOB)
Bertrand Loisin (BFS)
Melinda Lohmann (Universität St.Gallen)
Martina Müggler / Andreas Biedermann (PostAuto)
Gregor Ochsenbein (BAV)
Valentino Scarcia (ASTRA)
Olivier Verscheure (EPFL)

Antragsteller

Arbeitsgruppe Mobilität 4.0 (MB4)

Bezugsquelle

Das Dokument kann kostenlos von http://www.mobilityplatform.ch heruntergeladen werden.

Inhaltsverzeichnis

Zusammenfassung

Problembeschreibung
Elektrifizierung, Automatisierung und Digitalisierung sind jene technologischen Entwicklungsfelder, welche das Angebot an Verkehrsmitteln derzeit stark verändern. Diese Technologien ermöglichen neben elektrisch betriebenen, automatisierten und vernetzten Fahrzeugen und Infrastrukturen insbesondere auch neue Angebote an Mobilitätsdiensten. Anbieter von Mobilitätsdiensten versuchen die gesellschaftlichen Bedürfnisse nach Mobilität durch leicht zugängliche und individualisierte Angebote und mit **neuen Geschäftsmodellen** zu befriedigen.

Während im herkömmlichen Mobilitätsgeschäft die Fahrzeuge und die Infrastruktur die wichtigsten Aktivposten der Betreiber waren, sind es im künftigen Mobilitätsgeschäft digitale Plattformen, Dienstleistungsbündel, vernetzte Angebote und eine zunehmend globale Reichweite. Die Dienstleistungen für die Nutzerinnen und Nutzer sind dabei, sich völlig zu verändern: Heute besteht das Angebot aus "Verkehr und Transport", oft mit einem einzigen Verkehrsmittel. In Zukunft wird das Grundangebot "Mobilität" sein. Um diese neuartigen Mobilitätsdienste zu ermöglichen, sind grosse Datenmengen sowie "intelligente" Prozesse zur Analyse und Verarbeitung der sehr diversen **Daten** notwendig.

Mit dem Projekt DAGSAM sollen für solche anspruchsvolle datengestützte Systeme in der digitalisierten Mobilitätswelt rechtliche, technische und organisatorische Systemansätze gefunden werden, die es ermöglichen, die Hoheit über die Daten und deren Nutzung mittels einer **"Data Governance"** zu regeln und dabei die Interessen aller beteiligten Akteure zu wahren. Das Hauptziel des Projekts besteht dabei darin, ein Governance-Modell zu finden, das auf definierten Beziehungen zwischen den Akteuren beruht und durch technische Mittel unterstützt wird.

Systematisierung der Mobilitätsangebote
Smart Mobility-Anwendungen entwickeln sich aufgrund der Digitalisierung, der Automatisierung, der Vernetzung und des technologischen Fortschritts schnell. DAGSAM stellt einen Werkzeugkasten bereit, um Governance-Fragen zu adressieren. Um angesichts der Vielfalt und Marktdynamik bei **Smart Mobility**-Anwendungen allgemeingültige Aussagen zu Governance-Fragen treffen zu können, wurden in einem ersten Schritt die involvierten Akteure und die bestehenden Datenflüsse identifiziert.

Es zeigte sich für sämtliche Smart Mobility-Anwendungen, dass die Rollen der Akteure mit einem generisches Rollenmodell abgebildet werden können. Der **Leistungserbringer** stellt dabei die zugrundeliegende Dienstleistung wie z.B. den Transport von Personen zur Verfügung. Der **Vermittler** hat die primäre vertragliche Beziehung zum Nutzer, führt Angebot und Nachfrage zusammen, bündelt Angebote und bietet Mobilitätsprodukte an. Der **Nutzer** konsumiert mobilitätsbezogene Dienstleistungen und der **Regulator** ist jene Instanz, welche die allgemeinen Rahmenbedingungen festlegt.

Anhand einer Prozessanalyse wurden sodann die Datenflüsse zwischen den Akteuren bestimmt und generischen Datentypen zugeordnet. Es zeigte sich, dass das Rollenmodell sowie die Einteilung der Datenflüsse in generischen Datentypen für alle betrachteten Smart Mobility-Anwendungen anwendbar sind.

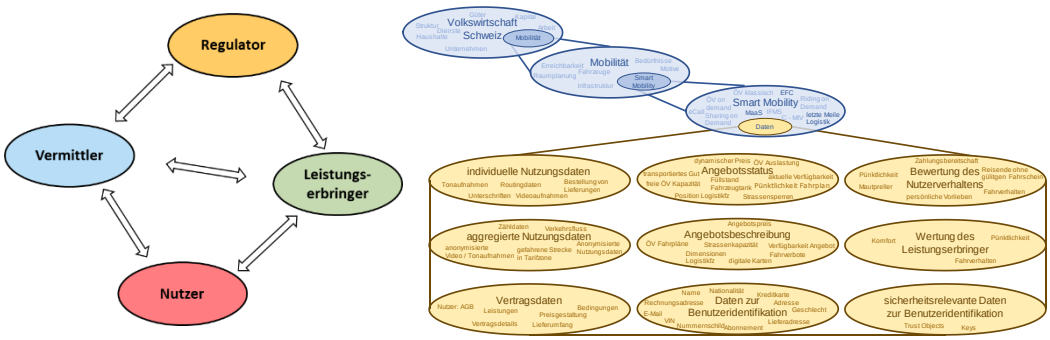


Abb. 1 verwendetes Rollenmodell und generische Datentypen

Juristische Instrumente

Zur Klärung der rechtlichen Aspekte der Data Governance, wurden die entsprechenden juristischen Instrumente zusammengefasst. Obwohl in der Schweizer Rechtsordnung kein Eigentumsrecht an Daten bekannt ist, existieren einige Instrumente, welche **eine Zuordnung von Daten** bewirken können. Dabei lassen sich Zuordnungsnormen, Schutznormen, die vertragliche Zuordnung von Daten und die Zuordnung aufgrund des Datenschutzrechts unterscheiden.

Als **Zuordnungsnormen** werden jene Instrumente bezeichnet, welche einer natürlichen oder juristischen Person Ausschliesslichkeitsrechte (absolute Rechte) an Daten gewähren. Als mögliche absolute Rechte an Daten kommen in der Schweiz die Immaterialgüterrechte (Urheberrecht, Patentrecht, Designrecht, Markenrecht) und die im Urheberrecht geregelten so genannten Leistungsschutzrechte in Frage. Unter **Schutznormen** laufen jene Instrumente, die einer natürlichen oder juristischen Person einen rechtlichen Schutz an Daten einräumen, die von der jeweiligen Person faktisch kontrolliert werden. In den Genuss des Schutzes kommt also, wer die tatsächliche Herrschaft über die Daten ausübt. Eine solche Bestimmung findet sich beispielsweise im wettbewerbsrechtlichen Schutz von Fabrikations- und Geschäftsgeheimnissen (Art. 6 UWG). Daten können auch mittels **vertraglicher Vereinbarungen** einem Rechtsträger zugeordnet werden. Zwar wirken solche Verträge nur zwischen den Vertragsparteien. Die Vertragsfreiheit gewährt den Parteien jedoch die Möglichkeit, eine Rechtslage zu schaffen, die einem Ausschliesslichkeitsrecht recht nahekommt. Schliesslich sorgt das **Datenschutzrecht** für eine gewisse Zuordnung von Daten, welche einen Bezug zu einer oder mehreren Personen aufweisen. Den Umgang mit Personendaten regelt das Schweizer Datenschutzgesetz, das am 1. September 2023 in revidierter Fassung in Kraft tritt (nDSG).

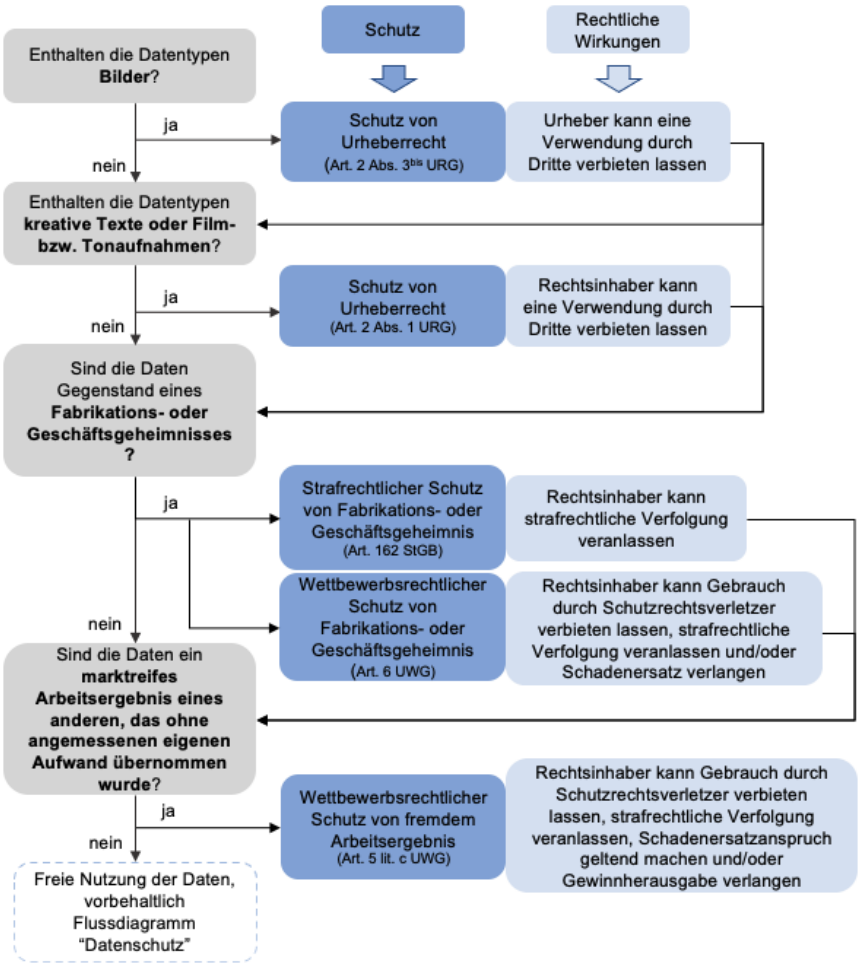


***Abb. 2** Prüfschema zur Datenzuordnung*

Technologische Instrumente
Damit die Data Governance technologisch umgesetzt werden kann, werden ausgewählte Technologien präsentiert. Diese erlauben es, Berechnungen auf Daten durchzuführen und gleichzeitig die Interessen der beteiligten Akteure zu wahren, sei es aus Sicht des Schutzes personenbezogener Daten oder von Geschäftsgeheimnissen. Je nach Anwendungsfall und entsprechender Komplexität der Berechnungen sind die ausgewählten Technologien unterschiedlich geeignet.

Secure Multi-Party Computation (MPC) beschreibt eine Klasse von kryptographischen Protokollen, die es mehreren Parteien erlauben, gemeinsame Berechnungen auf vertraulichen Eingabedaten durchzuführen. Dabei wird sichergestellt, dass jede Partei nur das definierte Ergebnis der Berechnung kennt, nicht jedoch weitere Informationen über die Eingabedaten der anderen Teilnehmer.

Ein **Trusted Execution Environment** (TEE) schafft eine geschützte Umgebung, in der sensitive Daten und Codes vor Zugriff durch aussenstehende Prozesse, inklusive des Betriebssystems abgeschirmt sind. Es handelt sich um eine Hardwareerweiterung, welche das vertrauenswürdige Ausführen von Berechnungen innerhalb einer ansonsten potentiell nicht vertrauenswürdigen Umgebung erlaubt. In einer TEE werden die Vertraulichkeit, die Authentizität des ausgeführten Programmcodes sowie die Integrität der ausgeführten Berechnungen mittels Zertifizierungen garantiert.

Vollhomomorphe Verschlüsselung (Fully Homomorphic Encryption, FHE) erlaubt es, beliebige Berechnungen in verschlüsselten Domänen durchzuführen. Die Daten müssen also für die Berechnungen nicht entschlüsselt werden. Dies ermöglicht insbesondere die Auslagerung von Berechnungen in nicht-vertrauenswürdige Cloudumgebungen, da die Vertraulichkeit der Daten nicht unterminiert wird.

Governance-Modell
Das generische Governance-Modell berücksichtigt die Gesamtheit aller Normen und Bedingungen, die für das Funktionieren einer Smart Mobility-Anwendung massgebend sind. Dabei können die Normen sowohl technischer als auch organisatorischer Natur sein, und sie können durch normative Verweisung Teil der Gesetzgebung werden. Zu den Bedingungen gehören die Wirtschaftlichkeit eines Mobilitätsangebots sowie als elementarer Aspekt das zwischen den Akteuren notwendige Vertrauen.

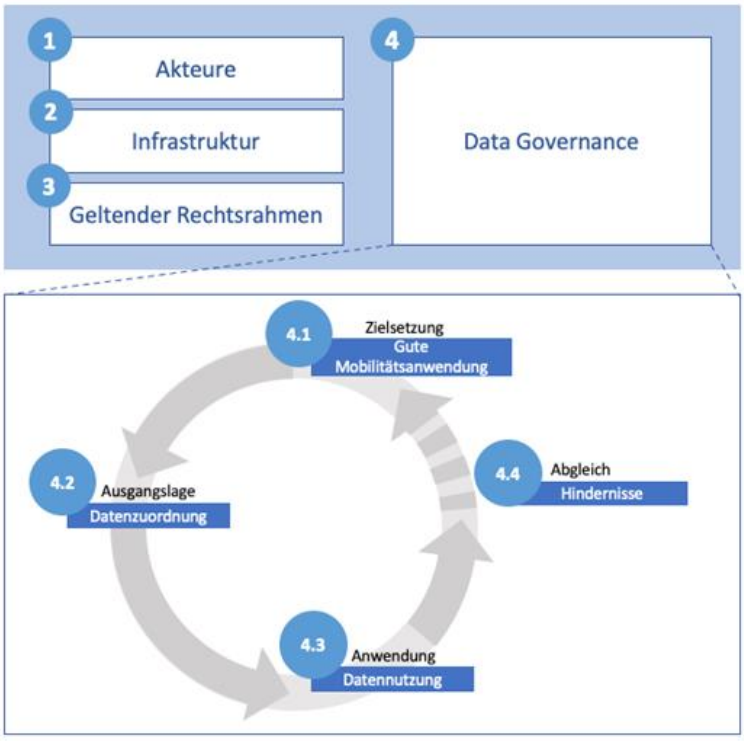


***Abb. 3** generisches Governance Modell in vier Schritten*

In einem ersten Schritt werden zunächst die **Akteure** identifiziert. Dies erlaubt die Zuständigkeiten und Verantwortlichkeiten zu regeln. Anschliessend wird die für den Datenaustausch notwendige **Infrastruktur** thematisiert, um die Verwaltung von Datenzugriff und Datenverarbeitung zwischen den Akteuren sicherzustellen. In einem dritten Schritt wird der **geltende Rechtsrahmen** untersucht. In einem letzten Schritt geht es um den eigentlichen Kern – die **Data Governance** – und damit um den konkreten Umgang mit Mobilitätsdaten. Mittels eines detaillierten Analyserasters kann ermittelt werden, welche technischen, rechtlichen oder organisatorischen Prinzipien bzw. Regeln in Bezug auf die konkrete Mobilitätsanwendung erforderlich sind. In diesem Analyseraster sind wiederum verschiedene Schritte vorgesehen. Zunächst wird die gute Mobilitätsanwendung als Zielsetzung definiert. Es folgt eine Analyse der Datenzuordnung in der Ausgangslage. In einem dritten Schritt wird die Datennutzung für die Anwendung spezifiziert. Im letzten Schritt werden schliesslich die bestehenden Hindernisse identifiziert und mit rechtlichen, technischen oder organisatorischen Massnahmen adressiert.

Dieses Governance-Modell wurde anhand der zwei konkreten Smart Mobility-Anwendungen Mobility-as-a-Service (MaaS) und Strassengebührenerhebung (Road User Charge, RUC) entwickelt und getestet.

Governance-Modell MaaS
Bei MaaS bieten verschiedene Leistungserbringer ihre Mobilitätsangebote auf der Plattform des Vermittlers an. Dieser bündelt die Angebote und stellt sie den Nutzern zur Verfügung. Es zeigt sich, dass sich bei der Umsetzung solcher MaaS-Angebote in Bezug auf die Data Governance hauptsächlich **juristische Hindernisse** stellen und es darum geht, Bedingungen festzulegen, unter denen die Akteure bereit sind, ihre Daten zu teilen. Technische Aspekte bleiben dagegen eher im Hintergrund.

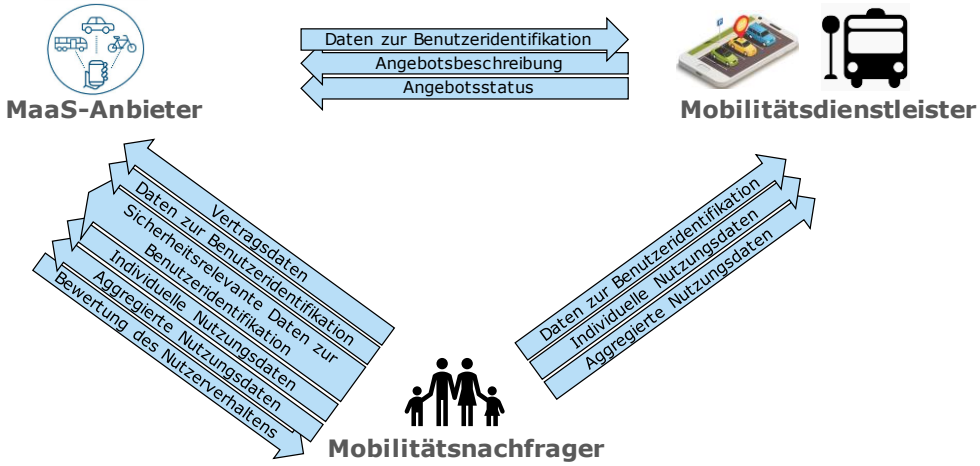


Abb. 4 *Datenflüsse bei der Smart Mobilty-Anwendung MaaS*

Konkret sind Mobilitätsdienstleister in der Regel bereit, Daten zum Angebot zur Verfügung zu stellen, dürften hingegen bezüglich der allgemeinen Zugänglichmachung von Daten über den Vertrieb (insb. individuelle und aggregierte Nutzungsdaten, Daten über den Angebotsstatus und Vertragsdaten) Vorbehalte haben, da diese einen grossen wirtschaftlichen Wert für die Mobilitätsdienstleister darstellen. Es braucht deshalb klare Grundsätze und **Regeln** betreffend **Datenbezug** und **Datenverwendung**, die von einer neutralen Instanz unter Einbezug der relevanten Stakeholder zu entwickeln sind. Aus datenschutzrechtlicher Sicht könnte die Einführung gemeinsamer Verhaltensregeln und Datenschutzzertifizierungen im Zusammenhang mit zentralen Mobilitätsdateninfrastrukturen **Vertrauen** seitens der potentiellen Datenlieferanten schaffen und damit den Datenaustausch fördern. Das Vertrauen der Mobilitätsdienstleister und der MaaS-Anbieter hängt massgeblich davon ab, ob klare Regeln und Pflichten, insbesondere betreffend Zugang zur Infrastruktur und betreffend Routing bestehen, und in welchem Verfahren diese festgelegt werden.

Governance-Modell RUC
Bei der als fiktive Beispielsanwendung für RUC betrachteten Umsetzung einer flächendekkenden fahrleistungsabhängigen Abgabe für sämtliche Motorfahrzeuge privater Nutzer in

der Schweiz als Ersatz der Treibstoffabgaben steht der **Schutz der persönlichen Daten**, insbesondere der individuellen Fahrprofile, besonders im Fokus.

Damit die Erfassung aller Infrastrukturbenutzer garantiert werden kann, braucht es nutzungsspezifische Angebote für die Erhebung der notwendigen Fahrdaten. Diese können etwa von vernetzten Fahrzeugen, dedizierten Geräten oder Mobiltelefonen stammen. Da es sich um eine verpflichtende Abgabe handelt, die basierend auf der massenhaften Erhebung von Mobilitätsdaten berechnet wird, ist insbesondere der Grundsatz des **Datenschutzes durch Technik** ("privacy by design") ernst zu nehmen, um die Privatsphäre der Einzelnen zu wahren.

Um hohe technische Standards bezüglich Data Governance zum Schutz der Bewegungsprofile einzelner Infrastrukturbenutzer zu erreichen, muss gewährleistet werden, dass sensitive Daten nur für die Gebührenberechnung verwendet werden und nicht im Klartext von anderen Entitäten abseits des Infrastrukturbenutzers gelesen, verarbeitet, oder manipuliert werden können. Dies kann durch die Verwendung von TEEs garantiert werden, innerhalb derer Nutzerdaten ausschliesslich von zertifizierten Algorithmen verarbeitet werden. Jegliche anderen Zugriffe werden verhindert, da die Daten sowie Zwischenresultate der Berechnung im Speicher ausschliesslich in verschlüsselter Form vorliegen, und lediglich während der Verarbeitung innerhalb der TEE entschlüsselt werden.

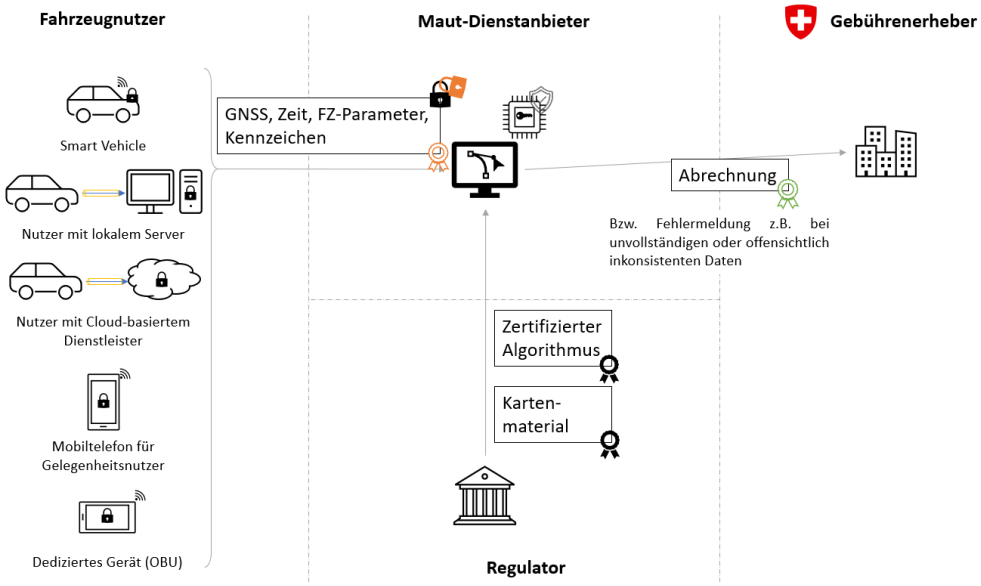


Abb. 5 *Datenschutzfreundlicher Ansatz für eine Strassengebührenerhebung (RUC)*

Evaluation des Governance Modells

Die Ausarbeitung generischer Elemente hat eine systematische Analyse ermöglicht und sich für die Entwicklung von Data Governance-Modellen bewährt. Die Strukturierung der Datenflüsse anhand der generischen Datentypen bietet eine Grundlage für die Erstellung von Governance-Modellen. Zudem erwies sich das verwendete Rollenmodell als ein nützliches Instrument, um die Verantwortlichkeiten der Akteure klar abzugrenzen. Die angewendete **Systematisierung** eignet sich, um die organisatorischen Aspekte hinsichtlich der Verantwortlichkeiten der unterschiedlichen Akteure einzuordnen. Dies bietet zudem eine erforderliche Grundlage, um die juristischen sowie technischen Aspekte zu entwickeln.

Die **juristischen Instrumente** aus dem Immaterialgüterrecht, dem Schutz von Geschäftsgeheimnissen und dem Datenschutzrecht haben unterschiedliche Anwendungsvoraussetzungen, Zielsetzungen und Rechtsfolgen. Insgesamt kann sich so in Bezug auf Smart Mobility ein komplexes Geflecht von **Zuordnungen** ergeben. Es wurden **Prüfschemata** entwickelt, mit denen sich prüfen lässt, welche Akteure in einem konkreten Mobilitätsangebot an welchen Daten berechtigt sind. Diese Zuordnung ist wesentlich für die Data Governance: Die initiale Zuordnung von Daten kann die Nutzung bestimmter Mobilitätsangebote begünstigen, erschweren oder verunmöglichen (und muss sodann im Rahmen der Data Governance korrigiert werden). Im Gegensatz zu den Zuordnungsinstrumenten ist die Zahl der rechtlichen Instrumente, welche Akteuren einen **Zugang** zu den Daten anderer Akteure

verschaffen, kleiner. Dennoch konnten auch hier rechtliche Bestimmungen identifiziert werden, welche sich auf die Data Governance auswirken können. Es handelt sich um Auskunfts- und Einsichtsrechte, die sich aus dem Öffentlichkeitsgesetz ergeben und um spezifische Offenlegungspflichten in öffentlich-rechtlichen Spezialgesetzen, die typischerweise konzessionierte Leistungserbringer betreffen.

Die Wahl der **technologischen Instrumente** hängt stark vom betrachteten Mobilitätsangebot ab. Eine klare Spezifikation des Anwendungsfalls erlaubt die konkrete Auswahl technologischer und kryptographischer Methoden für **Datenschutz**, **Authentizität**, oder **Auditierbarkeit**. Es können keine generischen technischen Empfehlungen für sämtliche Smart Mobility-Anwendungen abgegeben werden. Diese müssen vielmehr anwendungsspezifisch erarbeitet werden, um technologisch bestmöglichen Datenschutz und Datensicherheit bei gleichzeitig hohem Anspruch an Effizienz und Skalierbarkeit umsetzen zu können. Hingegen erlaubt die Gruppierung von Smart Mobility Anwendungen, dass eine entwickelte Lösung grundsätzlich für eine ganze Klasse von Anwendungen eingesetzt werden kann. Bei jeder technischen Umsetzung sind zudem mindestens zwei zentrale Fragen zu stellen: Einerseits, ob das entwickelte System die gestellten **funktionalen Anforderungen** und **Datenschutzanforderungen** erfüllt. Dies kann sichergestellt werden, indem von der wissenschaftlichen Community geprüfte kryptographische Bausteine verwendet, indem Best Practices bei der Auswahl und Kombination von Komponenten befolgt und indem Datenschutz-Folgeabschätzungen ausgeführt werden. Andererseits stellt sich nach Fertigstellung eines Designs die Frage nach dessen korrekter **Umsetzung und Implementierung**. Neben der Auswahl hochqualitativer Bausteine für sicherheitssensitive Komponenten stellt insbesondere die erforderliche Art der Zertifizierung und Transparenz der Implementierung einen zentralen Aspekt dar, um über "gefühltes Vertrauen" Akzeptanz bei allen involvierten Akteuren einer Smart Mobility-Anwendung zu erreichen.

Das **generische Data Governance-Modell** mit dem Vorgehen in vier Schritten wurde für den Anwendungsfall MaaS und die Strassengebührenerhebung (RUC) entwickelt, angewendet und getestet. Es zeigt sich, dass sich die Massnahmen zur Beseitigung der Hindernisse je nach Anwendungsfall unterscheiden. Je nach der verwendeten Infrastruktur, den sich ergebenden Datenflüssen und der rechtlichen Kontrolle über die Daten kann der Schwerpunkt der Massnahmen eher auf dem rechtlichen oder auf dem technischen Aspekt liegen. Das generische Data Governance-Modell hat sich insofern bewährt, da es – soweit ersichtlich – auf alle betrachteten Mobilitätsanwendungen anwendbar ist, um anwendungsspezifische Data Governance-Massnahmen zu entwickeln.

Im Zusammenhang mit **MaaS** zeigt ein Blick auf den **geltenden Rechtsrahmen**, dass der Gesetzgeber beim Erlass relevanter Bestimmungen implizit von monomodalem Reisen ausgegangen ist. Entsprechend bestehen Bestimmungen, die sich nicht oder nur schwer auf multimodales Reisen anwenden lassen. So gelten beim Ausfall oder einer Verspätung in einem Teil der Reisekette keine einheitlichen Regeln betreffend Anspruch auf Weiterreise, Erstattung oder Entschädigung. Eine Anpassung des Rechtsrahmens könnte zur Steigerung der Attraktivität von MaaS-Angeboten beitragen. Zudem ist die Wahl der technischen Infrastruktur bei MaaS entscheidend. Eine **zentrale Infrastruktur** mit einem so genannten Intermediary MaaS Integrator (IMI) wirkt einem fragmentierten Markt entgegen. Aus dieser Designentscheidung ergibt sich indes die Governance-Vorgabe, dass alle Akteure zu nicht-diskriminierenden Bedingungen an dieser Infrastruktur teilnehmen können müssen. In technischer Hinsicht steht im Vordergrund, wie Daten **interoperabel standardisiert** werden können und wie grosse Datenmengen mit schnellen Reaktionszeiten komplex berechnet werden können. In rechtlicher Hinsicht steht im Vordergrund, welche allgemeingültigen **Bedingungen** für die Nutzung der Infrastruktur aufgestellt werden können.

Im Zusammenhang mit der Strassengebührenerhebung **(RUC)** ist die Herausforderung für die Data-Governance die verpflichtende Datenlieferung durch die Nutzer. Dies erfordert ein **vertrauenswürdiges Systemdesign** mit ebenso vertrauenswürdigen **Prozessen** und **Akteuren**. Es geht hierbei nicht nur darum, sich vor einer möglichen Überwachung durch den Staat zu schützen, sondern auch darum, dass das System Sicherheiten bieten muss, damit Daten nicht an Dritte gelangen können. Unabdingbar in einem Marktmodell ist, dass alle Nutzer unabhängig von ihrer technischen Ausrüstung und dem gewählten Dienstanbieter für gleiche Strecken die gleichen Abgaben bezahlen. Dies wird durch die vorgestellte Lösung, mit der Zurverfügungstellung einer **TEE** mit einem zertifizierten Algorithmus zur Berechnung der Abgabe und zu deren Kontrolle gewährleistet. Nur innerhalb dieser

sicheren Rechenumgebung können Daten entschlüsselt und verarbeitet werden, ohne dass irgendeine Partei darauf Zugriff hat. Die **Zertifizierung** erfolgt durch eine dritte Stelle und stellt einen zentralen Vertrauensanker dar. Mit diesen Ansätzen wird sichergestellt, dass die organisatorische und juristische Governance durch den Einsatz technologischer Instrumente gewährleistet ist.

Schlussfolgerung und Empfehlungen
Im Rahmen dieser Arbeit zeigte sich, dass mit dem vorgeschlagenen Governance-Modell das **Zusammenspiel** organisatorischer, rechtlicher und technischer Aspekte einheitlich analysiert werden kann. So lässt sich bei der Entwicklung von Dienstleistungen in der "Neuen Mobilität" jeweils eine passende Data Governance entwickeln und implementieren. Je nach Mobilitätsanwendung können dabei eher rechtliche (wie bei MaaS) oder eher technische Aspekte (wie bei RUC) im Vordergrund stehen. Eine zentrale Erkenntnis des Forschungsprojekts lautet, dass Governance-Strukturen – ganz unabhängig von der konkreten Mobilitätsanwendung – zuvorderst **Vertrauen** zwischen den Akteuren schaffen müssen und dass der Aufbau des Vertrauens im Idealfall die frühzeitige Integration sämtlicher Interessengruppen erfordert.

Die in diesem Forschungsprojekt entwickelten Modelle können einen Beitrag leisten, um die Data Governance für die Schweizer Mobilität zu fördern. Konkret ergeben sich aus Sicht der am Forschungsprojekt beteiligten Disziplinen drei Empfehlungen:

1. **Anwendung** und ggf. Weiterentwicklung des allgemeinen Governance-Modells
2. **Anpassung** des Rechtsrahmens für MaaS
3. **Machbarkeitsstudie** zu sicheren Rechenumgebungen für RUC

Résumé

Description du problème
L'électrification, l'automatisation et la numérisation sont les domaines de développement technologique qui modifient actuellement fortement l'offre de moyens de transport. Outre les véhicules et les infrastructures électriques, automatisés et connectés, ces technologies permettent également de proposer de nouvelles offres de services de mobilité. Les fournisseurs de services de mobilité tentent de répondre aux besoins de mobilité de la société en proposant des offres facilement accessibles et individualisées ainsi que de **nouveaux modèles commerciaux**.

Alors que dans l'activité de mobilité traditionnelle, les véhicules et l'infrastructure étaient les principaux actifs des opérateurs, dans l'activité de mobilité future, ce sont les plateformes numériques, les bouquets de services, les offres en réseau et une portée de plus en plus mondiale. Les services proposés aux usagers sont en train de se transformer complètement : Aujourd'hui, l'offre consiste en "circulation et transport", souvent avec un seul moyen de transport. À l'avenir, l'offre de base sera la "mobilité". Pour permettre la mise en place de ces services de mobilité d'un nouveau genre, il est nécessaire de disposer de grandes quantités de données ainsi que de processus "intelligents" pour analyser et traiter ces **données** très diverses.

Le projet DAGSAM vise à trouver, pour de tels systèmes exigeants basés sur des données dans le monde de la mobilité numérisée, des approches de systèmes juridiques, techniques et organisationnelles qui permettent de régler la souveraineté sur les données et leur utilisation au moyen d'une "**gouvernance des données**", tout en préservant les intérêts de tous les acteurs impliqués. L'objectif principal du projet est de trouver un modèle de gouvernance basé sur des relations définies entre les acteurs et soutenu par des moyens techniques.

Systématisation des offres de mobilité
Les applications de mobilité intelligente se développent rapidement en raison de la numérisation, de l'automatisation, de la mise en réseau et des progrès technologiques. DAGSAM fournit une boîte à outils pour aborder les questions de gouvernance. Afin de pouvoir tirer des conclusions générales sur les questions de gouvernance, compte tenu de la diversité et de la dynamique du marché des applications de **mobilité intelligente**, les acteurs impliqués et les flux de données existants ont été identifiés dans un premier temps.

Pour toutes les applications Smart Mobility, il s'est avéré que les rôles des acteurs pouvaient être représentés par un modèle de rôle générique. Le **fournisseur de services** met à disposition le service sous-jacent, comme le transport de personnes. L'**intermédiaire** a la relation contractuelle primaire avec l'utilisateur, réunit l'offre et la demande, regroupe les offres et propose des produits de mobilité. L'**utilisateu**r consomme des services liés à la mobilité et le **régulateur** est l'instance qui fixe les conditions générales.

Les flux de données entre les acteurs ont ensuite été déterminés à l'aide d'une analyse de processus et attribués à des types de données génériques. Il s'est avéré que le modèle de rôle ainsi que la répartition des flux de données en types de données génériques étaient applicables à toutes les applications de mobilité intelligente considérées.

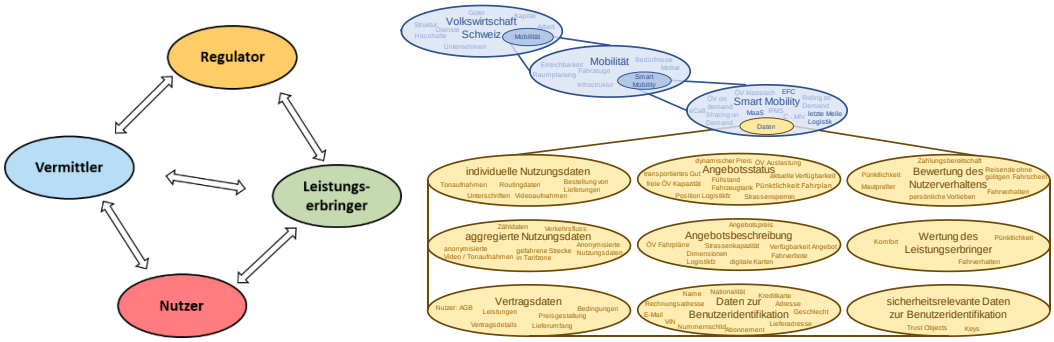


***Fig. 1** Modèle de rôle utilisé et types de données génériques*

Instruments juridiques

Afin de clarifier les aspects juridiques de la gouvernance des données, les instruments juridiques correspondants ont été résumés. Bien que l'ordre juridique suisse ne connaisse pas de droit de propriété sur les données, il existe quelques instruments qui peuvent entraîner une **attribution des données**. On distingue les normes d'attribution, les normes de protection, l'attribution contractuelle des données et l'attribution sur la base du droit de la protection des données.

On appelle **normes d'attribution** les instruments qui confèrent à une personne physique ou morale des droits exclusifs (droits absolus) sur les données. En Suisse, les droits de propriété intellectuelle (droit d'auteur, droit des brevets, droit des designs, droit des marques) et les droits voisins régis par le droit d'auteur peuvent être considérés comme des droits absolus sur les données. Les **normes de protection** sont des instruments qui confèrent à une personne physique ou morale une protection juridique sur des données qu'elle contrôle de facto. La protection est donc accordée à la personne qui exerce un contrôle effectif sur les données. Une telle disposition se trouve par exemple dans la protection des secrets de fabrication et d'affaires en vertu du droit de la concurrence (art. 6 LCD). Les données peuvent également être attribuées à une entité juridique par le biais **d'accords contractuels**. Certes, de tels contrats n'ont d'effet qu'entre les parties contractantes. La liberté contractuelle permet toutefois aux parties de créer une situation juridique qui se rapproche d'un droit d'exclusivité. Enfin, le droit de la protection des données assure une certaine attribution des données qui présentent un lien avec une ou plusieurs personnes. Le traitement des données personnelles est régi par la loi suisse sur la protection des données, dont la version révisée entrera en vigueur le 1er septembre 2023 (nLPD).

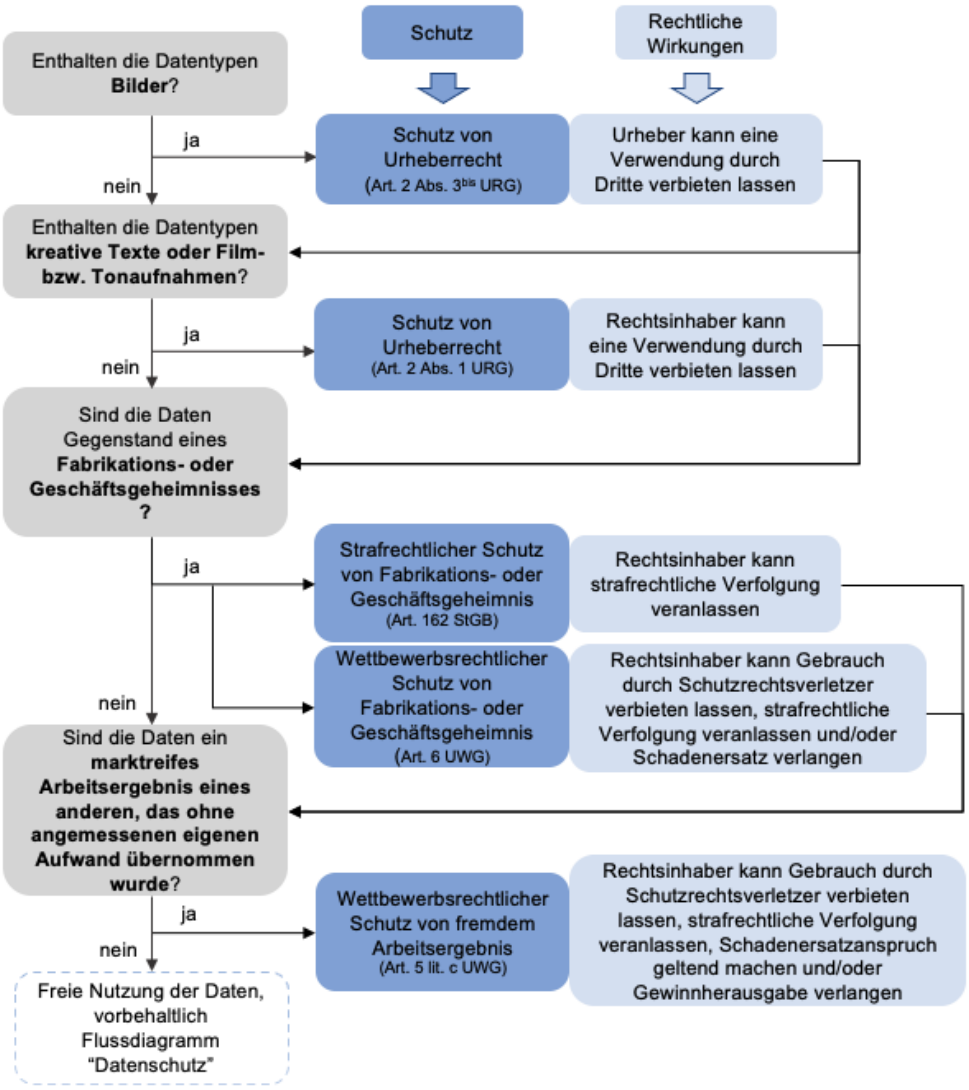


***Fig. 2** Schéma de contrôle pour l'attribution des données*

Instruments technologiques
Afin que la gouvernance des données puisse être mise en œuvre sur le plan technologique, une sélection de technologies est présentée. Celles-ci permettent d'effectuer des calculs sur les données tout en préservant les intérêts des acteurs impliqués, que ce soit du point de vue de la protection des données personnelles ou des secrets commerciaux. Selon le cas d'application et la complexité correspondante des calculs, les technologies sélectionnées sont plus ou moins appropriées.

Secure Multi-Party Computation (MPC) décrit une classe de protocoles cryptographiques qui permettent à plusieurs parties d'effectuer des calculs communs sur des données d'entrée confidentielles. Il s'agit de s'assurer que chaque partie ne connaît que le résultat défini du calcul, mais pas d'autres informations sur les données d'entrée des autres participants.

Un **Trusted Execution Environment** (TEE) crée un environnement protégé dans lequel les données et les codes sensibles sont protégés contre l'accès par des processus externes, y compris le système d'exploitation. Il s'agit d'une extension matérielle qui permet d'exécuter des calculs en toute confiance au sein d'un environnement qui, autrement, ne serait pas potentiellement fiable. Dans une TEE, la confidentialité, l'authenticité du code de programme exécuté et l'intégrité des calculs effectués sont garanties par des certifications.

Le chiffrement entièrement homomorphe (Fully Homomorphic Encryption, FHE) permet d'effectuer n'importe quel calcul dans des domaines chiffrés. Les données ne doivent donc pas être décryptées pour les calculs. Cela permet notamment d'externaliser les calculs dans des environnements de cloud non fiables, car la confidentialité des données n'est pas compromise.

Modèle de gouvernance
Le modèle de gouvernance générique prend en compte l'ensemble des normes et conditions qui sont déterminantes pour le fonctionnement d'une application Smart Mobility. Les normes peuvent être de nature technique ou organisationnelle et peuvent faire partie de la législation par le biais de renvois normatifs. Parmi les conditions figurent la rentabilité d'une offre de mobilité et, aspect élémentaire, la confiance nécessaire entre les acteurs.

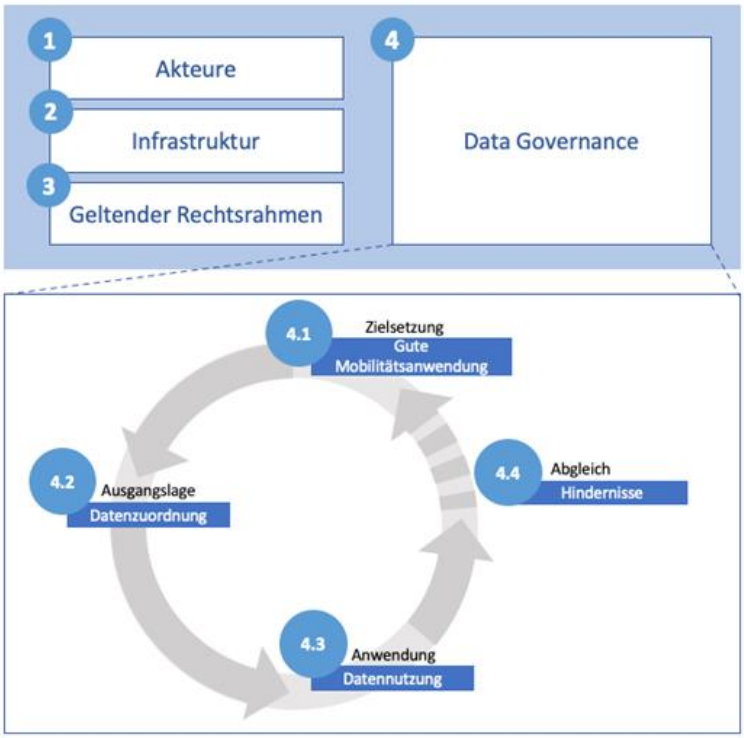


***Fig. 3** generisches Governance Modell in vier Schritten*

Dans un premier temps, les **acteurs** sont identifiés. Cela permet de définir les compétences et les responsabilités. Ensuite, l'**infrastructure** nécessaire à l'échange de données est abordée afin d'assurer la gestion de l'accès et du traitement des données entre les acteurs. Dans un troisième temps, le **cadre juridique en vigueur** est examiné. Enfin, la dernière étape porte sur le cœur même du sujet - la **gouvernance des données** - et donc sur le traitement concret des données de mobilité. Une grille d'analyse détaillée permet de déterminer quels principes ou règles techniques, juridiques ou organisationnels sont nécessaires en ce qui concerne l'application concrète de la mobilité. Cette grille d'analyse prévoit à son tour différentes étapes. Tout d'abord, la bonne application de la mobilité est définie comme objectif. Il s'ensuit une analyse de l'affectation des données dans la situation initiale. Dans une troisième étape, l'utilisation des données pour l'application est spécifiée. Enfin, la dernière étape consiste à identifier les obstacles existants et à les adresser par des mesures juridiques, techniques ou organisationnelles.

Ce modèle de gouvernance a été développé et testé à l'aide de deux applications concrètes de mobilité intelligente : la mobilité en tant que service (MaaS) et la tarification routière (Road User Charge, RUC).

Modèle de gouvernance MaaS
Dans le cas du MaaS, différents prestataires de services proposent leurs offres de mobilité sur la plateforme de l'intermédiaire. Celui-ci regroupe les offres et les met à la disposition des utilisateurs. Il apparaît que la mise en œuvre de telles offres MaaS se heurte principalement à des **obstacles juridiques** en termes de gouvernance des données et qu'il s'agit de définir les conditions dans lesquelles les acteurs sont prêts à partager leurs données. Les aspects techniques restent en revanche plutôt en retrait.

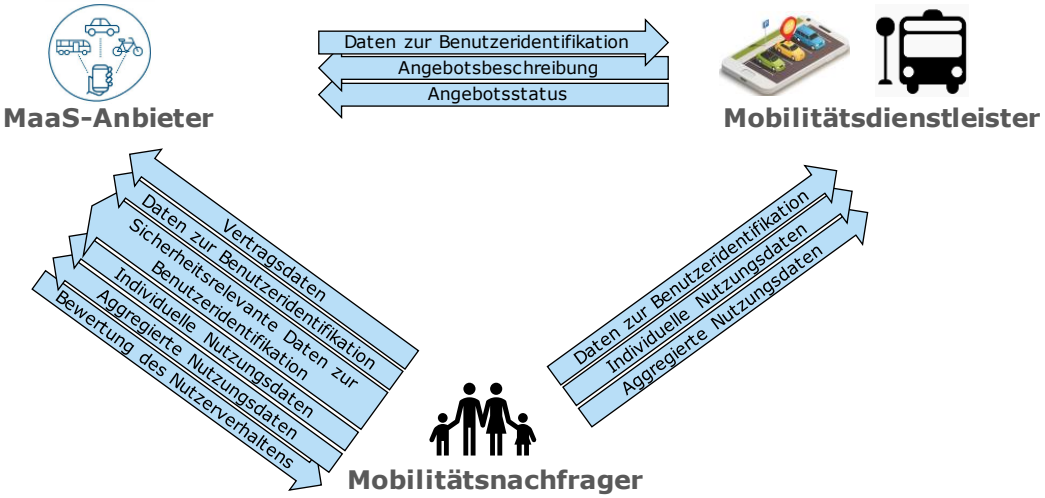


Fig. 4 *Flux de données dans l'application Smart Mobilty MaaS*

Concrètement, les prestataires de services de mobilité sont généralement prêts à mettre à disposition des données relatives à l'offre, mais peuvent émettre des réserves quant à l'accès généralisé aux données relatives à la distribution (notamment les données d'utilisation individuelles et agrégées, les données relatives à l'état de l'offre et les données contractuelles), car elles représentent une grande valeur économique pour les prestataires de services de mobilité. Il faut donc des principes et des **règles** clairs concernant l'**acquisition** et l'**utilisation des données**, qui doivent être développés par une instance neutre avec la participation des parties prenantes concernées. Du point de vue de la protection des données, l'introduction de règles de conduite communes et de certifications de protection des données en rapport avec les infrastructures centrales de données de mobilité pourrait créer la **confiance** de la part des fournisseurs de données potentiels et ainsi encourager l'échange de données. La confiance des prestataires de services de mobilité et des fournisseurs de MaaS dépend dans une large mesure de l'existence de règles et d'obligations claires, notamment en ce qui concerne l'accès à l'infrastructure et le routage, et de la procédure suivie pour les établir.

Modèle de gouvernance RUC

Dans le cadre de la mise en œuvre d'une redevance kilométrique généralisée pour tous les véhicules à moteur des utilisateurs privés en Suisse en remplacement des taxes sur les carburants, considérée comme un exemple d'application fictive de RUC, la **protection des données personnelles**, en particulier des profils de conduite individuels, est particulièrement importante.

Afin de garantir la saisie de tous les utilisateurs de l'infrastructure, il faut des offres spécifiques à l'utilisation pour la collecte des données de conduite nécessaires. Celles-ci peuvent provenir de véhicules en réseau, d'appareils dédiés ou de téléphones portables. Comme il s'agit d'une taxe obligatoire calculée sur la base de la collecte massive de données de mobilité, le principe de la **protection des données par la technique** ("privacy by design") doit être pris au sérieux afin de préserver la vie privée des individus.

Afin d'atteindre des normes techniques élevées en matière de gouvernance des données pour protéger les profils de mouvement des différents utilisateurs de l'infrastructure, il faut garantir que les données sensibles ne soient utilisées que pour le calcul des redevances et ne puissent pas être lues, traitées ou manipulées en texte clair par d'autres entités en dehors de l'utilisateur de l'infrastructure. Cela peut être garanti par l'utilisation de TEE au sein desquels les données des utilisateurs sont traitées exclusivement par des algorithmes certifiés. Tout autre accès est empêché, car les données et les résultats intermédiaires du calcul sont exclusivement disponibles sous forme cryptée dans la mémoire et ne sont décryptés que pendant le traitement au sein de la TEE.

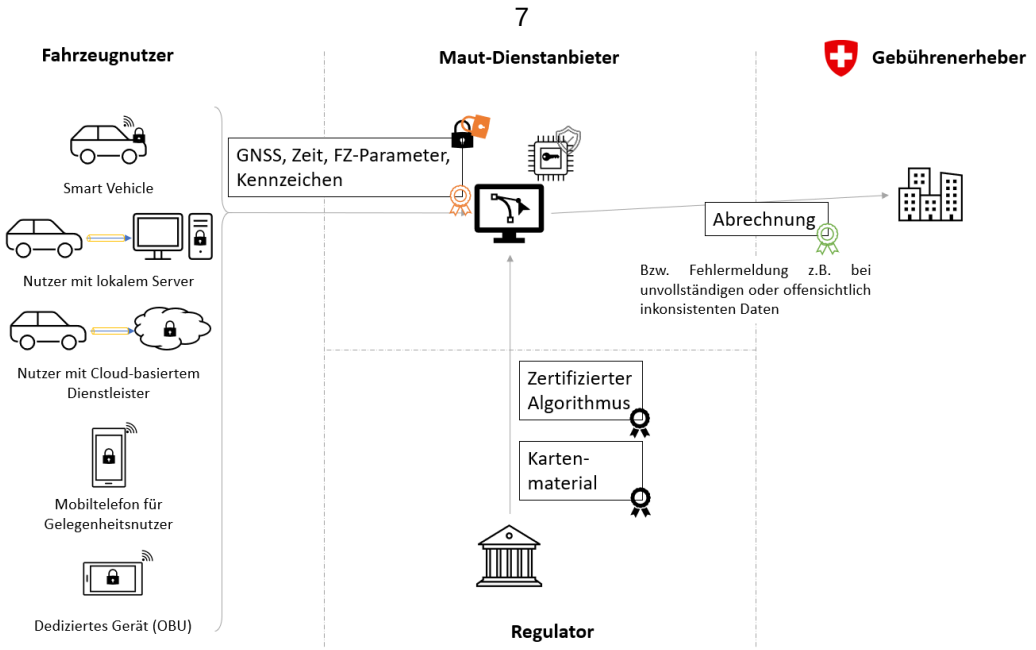


***Fig. 5** Approche respectueuse de la protection des données pour une tarification routière (RUC)*

Évaluation du modèle de gouvernance

L'élaboration d'éléments génériques a permis une analyse systématique et a fait ses preuves pour l'élaboration de modèles de gouvernance des données. La structuration des flux de données à l'aide des types de données génériques offre une base pour l'élaboration de modèles de gouvernance. En outre, le modèle de rôles utilisé s'est avéré être un instrument utile pour délimiter clairement les responsabilités des acteurs. La **systématisation** utilisée permet de classer les aspects organisationnels en fonction des responsabilités des différents acteurs. Elle offre également une base nécessaire pour développer les aspects juridiques et techniques.

Les **instruments juridiques** issus du droit de la propriété intellectuelle, de la protection des secrets commerciaux et du droit de la protection des données ont des conditions d'application, des objectifs et des conséquences juridiques différents. Dans l'ensemble, il peut en résulter un réseau complexe d'**attributions** en matière de Smart Mobility. Des **schémas de contrôle** ont été développés pour vérifier quels acteurs sont autorisés à utiliser quelles

données dans une offre de mobilité concrète. Cette attribution est essentielle pour la gouvernance des données : l'attribution initiale des données peut favoriser, compliquer ou rendre impossible l'utilisation de certaines offres de mobilité (et doit ensuite être corrigée dans le cadre de la gouvernance des données). Contrairement aux instruments d'attribution, le nombre d'instruments juridiques permettant aux acteurs **d'accéder aux données** d'autres acteurs est plus restreint. Néanmoins, des dispositions juridiques pouvant avoir un impact sur la gouvernance des données ont pu être identifiées ici aussi. Il s'agit de droits d'accès et de consultation découlant de la loi sur la transparence et d'obligations de divulgation spécifiques dans des lois spéciales de droit public, qui concernent typiquement les fournisseurs de prestations concessionnaires.

Le choix des **outils technologiques** dépend fortement de l'offre de mobilité considérée. Une spécification claire du cas d'utilisation permet de choisir concrètement des méthodes technologiques et cryptographiques pour la **protection des données**, **l'authenticité** ou **l'auditabilité**. Il n'est pas possible de donner des recommandations techniques génériques pour toutes les applications de mobilité intelligente. Celles-ci doivent plutôt être élaborées en fonction de l'application, afin de pouvoir mettre en œuvre la meilleure protection et sécurité des données possible sur le plan technologique, tout en répondant à des exigences élevées en matière d'efficacité et d'évolutivité. En revanche, le regroupement d'applications de mobilité intelligente permet à une solution développée d'être utilisée pour toute une classe d'applications. Pour chaque mise en œuvre technique, il convient en outre de se poser au moins deux questions centrales : D'une part, si le système développé répond aux **exigences fonctionnelles** et **de protection des données** posées. Cela peut être garanti par l'utilisation de modules cryptographiques testés par la communauté scientifique, par le respect des meilleures pratiques lors du choix et de la combinaison des composants et par la réalisation d'évaluations d'impact sur la protection des données. D'autre part, une fois qu'une conception est terminée, la question se pose de savoir si elle est correctement **mise en œuvre et implémentée**. Outre le choix de modules de haute qualité pour les composants sensibles à la sécurité, le type de certification nécessaire et la transparence de l'implémentation constituent un aspect central pour obtenir l'acceptation de tous les acteurs impliqués dans une application de mobilité intelligente par le biais d'une "confiance perçue".

Le **modèle générique de gouvernance des données** avec la procédure en quatre étapes a été développé, appliqué et testé pour le cas d'application MaaS et la perception de taxes routières (RUC). Il s'avère que les mesures à prendre pour éliminer les obstacles diffèrent selon le cas d'application. Selon l'infrastructure utilisée, les flux de données qui en résultent et le contrôle juridique sur les données, l'accent des mesures peut être mis plutôt sur l'aspect juridique ou sur l'aspect technique. Le modèle générique de gouvernance des données a fait ses preuves dans la mesure où il est - pour autant que l'on puisse en juger - applicable à toutes les applications de mobilité considérées, afin de développer des mesures de gouvernance des données spécifiques à l'application.

En ce qui concerne le **MaaS, l'**examen du **cadre juridique actuel** montre que le législateur a implicitement pris en compte le voyage monomodal lors de l'adoption des dispositions pertinentes. Par conséquent, il existe des dispositions qui ne s'appliquent pas ou difficilement aux voyages multimodaux. Ainsi, en cas de suppression ou de retard dans une partie de la chaîne de voyage, il n'existe pas de règles uniformes concernant le droit à la poursuite du voyage, au remboursement ou à l'indemnisation. Une adaptation du cadre juridique pourrait contribuer à augmenter l'attractivité des offres MaaS. En outre, le choix de l'infrastructure technique est décisif pour le MaaS. Une **infrastructure centrale** avec un intégrateur MaaS intermédiaire (IMI) permet de lutter contre la fragmentation du marché. Cette décision de conception implique toutefois une exigence de gouvernance selon laquelle tous les acteurs doivent pouvoir participer à cette infrastructure à des conditions non discriminatoires. D'un point de vue technique, il s'agit de savoir comment les données peuvent être **standardisées de manière interopérable** et comment de grandes quantités de données peuvent être calculées de manière complexe avec des temps de réaction rapides. D'un point de vue juridique, il s'agit de savoir quelles **conditions** générales peuvent être établies pour l'utilisation de l'infrastructure.

Dans le contexte de la tarification routière **(RUC)**, le défi de la gouvernance des données est la fourniture obligatoire de données par les utilisateurs. Cela nécessite une **conception de système digne de confiance** avec des **processus** et **des acteurs** tout aussi dignes de confiance. Il ne s'agit pas seulement de se protéger d'une éventuelle surveillance par

l'État, mais aussi de faire en sorte que le système offre des garanties afin que les données ne puissent pas être transmises à des tiers. Ce qui est indispensable dans un modèle de marché, c'est que tous les utilisateurs paient les mêmes redevances pour les mêmes trajets, indépendamment de leur équipement technique et du fournisseur de services choisi. C'est ce que garantit la solution présentée, avec la mise à disposition d'un **TEE** doté d'un algorithme certifié pour le calcul de la redevance et son contrôle. Ce n'est qu'au sein de cet environnement de calcul sécurisé que les données peuvent être décryptées et traitées sans qu'aucune partie n'y ait accès. La **certification est** effectuée par un organisme tiers et constitue un ancrage central de confiance. Ces approches permettent de s'assurer que la gouvernance organisationnelle et juridique est garantie par l'utilisation d'outils technologiques.

Conclusion et recommandations
Dans le cadre de ce travail, il s'est avéré que le modèle de gouvernance proposé permettait d'analyser de manière uniforme l'**interaction entre les** aspects organisationnels, juridiques et techniques. Ainsi, lors du développement de services dans la "nouvelle mobilité", il est possible de développer et d'implémenter une gouvernance des données adaptée. Selon l'application de mobilité, l'accent peut être mis sur les aspects juridiques (comme pour le MaaS) ou techniques (comme pour le RUC). L'une des principales conclusions du projet de recherche est que les structures de gouvernance - indépendamment de l'application concrète de la mobilité - doivent avant tout instaurer **la confiance** entre les acteurs et que l'instauration de cette confiance nécessite, dans l'idéal, l'intégration précoce de tous les groupes d'intérêt.

Les modèles développés dans ce projet de recherche peuvent contribuer à promouvoir la gouvernance des données pour la mobilité suisse. Concrètement, trois recommandations se dégagent du point de vue des disciplines impliquées dans le projet de recherche :

1. **Appliquer** et, le cas échéant, développer le modèle général de gouvernance
2. **Adaptation** du cadre juridique pour le MaaS
3. **Étude de faisabilité** sur les environnements de calcul sécurisés pour RUC

Summary

Problem description
Electrification, automation and digitalisation are the technological developments that are currently changing the offerings of transport means. These technologies enable not only electric-powered, automated, and networked vehicles and infrastructures, but also new offerings of mobility services. Providers of mobility services are trying to satisfy the societal needs for mobility with easily accessible and personalized offers and with **new business models**.

In traditional mobility businesses, vehicles and infrastructure were the main assets of operators, but in the future mobility business, digital platforms, service bundles, connected offers and increasingly global reach will be key. The services for users are changing completely: today the offering consists of "traffic and transport" often with a single mode of transport. In the future, the basic offering will be "mobility". To enable these new mobility services, large amounts of data and "intelligent" processes for the analysis and processing of very diverse **data** are necessary.

The DAGSAM project aims to find legal, technical and organisational system approaches for such demanding data-driven systems in the digitalised mobility world that make it possible to regulate sovereignty over the data and its use by means of a **"data governance"** while safeguarding the interests of all involved parties. The main goal of the project is to find a governance model based on defined relationships between the actors and supported by technical means.

Systematisation of the mobility offers
Smart **mobility** applications are evolving rapidly due to digitalisation, automation, connectivity and technological advances. DAGSAM provides a toolbox to address governance issues. To be able to make generally valid statements on governance questions in view of the diversity and market dynamics of **smart mobility applications**, the first step was to identify the involved actors and the existing data flows.

It was shown for all Smart Mobility applications that the roles of the actors can be represented with a generic role model. The **service provider** supplies the underlying service, such as the transport of people. The **intermediary** has the primary contractual relationship with the user, brings together supply and demand, bundles offers and offers mobility products. The **user** consumes mobility-related services and the **regulator** is the entity that sets the general framework.

Through a process analysis, the data flows between the actors were then determined and generic data types assigned. It was shown that the role model and the classification of the data flows into generic data types are applicable to all the smart mobility applications considered.

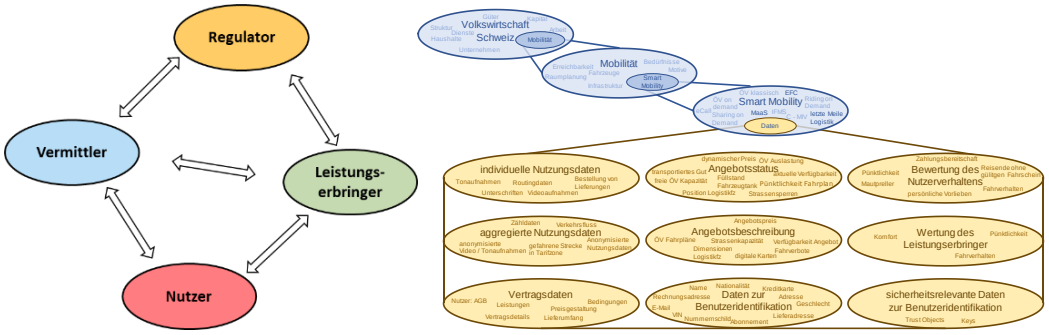


***Fig. 1** Role model used and generic data types*

Legal instruments
In order to clarify the legal aspects of data governance, the relevant legal instruments have been compiled. Although there is no known ownership right to data in the Swiss legal system, there are several instruments that can be used to **attribute data** to somebody. These

include assignment norms, protection norms, the contractual assignment of data and assignment based on data protection law.

A first group of provisions refers to those instruments that grant exclusive rights (**absolute rights**) to data to a natural or legal person. Possible absolute rights to data in Switzerland include intellectual property rights (copyright, patent law, design law, trademark law) and the so-called performance protection rights regulated by copyright law. A second group of provisions refers to those instruments that grant a **legal protection** to data that is actually controlled by a natural or legal person. Thus, the protection applies to whoever exercises actual dominion over the data. Such a provision can be found, for example, in the competition law protection of manufacturing and trade secrets (art. 6 UWG). Data can also be assigned to a rights holder by means of **contractual agreements**. Although such contracts only apply between the parties to the contract, the freedom of contract allows the parties to create a legal situation that is close to an exclusive right. Finally, **data protection law provides** for a certain attribution of data that relates to one or several persons. The handling of personal data is regulated by the Swiss Data Protection Act, which will enter into force in revised form on 1 September 2023 (nDSG).

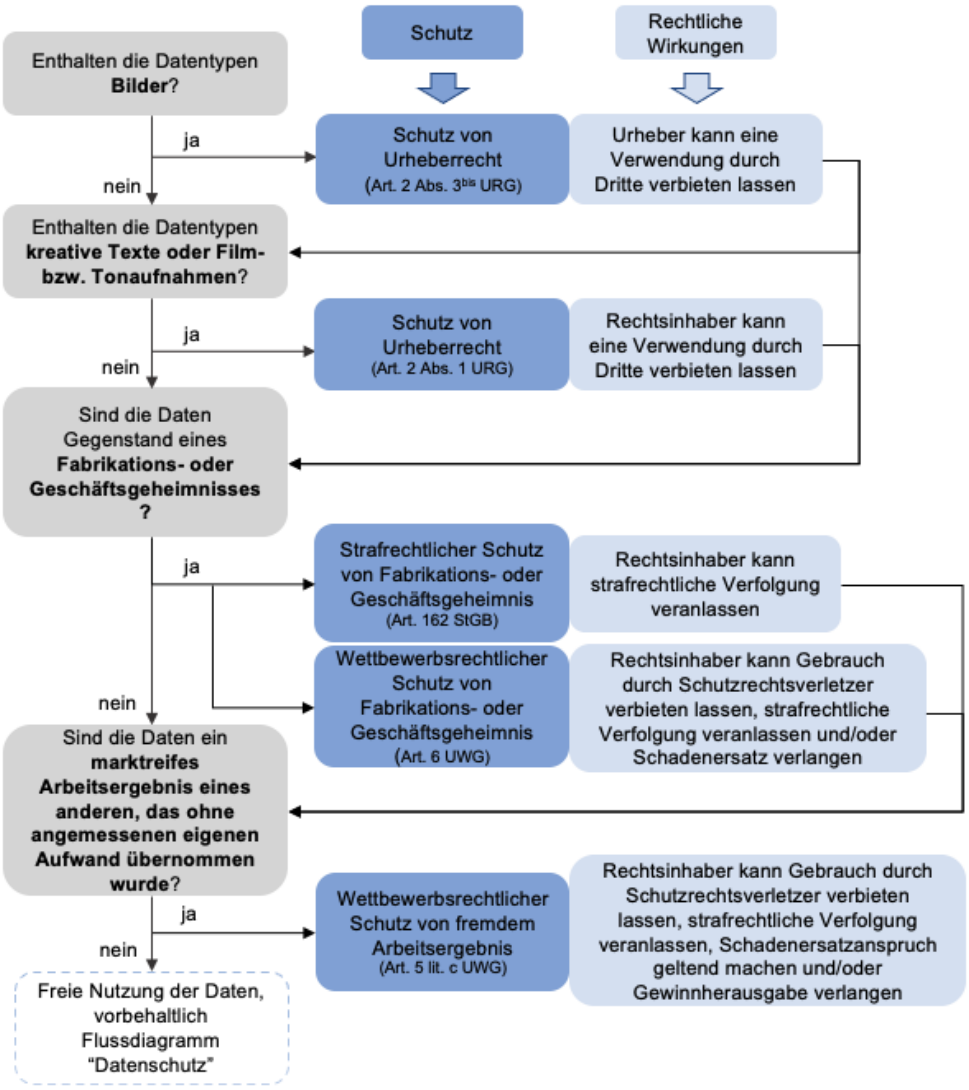


Fig. 2 *Verification scheme to attribute the data*

Technological instruments

In order to implement Data Governance technologically, selected technologies are presented. These allow calculations to be performed on data while at the same protecting the interests of the parties involved, be it in terms of personal data protection or of business secrets. Depending on the application and the corresponding complexity of the calculations, the selected technologies are suitable to varying degrees.

Secure Multi-Party Computation (MPC) describes a class of cryptographic protocols that allow multiple parties to perform joint computations on confidential input data. It ensures that each party only knows the defined result of the computation, but not further information about the input data of the other participants.

A **Trusted Execution Environment** (TEE) creates a secure environment in which sensitive data and code are shielded from access by external processes, including the operating system. It is a hardware extension that allows for the trusted execution of computations within an otherwise potentially untrustworthy environment. In a TEE, the confidentiality, authenticity of the executed programme code, and the integrity of the executed computations are guaranteed by means of certifications.

Fully Homomorphic Encryption (FHE) allows any calculations to be performed in encrypted domains. That is, the data does not have to be decrypted for the calculations. In particular, this enables the outsourcing of computations to untrusted cloud environments, as the confidentiality of the data is not undermined.

Governance model

The generic governance model takes into account the totality of all norms and conditions that are decisive for the functioning of a Smart Mobility application. The norms can be both technical and organisational in nature, and can become part of the legislation by normative reference. The conditions include the economic viability of a mobility offer and, as an elementary aspect, the necessary trust between the actors.

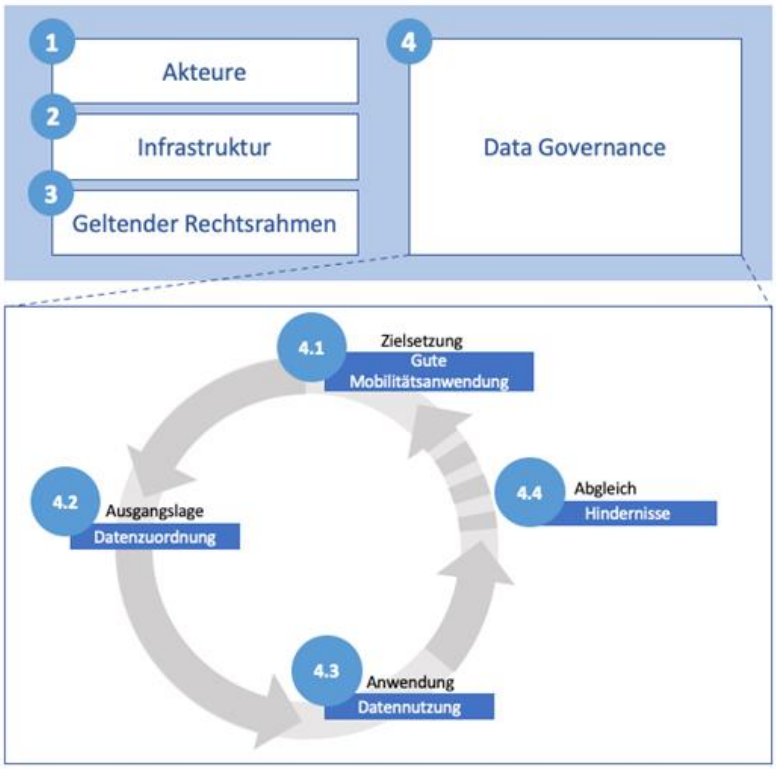


***Fig. 3** Generic governance model in four steps*

The first step is to identify the **actors** and define their competences and responsibilities. Subsequently, the **infrastructure** necessary for data exchange is addressed to ensure the management of data access and data processing between the actors. In a third step, the **applicable legal framework is** examined. In a final step, the core of the matter is addressed - **data governance** - and thus the concrete handling of mobility data. A detailed analysis grid can be used to determine which technical, legal or organisational principles or rules are required in relation to the specific mobility application. This analysis grid, in turn, provides for various steps. First, the good mobility application is defined as a goal. This is followed by an analysis of the data assignment in the initial situation. In a third step, the data

usage for the application is specified. Finally, in the last step, the existing obstacles are identified and addressed with legal, technical or organisational measures.

This governance model was developed and tested on the basis of two concrete smart mobility applications, Mobility-as-a-Service (MaaS) and Road User Charge (RUC).

Governance-Model MaaS
With MaaS, various service providers offer their mobility services on the platform of the intermediary. The intermediary bundles the offers and makes them available to the users. It turns out that when implementing such MaaS offers with regard to data governance, mainly **legal obstacles** arise and it is about setting conditions under which the actors are willing to share their data. Technical aspects remain rather in the background.

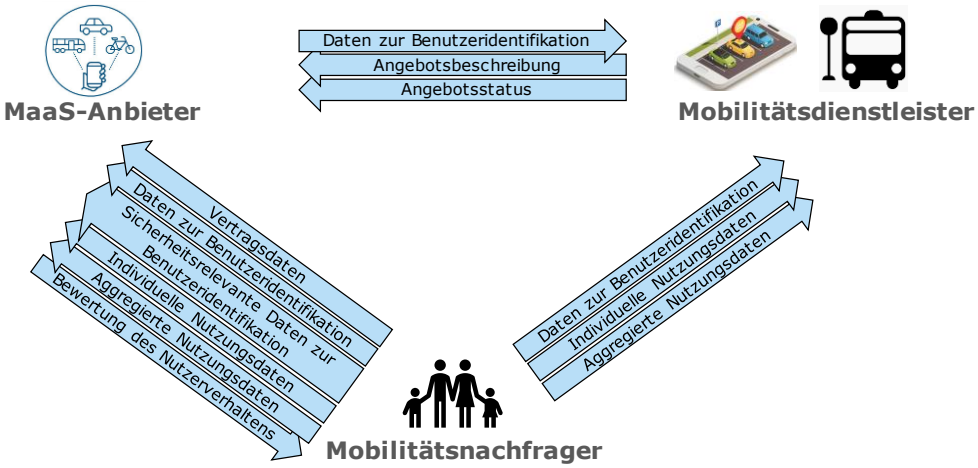


Fig. 4 *Data flows in the Smart Mobility application MaaS*

Mobility service providers are generally willing to provide data on their offerings, but they may have reservations about making data on their sales accessible (especially individual and aggregated usage data, data on the availability of the service, and contract data) because this data represent a great economic value for them. Therefore, clear principles and **rules** concerning **data access and use** need to be developed by a neutral party involving relevant stakeholders. From a data protection perspective, the introduction of common codes of conduct and data protection certifications in connection with central mobility data infrastructures could create **trust** on the part of potential data providers and thus promote data exchange. The trust of mobility service providers and MaaS providers depends largely on whether there are clear rules and obligations, in particular regarding access to the infrastructure and routing, and in which procedure these are established.

Governance-Modell RUC
In the implementation of a nationwide mileage-based levy for all motor vehicles of private users in Switzerland as a replacement for fuel levies, considered as a fictitious example application for RUC, the **protection of personal data**, in particular individual driving profiles, is a particular focus.

In order to ensure the coverage of all infrastructure users, user-specific offers are needed for collecting the necessary driving data. These can come from networked vehicles, dedicated devices or mobile phones. Since this is a mandatory levy calculated based on the mass collection of mobility data, the principle of **privacy by design** must be taken seriously in order to protect the privacy of individuals.

To achieve high technical standards of data governance to protect the movement profiles of individual infrastructure users, it must be ensured that sensitive data is only used for charging purposes and cannot be read, processed or manipulated in plain text by other entities apart from the infrastructure user. This can be guaranteed by the use of TEEs, within which user data is processed exclusively by certified algorithms. Any other access is prevented, as the data as well as intermediate results of the computation are stored exclusively in encrypted form and are only decrypted during processing within the TEE.

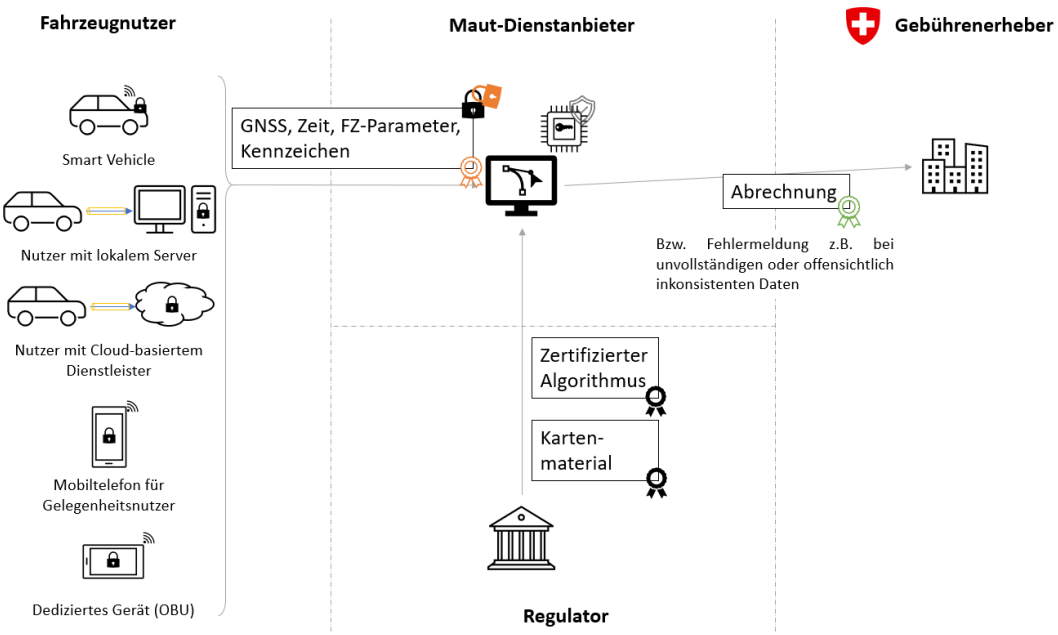


***Fig. 5** Privacy-friendly approach to road user charging (RUC)*

Evaluation of the governance model

The elaboration of generic elements has enabled a systematic analysis and has proven useful for the development of data governance models. The structuring of data flows based on the generic data types provides a basis for the creation of governance models. In addition, the role model used proved to be a useful tool for clearly delineating the responsibilities of the actors. The **systematisation** used is suitable for classifying the organisational aspects in terms of the responsibilities of the different actors. This also provides a necessary basis for developing the legal and technical aspects.

The **legal instruments** from intellectual property law, the protection of trade secrets and data protection law have different application requirements, objectives and legal consequences. All in all, this can result in a complex network of **allocations** in relation to smart mobility. **Test schemes** have been developed that can be used to check which actors are entitled to which data in a specific mobility service. This allocation is essential for data governance: the initial allocation of data can facilitate, hinder or make impossible the use of certain mobility offers (and must then be corrected as part of the data governance). In contrast to the allocation instruments, the number of legal instruments that provide actors with **access** to the data of other actors is smaller. Nevertheless, legal provisions that can have an impact on data governance could also be identified here. These are rights to information and inspection that arise from the Public Information Act and specific disclosure obligations in special laws under public law that typically concern state-licensed service providers.

The choice of **technological tools** strongly depends on the mobility service under consideration. A clear specification of the use case allows the selection of specific technological and cryptographic methods for **data protection**, **authenticity** or **auditability**. There cannot be any generic technical recommendations for all Smart Mobility applications. Rather, these must be worked out on an application-specific basis in order to be able to implement the best possible technological data protection and data security with simultaneously high demands on efficiency and scalability. On the other hand, the grouping of smart mobility applications allows a developed solution to be used for an entire class of applications. With every technical implementation, at least two central questions must be asked: On the one hand, whether the developed system fulfils the **functional** and **data protection requirements.** This can be ensured by using cryptographic building blocks tested by the scientific community, by following best practices in the selection and combination of components and by carrying out privacy impact assessments. On the other hand, once a design has been finalised, the question arises as to its **correct realisation and implementation**. In addition to the selection of high-quality building blocks for security-sensitive components, the required type of certification and transparency of the implementation are a central aspect to

achieve "perceived trust" and thereby creating acceptance by all actors involved in a smart mobility application.

The **generic data governance model** with the four-step approach was developed, applied and tested for the MaaS and road user charging (RUC) use cases. It turns out that the measures to remove the obstacles differ depending on the use case. Depending on the infrastructure used, the resulting data flows and the legal control over the data, the focus of the measures can be more on the legal or on the technical aspect.

The generic data governance model has proven itself in that it is - as far as can be seen - applicable to all mobility applications considered to develop application-specific data governance measures.

In the context of **MaaS,** a look at the **current legal framework** shows that the legislator implicitly assumed monomodal travel when enacting relevant regulations. Accordingly, there are regulations that cannot be applied to multimodal travel, or can only be applied with difficulty. For example, in the event of a breakdown or delay in one part of the travel chain, there are no uniform rules regarding entitlement to onward travel, reimbursement or compensation. In this regard, an adjustment of the legal framework could contribute to increasing the attractiveness of MaaS offers. In addition, the choice of technical infrastructure is crucial for MaaS. A **central infrastructure** with a so-called Intermediary MaaS Integrator (IMI) is intended to counteract a fragmented market. However, this design decision implies the governance requirement that all actors must be able to participate in this infrastructure on non-discriminatory terms. From a technical point of view, the focus is on how data can be **standardised in an interoperable way** and how large amounts of data can be calculated in a complex way with fast response times. In legal terms, the focus is on which generally applicable **conditions** can be established for the use of the infrastructure.

In the context of road user charging **(RUC),** the challenge for data governance is the mandatory data delivery by the users. This requires a **trustworthy system design** with equally trusted **processes** and **actors**. This is not only about protecting oneself from possible state surveillance, but also about the system having to provide safeguards to prevent data from being leaked to third parties. It is indispensable in a market model that all users pay the same charges for the same routes, regardless of their technical equipment and service provider. This is guaranteed by the solution presented, with the provision of a **TEE** with a certified algorithm for calculating the levy and for its control. Only within this secure computing environment can data be decrypted and processed without any party having access to it. **Certification** is done by a third party and provides a central anchor of trust. These approaches ensure that organisational and legal governance is guaranteed using technological tools.

Conclusion and recommendations

This research showed that the proposed governance model can be used to uniformly analyse the interplay of organizational, legal and technical aspects when developing services in the “new mobility”. Depending on the mobility application, the focus can be on legal aspects (as with MaaS) or technical aspects (as with RUC). A central finding of the research project is that governance structures - regardless of the concrete mobility application - must first and foremost create **trust** between the actors and that the building of trust ideally requires the early integration of all stakeholders.

The models developed in this research project can contribute to promoting data governance for Swiss mobility. Specifically, from the perspective of the disciplines involved in the research project, three recommendations arise:

1. **Application** and, if necessary, further development of the general governance model
2. **Adaptation of** the legal framework for MaaS
3. **Feasibility study** on secure computing environments for RUC

1 Zielsetzung und Ausgangslage

1.1 Problembeschreibung

Elektrifizierung, Automatisierung und Digitalisierung sind die technologischen Entwicklungsfelder, die das Angebot an Verkehrsmitteln derzeit stark verändern. Diese Technologien ermöglichen jedoch neben elektrisch betriebenen, automatisierten und vernetzten Fahrzeugen und Infrastrukturen insbesondere auch neue Angebote an Mobilitätsdiensten. Mobilitätsdiensteanbieter versuchen die gesellschaftlichen Bedürfnisse nach Mobilität durch leicht zugängliche und individualisierte Angebote und mit neuen Geschäftsmodellen zu befriedigen

Während im herkömmlichen Mobilitätsgeschäft die Fahrzeuge und Infrastruktur die wichtigsten Aktivposten der Betreiber waren, sind es im künftigen Mobilitätsgeschäft digitale Plattformen, Dienstleistungsbündel, vernetzte Angebote und eine zunehmend globale Reichweite. Die Dienstleistungen, die den Nutzerinnen und Nutzern angeboten werden, sind im Begriff, sich völlig zu verändern: Heute besteht das Angebot aus "Verkehr und Transport", oft mit einem einzigen Verkehrsmittel. In Zukunft wird das Grundangebot "Mobilität" sein. Den Nutzerinnen und Nutzern wird ermöglicht, Orte zu erreichen, die ihren Interessen entsprechen, ohne dass sie sich um die Verkehrsmittel zu kümmern brauchen. Dies zeigt sich exemplarisch am Konzept "Mobility-as-a-Service (MaaS)": Die Nutzerinnen oder Nutzer[1] müssen kein Auto besitzen, keine Fahrkarten kaufen und sich nicht mit der Wahl der geeigneten Verkehrsmittel beschäftigen. Stattdessen ermöglichen integrierte intermodale Mobilitätsdienstleistungen den Nutzern, sich nur auf das Ziel der Reise zu fokussieren und auf dem Weg dahin nahtlos von einem Verkehrsmittel auf andere umzusteigen.

Für die fernere Zukunft wird erwartet, dass diese neue Mobilität noch fortschrittlichere Geschäftsmodelle hervorbringen wird, die den "Zweck der Mobilität" verkaufen. So wäre die Beförderung einer Person nur noch ein untergeordneter Aspekt und Mobilität würde schliesslich zur "commodity", d.h. zur zunehmend gesichtslosen Massenware. Mit neuen Geschäftsmodellen betreten auch neue Akteure das Feld, die ihrerseits ein breiteres Spektrum an Dienstleistungen anbieten und neue Arten der Wertschöpfung generieren (siehe *Abb. 1*).

Die Abbildung verdeutlicht, dass sich der Umfang der Geschäftsmodelle von unten nach oben, d. h. von der Vergangenheit in die Zukunft, erweitert, gleichzeitig die Akteure grösser und globaler und die Geschäftsgüter zunehmend virtuell werden.

An solchen Zukunftsmärkten für Mobilitätsdienstleistungen besteht allgemein ein grosses Interesse, weil diese eine effizientere Infrastruktur- und Ressourcennutzung sowie ein nachhaltigeres Verkehrs- und Transportsystem versprechen (vgl. der Europäische Grüne Deal der EU).

[1] In der Folge wird für die Beschreibung der “Rolle” der Nutzerinnen und Nutzern nur noch der generische Begriff “Nutzer” verwendet. Dieser inkludiert sämtliche Personen, die Dienstleistungen im Bereich der Mobilität konsumieren.

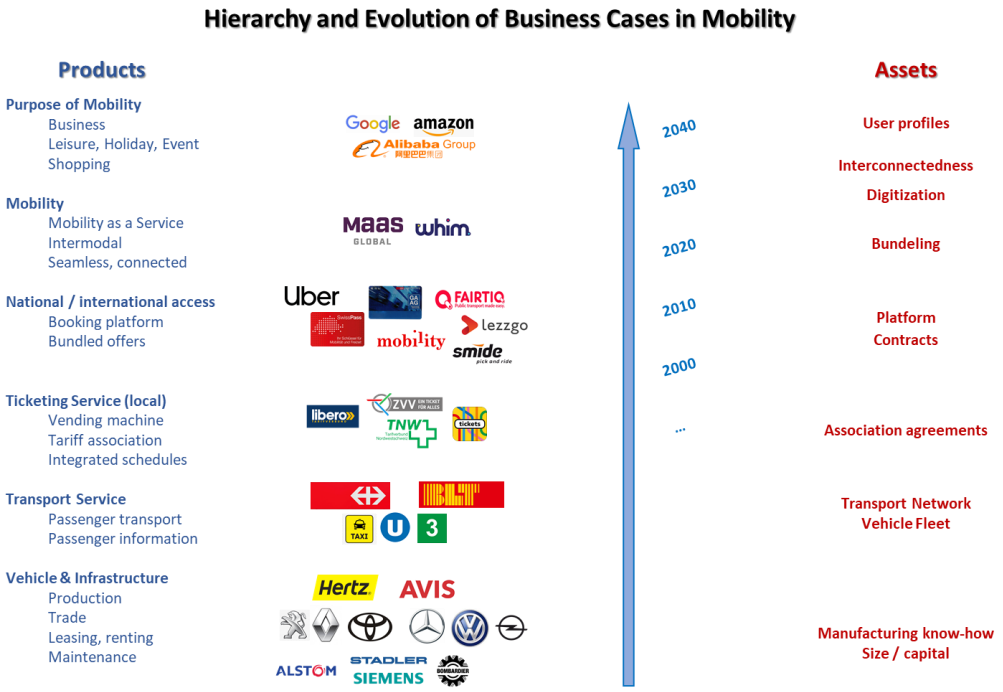


***Abb. 1** Entwicklung der Produktmärkte für Mobilität (its-ch, Arbeitsgruppe "Daten", https://www.its-ch.ch/publikationen/)*

Um diese neuartigen Mobilitätsdienste zu ermöglichen, sind grosse Datenmengen sowie "intelligente" Prozesse zur Analyse und Verarbeitung der sehr diversen Daten notwendig. Benötigt werden statische, dynamische und Echtzeit-Daten über Fahrzeuge, Infrastruktur, Dienstleistungsangebote, Ereignisse sowie Nutzer und Nutzerinnen. Die Datensätze haben unterschiedlichste Eigenschaften, bspw. in Bezug auf deren Vollständigkeit, Korrektheit, Qualität, Aktualität, Inhaberschaft und Stellung hinsichtlich datenschutzrechtlicher Vorgaben. Daten werden zudem auch durch die Bereitstellung der Dienste selbst generiert, wie z.B. Verkehrsdaten, Bewegungsdaten und Abrechnungsdaten. Oft führen gerade die so erzeugten und weiterverarbeiteten Daten z.B. in Form von Nutzerprofilen, von Informationen über Mobilitätsmerkmale oder von mobilitätsspezifischen Präferenzen zu einem gewinnbringenden Geschäft.

Auch für regulatorische Stellen wird zunehmend die Auswertung grösserer Datenmengen relevant. Beispielsweise liesse sich ein Erhebungssystem für Strassengebühren, welches die tatsächlich gefahrenen Strecken eines Fahrzeugs berücksichtigt, effizient umsetzen, indem künftig die Strassenverkehrsteilnehmenden verpflichtet werden, relevante Informationen (Bewegung, aber evtl. auch zur Belegung des Fahrzeugs) durch Erfassungsgeräte aufzeichnen zu lassen. Auf dieser Basis liessen sich aber nicht nur die Strassengebühren berechnen, sondern aus den Bewegungsprofilen neben der Identität des Nutzers auch weitreichende Informationen zu seinem Verhalten extrahieren. Viele Mobilitätsanwendungen bearbeiten in ähnlicher Weise äusserst sensible persönliche Daten. Es genügt hierbei nicht, die datenschutzrechtlichen Vorgaben formell einzuhalten. Gefordert ist nach dem Prinzip "privacy by design" bereits eine datenschutzfreundliche technische Konzeption des Systems. Darüber hinaus braucht es die Akzeptanz der Bevölkerung. Stellt sich bei den Nutzerinnen und Nutzern das Gefühl ein, "der Staat fahre mit", kann dies auch durch eine datenschutzkonforme Umsetzung nicht aus der Welt geschafft werden. Entsprechend braucht es versteh- und überprüfbare Massnahmen, die Vertrauen in den Schutz der persönlichen Daten schaffen.

Es ist ein Ziel von DAGSAM, für solche anspruchsvolle datengestützte Systeme in der digitalisierten Mobilitätswelt rechtliche, technische und organisatorische Systemansätze zu finden, die die Interessen aller beteiligten Akteure möglichst gut zu wahren imstande sind. Neben rechtlichen Vorgaben und technischen Ansätzen können auch organisatorische Massnahmen helfen, die Hoheit über die Daten, die "Data Governance", so auszugestalten, dass die Interessen der Akteure ausgewogen berücksichtigt werden. Auch wenn im

Beispiel der Gebührenerhebung heute beide Kerntätigkeiten, die Erfassung der Daten und die Erhebung der Gebühren, von ein und derselben Institution wahrgenommen werden, ist ein Rollenmodell vorzuziehen, das zwischen der Rolle desjenigen, der das Fahrprofil erfasst (der "Dienstleister") und demjenigen, der die Gebühr abrechnet (der "Erheber") trennt. Dem Erheber muss im Grunde nur die Fahrleistung pro Fahrzeug bekannt sein, jedoch nicht die genauen Orte und Fahrtrouten der Fahrzeuge (INFRAS/Rapp/Ecoplan, 2021). Der Dienstleister kennt zwar potenziell die Fahrprofile seiner Kunden, kann aber vom Nutzer auch frei gewählt werden. Der Nutzer kann sich also am Markt unter mehreren Angeboten den Dienstleister seines Vertrauens auszusuchen. Entsprechend würde die künftige institutionelle Trennung der Rollen die Hoheit über die Daten angemessener verteilen. Neben solchen organisatorischen Ansätzen untersucht DAGSAM auch technische Ansätze, die Datenzugänge durch kryptographische Methoden nur denjenigen eröffnen, die sie benötigen, und nur so weit, wie zur Erbringung ihrer Tätigkeiten notwendig. Wichtig sind dabei die Verständlichkeit und Beherrschbarkeit durch "normale Nutzer und Nutzerinnen“ ohne technische Kenntnisse.

Bei digitalen Infrastrukturen, die zwischen Akteuren der Mobilität vermitteln und es erlauben, Mobilitätsprodukte aus der Kombination mehrerer Einzelangebote verschiedener Transportunternehmen zusammenzustellen, stellen sich ebenfalls viele Fragen der Governance. Es geht insbesondere um Fragen der Haftung, um den Schutz von "*business assets*" und um die Hoheit über die genutzten Daten sowie die jeweilige Infrastruktur. Zur Realisierung einer digitalen Infrastruktur für Smart Mobility-Anwendungen, die die gesamte Intermodalität von öffentlichem Verkehr über privatwirtschaftliche Mobilitätsdienstleister bis hin zur Nutzung des motorisierten Individualverkehrs berücksichtigt, ist es zwingend notwendig, die Interessen aller Stakeholder abzubilden. Ansonsten entsteht die Gefahr, dass sich bedeutsame Stakeholder nicht am virtuellen Marktplatz der digitalen Infrastruktur beteiligen. Mit der NOVA-Plattform hat der öffentliche Verkehr (öV) in der Schweiz bereits eine Dateninfrastruktur für den übergreifenden Vertrieb von Fahrkarten geschaffen. NOVA ist die Vertriebsdrehscheibe und Datenbank für den öV der Schweiz, über die fast alle öV-Fahrausweise verkauft werden. Unterschiedliche Vertriebskanäle wie Mobile Apps, Ticketautomaten oder Busfahrer-Geräte beziehen die Verkaufsdaten von der NOVA-Plattform. NOVA vereint aktuell Angebote von rund 250 beteiligten Unternehmen. Entstanden ist NOVA aufgrund der Verpflichtung von konzessionierten Transportunternehmen zur gemeinsamen Ausgabe und gegenseitigen Anerkennung von Fahrausweisen. Daraus entstand eine gemeinsame Initiative der Transportunternehmen und Verbünde des öffentlichen Verkehrs für deren Umsetzung. Den Lead für die Umsetzung und den Betrieb von NOVA hat die SBB Informatik[2]. Die NOVA Plattform schloss - trotz formaler Öffnung - privatwirtschaftliche Mobilitätsdienstleister bis heute mittels hoher Hürden praktisch aus. Die NOVA-Plattform war *de facto* ein geschlossenes System, das nur konzessionierten Verkehrsunternehmen zur kommerziellen Nutzung offenstand. In der Revision des Personenbeförderungsgesetzes kam es diesbezüglich zu Anpassungen. Neu sollen diskriminierungsfreie Bedingungen für die Nutzung der Vertriebsinfrastruktur durch Dritte gelten (Bundesversammlung, 2022). Zudem werden über NOVA keine personenbezogenen Daten ausgetauscht, welche z.B. für Reservationen nötig wären.

Erweiterte Plattformen, die neben dem klassischen öV auch privatwirtschaftliche Mobilitätsdienstleister umfassen, haben weitere Hürden zu meistern. Die Angebote der Dienstleister stehen in Konkurrenz zueinander und haben keinen weitgehenden Gebietsschutz wie der klassische öV. Zudem haben privatwirtschaftliche Akteure Vertragsfreiheit, sie sind somit nicht in jedem Fall zu Angeboten verpflichtet und können verschiedenen Kunden oder Vertragspartnern verschiedene Tarife und Konditionen anbieten. Umso wichtiger ist für digitale Mobilitätsinfrastrukturen, dass die Kontrolle und Hoheit über die Daten von einer vertrauenswürdigen, neutralen Institution wahrgenommen und ein fairer Wettbewerb der Angebote gewährleistet wird. Ein virtueller Mobilitätsmarktplatz muss beispielsweise sicherstellen, dass die Marktteilnehmer sich zwar über alle Angebote detailliert informieren können, sich gleichzeitig aber nicht gegenseitig ausspähen können, bspw. im Hinblick auf Kostenstrukturen oder Schwächen im Angebot. Auch müssen Regeln für das Verhältnis zwischen dem regulierten Markt der öffentlichen Anbieter und dem freien Markt der privaten Anbieter gesetzt und überwacht werden.

[2] aus https://www.allianceswisspass.ch/de/asp/News/Newsmeldung?newsid=111

In Bezug auf einige Daten ist es wesentlich, dass sie gemeinsam genutzt werden können und möglichst frei zugänglich sind. Gleichzeitig gibt es Daten, die geschützt werden müssen, sei es zum Schutz der Privatsphäre der Nutzer oder zum Schutz allfälliger Geschäftsgeheimnisse vor der Übernahme durch Markteilnehmer. Neben diesen offensichtlichen Interessens- und Anforderungskonflikten geht es auch um Sicherheits- und Haftungsaspekte der Datennutzung. Am Ausgangspunkt solcher Überlegungen steht oft die Frage, wem Daten rechtlich "gehören". Daten sind nicht an nationale Grenzen gebunden und das Geschäftsumfeld wird in der Mobilität zunehmend globaler, dennoch müssen diese Fragestellungen im Schweizer Kontext und vor dem Hintergrund der nationalen Vorschriften geklärt werden.

Das Forschungsprojekt ist auch deshalb von unmittelbarem Interesse, weil der Bundesrat dem UVEK den Auftrag erteilt hat, ein Gesetz für eine Mobilitätsdateninfrastruktur (MODI) auszuarbeiten. Als deren Kernelemente sollen eine Nationale Datenvernetzungsinfrastruktur Mobilität (NADIM) für den Austausch von Mobilitätsdaten und das Verkehrsnetz Schweiz (VnCH) als Referenzbasis entwickelt werden. NADIM soll "offen, diskriminierungsfrei und transparent sein. Zudem verbleiben die Daten beim jeweiligen Eigentümer, der sie auch verwaltet" (BAV, 2021d). Weitere Informationen zu diesen Entwicklungen sind in Kap. 1.5 erläutert.

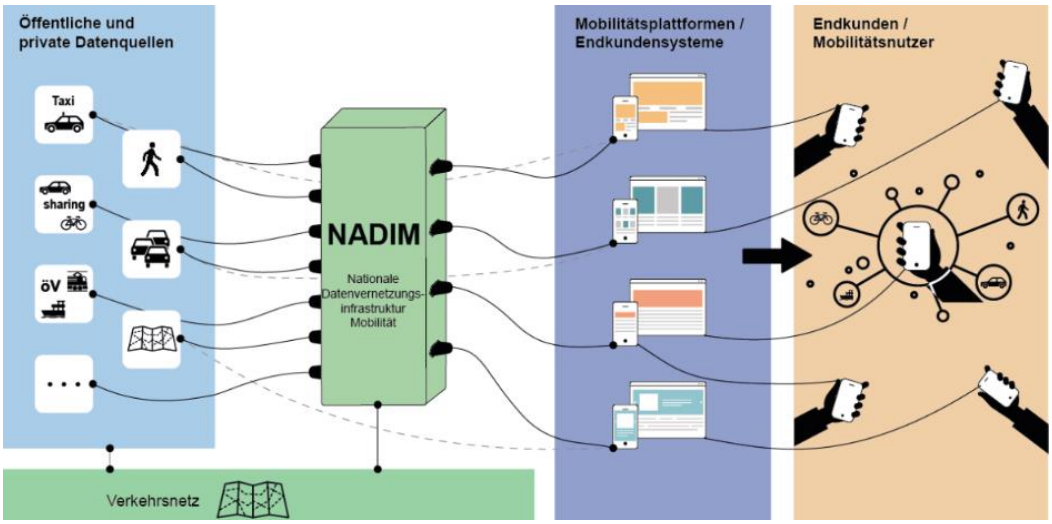


***Abb. 2** Konzeptionelle Funktionsweise der MODI*
Quelle (BAV, 2021d)

Die Industrie verlangt nach einem klaren und verlässlichen regulatorischen Umfeld, das die Entwicklung und Investition in die innovative Mobilität ermöglicht. Derzeit ist noch unklar, wie die legitimen Interessen der verschiedenen Akteure im Mobilitätsbereich miteinander in Einklang gebracht werden können. Diese ungeregelte Situation erleichtert derzeit einerseits die Entwicklung eines Dienstleistungsmarktes für intelligente Mobilität. Sie behindert aber gleichzeitig grossangelegte Einführungen und Investitionen aus der Sorge heraus, dass zu einem späteren Zeitpunkt *ad hoc*-Regelungen zu Sicherheits-/Haftungs-, Datenschutz- und Inhaberschaftsaspekten die Geschäftsmodelle behindern.

Die Veränderungen und Trends, die wir bereits erkennen können, deuten darauf hin, dass wir uns an einem kritischen Punkt für die Steuerung der intelligenten Mobilität befinden. Noch steht den politischen Entscheidungsträgern und Entscheidungsträgerinnen ein relativ breites Spektrum an Interventionsmöglichkeiten zur Verfügung, um in signifikanter Weise Einfluss auf neue Mobilitätsangebote zu nehmen (Docherty et al., 2018). In Anbetracht des Innovationstempos könnte dieses Zeitfenster für Smart Mobility jedoch sehr kurz sein und sollte genutzt werden.

Im Idealfall würde im Vorfeld eines regulatorischen Eingriffs ein Rahmen für die Datenverwaltung geschaffen, so dass die gemeinsame Nutzung von Daten bei Bedarf ermöglicht, der Zugang in gewissen Fällen aber kontrolliert oder einschränkt wird. Ein solcher Rahmen hat das Potenzial, den technisch-wirtschaftlichen und gesellschaftlichen Wandel zu

gestalten und erfordert eine Kombination aus rechtlichen, technischen und organisatorischen Instrumenten.

Vor diesem Hintergrund besteht das Hauptziel des Projekts darin, ein **Governance-Modell** zu finden, das auf definierten Beziehungen zwischen den Akteuren beruht und durch technische Mittel unterstützt wird. Hier kann die Schweiz (und Europa) die digitale Souveränität sicherstellen und sich klar und positiv positionieren zwischen dem amerikanischen Ansatz (maximale Wirtschaftsfreiheit für Unternehmen) und dem chinesischen Ansatz (maximale Kontrolle der Bevölkerung). Je nach Wahl der Infrastruktur und deren Grad der Zentralisierung können sich für die jeweilige Anwendung typische Systeme herausbilden, wie dies beispielsweise im Gesundheitssektor mit den so genannten Personal Information Management Systems (PIMS) zu beobachten ist. PIMS ermöglichen es den Patientinnen und Patienten, ihre persönlichen Informationen in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wann und mit wem sie wollen. PIMS werden geschaffen, um die Bedürfnisse des Einzelnen nach Privatsphäre mit den Vorteilen der gemeinsamen Nutzung von Daten in einer offenen Datenumgebung in Einklang zu bringen. Auf der Basis des Governance-Modells für Smart Mobility sollen für Mobilitätsanwendungen ähnliche Systeme entwickelt und ausgearbeitet werden können.

1.2 Projektvorhaben

1.2.1 Vorgehen und Methodik

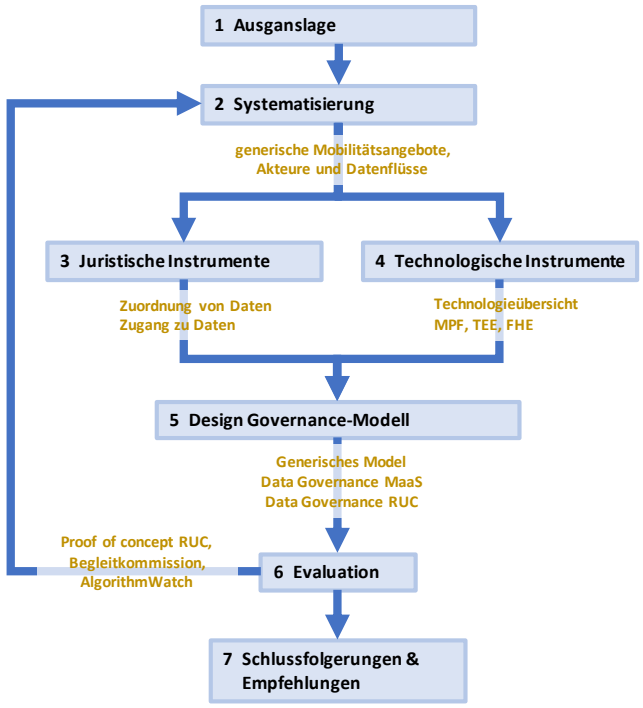


***Abb. 3** Methodik der Forschungsarbeit*

Um das oben beschriebenen Ziel zu erreichen, wurde in DAGSAM das in Abb. 3 dargestellte Vorgehen verfolgt. In einem ersten Schritt wird die Ausgangslage erarbeitet, um die Entwicklung des Governance-Modells in einen Gesamtkontext zu setzen (Kapitel 1).

Die Welt der Smart Mobility entwickelt sich rasant. Dadurch entstehen aktuell viele neue Mobilitätsangebote bzw. die bestehenden entwickeln sich weiter. Dies führt dazu, dass Mobilitätsangebote, die involvierten Akteure sowie die entstehenden Datenflüsse generalisiert und systematisiert werden müssen, damit ein generisches Governance-Modell entwickelt werden kann (Kapitel 2).

Daten sind keine physischen Sachen, sondern zunächst einmal bloss eine Folge von Nullen und Einsen, die – je nach Darstellungsform – einen Sinngehalt haben. Diese Eigenschaft macht die rechtliche Erfassung von Daten zu einer Herausforderung. Entsprechend müssen die juristischen Instrumente dargestellt werden, welche die Zuordnung von Daten und den Zugang zu Daten regeln (Kapitel 0).

Parallel dazu werden technologische Instrumente geprüft. Insbesondere werden die erfolgsversprechenden Technologien Multi Party Computation (MPC), Trusted Execution Environnements (TEE) sowie die vollständig homomorphe Verschlüsselung (FHE) genauer untersucht. Auf dieser Basis kann dargestellt werden, welche davon sich eignen, um Teile der Data Governance technologisch zu garantieren (Kapitel 4).

Mit den vorhandenen Grundlagen der systematisierten Mobilitätsangebote sowie den juristischen und technologischen Instrumenten wird 5 ein generisches Data Governance-Modell entwickelt. Das generische Modell wird anhand von zwei ausgewählten

Anwendungsfällen (Mobility as a Service – MaaS und Strassengebührenerhebung – RUC) angewendet, geprüft und weiterentwickelt (Kapitel 5).

Daran anschliessend werden die Resultate der Forschungsarbeit evaluiert. Dafür kommen mehrere Arbeitsschritte zur Anwendung. Einerseits werden die einzelnen Schritte bis zur Entwicklung eines Data Governance-Modells in den Kontext gestellt, in dem sie zwei Anwendungsfälle MaaS und RUC verwendet werden. Andererseits werden die Modelle anhand von Workshops mit der Begleitkommission sowie der AlgorithmWatch evaluiert (Kapitel 6).

Den Abschluss bilden konkrete Schlussfolgerungen, die sich aus dem Projekt und dem entwickelten Governance-Modell in den Gesamtkontext der smarten Mobilität einordnen lassen (Kapitel 7).

1.2.2 Eingrenzungen

Das vorliegende Projekt behandelt Fragen zur Governance von Mobilitätsdaten im Kontext von multimodalem Verkehr. In diesem Zusammenhang laufen seit Dezember 2018 Bestrebungen seitens des Bundes, eine nationale Mobiltätsdateninfrastruktur (MODI) aufzubauen, welche die Verfügbarkeit und den Austausch von Mobilitätsdatenflüssen zwischen Infrastrukturbetreibern, öffentlichen Verkehrsunternehmen und privaten Anbietern von Mobilitätsdienstleistungen sowie Kunden und Kundinnen gewährleisten soll. Die MODI enthält als Hauptbestandteile in einem ersten Schritt einerseits das Verkehrsnetz CH, welches die gesamte verkehrliche physische Infrastruktur der Schweiz einheitlich und digital abbilden soll und als räumliches Referenzsystem dient, und andererseits die NADIM, welche den Austausch von Mobilitätsdaten und die Vernetzung von Smart Mobility-Anwendungen erleichtern soll (BAV, 2021b; UVEK, 2022). Das im vorliegenden Projekt erstellte Governance-Modell wird unabhängig von den Vorhaben des Bundes im Zusammenhang mit der geplanten Mobilitätsdateninfrastruktur (MODI) entwickelt. Dies gilt insbesondere im Zusammenhang mit den Mobility-as-a-Service (MaaS). Es gehört weder zum Leistungsauftrag noch zum Ziel des vorliegenden Projekts, konkrete Umsetzungsvorschläge bezüglich der Regelung und dem Aufbau der MODI zu machen.

Das zu erarbeitende Governance-Modell soll naturgemäss möglichst generisch sein. Um aber dennoch konkrete und belastbare Aussagen machen zu können, wird das Governance-Modell anhand spezifischer Mobilitätsangebote entwickelt, geschärft und überprüft. Die Wahl der Mobilitätsangebote erfolgt nach bestimmten Kriterien (siehe dazu Kap. 5.1.3). Dennoch bleiben dadurch womöglich wichtige Aspekte anderer Mobilitätsangebote unberücksichtigt.

In sachlicher Hinsicht ist der Flugverkehr vom Anwendungsbereich des Forschungsprojekts ausgenommen, zumal das Hauptaugenmerk auf der schweizerischen Binnenmobilität liegt, für welche der Flugverkehr eine untergeordnete Rolle spielt.

Nicht gründlich vertieft werden im Weiteren die Wirtschaftlichkeit des Governance-Modells für einzelne Mobilitätsanwendungen, deren Qualitätssicherung und der unter Umständen notwendige technische und fachliche Support zu deren Umsetzung.

Und schliesslich kann das Forschungsprojekt auch nur in beschränktem Mass Aussagen dazu machen, wie das Vertrauen der Gesellschaft in die Bearbeitung der Mobilitätsdaten gesichert oder gestärkt werden kann: Während Aussagen zu rechtlichen, technischen und organisatorischen Vorkehrungen möglich sind, welche diesem Zweck dienen, sind psychologische oder politische Aspekte nicht Gegenstand des Projekts.

1.2.3 Kontext

Das vorliegende Projekt DAGSAM reiht sich in eine Serie von Forschungsprojekten im Bereich des Strassenwesens ein und ist Teil des Forschungskonzepts "Nachhaltiger Verkehr 2021-2024" und eines Forschungsschwerpunkts der Arbeitsgruppe "Mobilität 4.0" [3].

[3] Dokumente verfügbar unter: https://www.astra.admin.ch/astra/de/home/fachleute/weitere-bereiche/forschung/strategie-schwerpunkte.html

1.3 Stand der Forschung

Datenflüsse

Einige der Daten und Datenflüsse im Bereich von intelligenten Smart Mobility-Anwendungen sind bekannt. So sind beispielsweise die Datenflüsse im Zusammenhang mit kooperativen intelligenten Verkehrssystemen (C-ITS) weitgehend standardisiert (Festag, 2014; Javed et al., 2019). Ebenfalls ist das eCall-System der Europäischen Union, das im Falle eines Autounfalls automatisch die Rettungsdienste kontaktiert, gut dokumentiert (Bonyár et al., 2017). Entwicklungen wie diese haben die Automobilhersteller dazu veranlasst, Geräte zur Kommunikation und Geolokalisation in Fahrzeuge einzubauen, die die Grundlage für künftige Entwicklungen wie das autonome Fahren bilden werden. Derzeit liegt der Schwerpunkt darauf, die Kommunikationsbandbreite für die Fahrzeug-zu-Fahrzeug- oder Fahrzeug-zu-Infrastruktur-Kommunikation durch den Einsatz der mmWave-Technologie noch weiter zu erhöhen (Brambilla et al., 2019). Bei der mmWave Technologie handelt es sich um eine Funktechnologie in hohen, heute noch ungenutzten Frequenzbereichen, die als Teil des Mobilfunkstandards 5G zum Einsatz kommt. Künftige Fahrzeuge werden mit verschiedenen Clouds verbunden sein und diese mit Daten versorgen, um viele neuartige Dienste zu ermöglichen, z.B. auf der Grundlage von digitalen Zwillingen der Fahrzeuge. Als Teil der Standardwartung werden Fahrzeuge Software-Updates aus der Ferne benötigen, um die Cybersicherheit zu gewährleisten. Dieser Bereich wurde kürzlich durch neue Vorschriften der UNECE (UNECE, 2020) geregelt.

Während einige Datenflüsse öffentlich bekannt sind, sind viele Datenflüsse proprietär und unterstehen somit typischerweise einer Geheimhaltung. So ist beispielsweise nicht öffentlich bekannt, welche Daten die Fahrzeuge an die Cloud ihres Herstellers übermitteln, was zu Datenschutz- und Sicherheitsbedenken führt (z.B. Polizeifahrzeuge, deren Standort in Echtzeit verfolgt wird oder in denen die Kommunikation der Fahrzeuginsassen durch sprachaktivierte Assistenten laufend erfasst und möglicherweise aufgezeichnet wird). Die Identifizierung und Erfassung dieser proprietären Datenströme ist ein offenes Forschungsthema. Neben den Erstausrüstern werden auch Infrastrukturanbieter (für Autobahnen, Tunnel, Schienen), Telekommunikationsbetreiber (4G/5G-Netzdaten), Versicherungen (Unfallrecorder, Pay-as-you-drive) und Technologieunternehmen (Betriebssysteme, Clouddienste, Software, Navigation) und andere Akteure, die Daten produzieren, verarbeiten, sammeln und kombinieren, immer wichtigere Akteure in dem zukünftigen Ökosystem für intelligente Mobilität.

Datenschutz

Das Reisen auf der Strasse, in der Bahn oder in der Luft wird heute mehrheitlich digital erfasst. Durch Verkehrs-Apps, elektronische Tickets, private und staatliche Sensoren oder vernetzte Fahrzeuge können unsere Bewegungen im öffentlichen Raum und unser Aufenthalt an privaten Orten erfasst und gemessen werden. Durch die Kombination und Auswertung dieser Daten können Bewegungs- und Persönlichkeitsprofile erstellt werden.

Dies birgt verschiedene datenschutzrechtliche Gefahren (Lobsiger & Rudin, 2020), einschliesslich jener des Kontrollverlusts über Bewegungs- und Beziehungsdaten (Hilty, 2012; Schulz et al., 2020). Die strengere Regelung des sogenannten Profiling gehörte denn auch zu den umstrittensten Punkten bei der Revision des Datenschutzgesetzes (siehe Rosenthal, 2020).

Auf einer allgemeineren Ebene befasst sich die bestehende Forschung zu Profiling und Datenschutz in der Schweiz wie auch in der EU mit Fragen der Zweckbindung, Erkennbarkeit, Zustimmungsmöglichkeiten (Opt-in, Opt-out, etc.), Transparenz und Verhältnismässigkeit (Heuberger, 2020; Lorentz, 2020). Darüber hinaus beschäftigen sich einzelne Studien mit sektorspezifischen Fragen des Datenschutzes im Bereich der Mobilität (Baeriswyl, 2020; Gress & Springborn, 2020; Roßnagel, 2017; Sackmann, 2020; Spiecker-Döhmann, 2019). Die dort skizzierten Lösungsvorschläge bleiben unkonkret, wie z.B. die allgemeine Forderung nach einer Harmonisierung der Datenschutzbestimmungen im europäischen Binnenmarkt, dem Vorschlag einer Stärkung der exekutiven und judikativen Durchsetzung (Sackmann, 2020, S. 160 ff.) oder der Empfehlung an die verantwortlichen Stellen in UVEK und ASTRA, Konzepte für die Nutzung von Ortungsdaten zu entwickeln sowie sichere und vertrauenswürdige Anonymisierungsverfahren bereitzustellen (Hilty, 2012, S. 190 ff.). In den bisherigen Studien bzw. in der bisherigen Literatur wurde die Frage

des Profilings im Mobilitätssektor nur marginal behandelt. Im Rahmen der vorliegenden Studie wird deshalb insbesondere der Frage nachgegangen, wie mit Blick auf das Profiling effektive Governance-Modelle zum Schutz personenbezogener Daten im Mobilitätssektor ausgestaltet sein sollten.

Zuordnung von Daten und "Dateneigentum"

Bis heute sehen weder die Schweiz noch andere Rechtsordnungen in Europa ein spezifisches Ausschliesslichkeitsrecht an Daten im Sinne eines Eigentumsrechts vor (für die Schweiz Thouvenin & Früh, 2020) (für andere Länder Purtova, 2015), obwohl sowohl in der Schweiz als auch in der EU seit einigen Jahren die Notwendigkeit der spezifischen Einführung eines "Dateneigentums" kontrovers diskutiert wird. Während einige Autoren für ein solches Recht eintraten (Amstutz, 2018; Eckert, 2016; Fezer, 2017), wird die Einführung eines Dateneigentums vom grösseren Teil der Lehre und dem Bundesrat (Bundesrat, 2018) abgelehnt. Mit der Einführung eines allgemeinen Dateneigentums in der Schweiz ist aus heutiger Sicht nicht zu rechnen.

Obwohl an Daten kein Eigentumsrecht im engeren Sinne verliehen werden kann, können verschiedene Rechtsinstrumente wie das Immaterialgüterrecht (insbesondere das Patentrecht und das Urheberrecht) und der Schutz von Geschäftsgeheimnissen (durch Anwendung des Gesetzes gegen den unlauteren Wettbewerb [UWG] und des Strafrechts) ähnliche Wirkungen wie das Eigentumsrecht haben (Thouvenin & Früh, 2020, S. 10 ff.). Das Gleiche gilt für das Datenschutzrecht, da es dem Einzelnen spezifische, unveräusserliche Kontroll- und Zugangsrechte einräumt. Jedes dieser Instrumente zielt jedoch nicht auf Daten "als solche" ab und gilt nur unter bestimmten Voraussetzungen und Umständen. Dementsprechend ist jede Aussage zur Zuordnung von Daten im Mobilitätssektor höchst umständlich und die juristische Literatur zur Entwicklung spezifischer Ausschliesslichkeitsrechte in diesem Sektor ist spärlich (Priora & Sganga, 2020).

"**Data Governance**"

Die Rechtswissenschaft hat erkannt, dass die Zuordnung von Daten nur ein Teil einer umfassenden "Data Governance" ist. Die Praxis zeigt, dass Dateninhaber dazu tendieren, ihre gespeicherten Daten zu kontrollieren und nach aussen unter Verschluss zu halten, wobei jeweils von sog. Datensilos gesprochen wird. Um einen Ausgleich zwischen den Interessen aller Beteiligten (Einzelpersonen, Privatunternehmen, öffentlicher Verwaltung und Öffentlichkeit) zu schaffen, wurde dem Datenaustausch und der Gewährung von Datenzugangsrechten in der Rechtswissenschaft grosse Aufmerksamkeit geschenkt (Früh, 2018; Weber, 2019). Datenzugangsrechte sollen die gemeinsame Nutzung von Daten erleichtern und Datenökosysteme ermöglichen (Hofheinz & Osimo, 2017). Beispiele und Vorschläge für Datenzugriffsrechte beschränken sich stets auf einen engen Bereich (für das Kartellrecht etwa Drexl, 2017) und allgemeinere Regeln, wann der Zugang per Gesetz gewährt werden muss, sind noch rar (Früh, 2018).

Die Forschung an der Schnittstelle zwischen Recht und Technik hat sich in den letzten Jahren unter dem Stichwort Personal Information Management Systems (PIMS) mit Systemarchitekturen beschäftigt, die die informationelle Selbstbestimmung von betroffenen Personen stärken sollen, über die Daten bearbeitet werden (European Data Protection Supervisor, 2016). Allerdings reicht es nicht aus, diese Systeme zu haben. Diese sind auf einen rechtlichen Rahmen angewiesen, um zu funktionieren (Weber et al., 2017). Wie ein solcher entsprechender Rahmen für die Anwendung von PIMS in der Mobilität auszusehen hätte, ist noch unklar. Insgesamt gibt es – im Gegensatz zu anderen Bereichen wie z. B. dem Gesundheitswesen (Contreras, 2019; Evans, 2011) – kaum Forschung darüber, wie Ausschliesslichkeitsrechte an Daten und Governance-Grundsätze auf Mobilitätsdaten in einem bestimmten Land angewendet werden können.

Immer mehr Datenmärkte gehen die Herausforderungen des Datenschutzes mit kryptografischen Mitteln an, die eine Vielzahl unterschiedlicher Datenschutzgarantien bieten. Medicalchain (Medicalchain, 2018) und die MIDATA-Kooperative (MIDATA, 2021) erleichtern neben vielen anderen den Austausch medizinischer Daten, die Ende-zu-Ende gesichert sind. Agora (Koutsos et al., 2021) geht noch einen Schritt weiter und bietet einen Datenmarktplatz für datenschutzsensitive Daten, der auf funktionaler Verschlüsselung (FE) basiert. Boneh et al. (2012) propagieren ein Marktmodell, wo Datenkonsumenten Auswertungen bestimmter Funktionen auf Nutzerdaten kaufen können. Dabei werden nur die

Ergebnisse der Auswertung ausgetauscht, ohne dass die ursprünglichen Datensätze übertragen werden müssen. Neben der spezifischen FE-basierten Architektur bieten Koutsos et al. (2021) auch ein Sicherheitsmodell für die Vertraulichkeit der verarbeiteten Daten und berücksichtigen Zahlungen in ihrer Analyse. Das Sicherheitsmodell berücksichtigt jedoch nicht die Vertraulichkeit der Daten gegenüber dem Broker. In ähnlicher Weise bietet MyHealth-MyData FE-basierte Analysen mit dem Schwerpunkt auf medizinischen Daten, wobei die Vertraulichkeit der Daten im gesamten System gewährleistet ist (Morley-Fletcher, 2017). Enveil ist eine Plattform für ausgelagerte Datenverarbeitung unter Verwendung vollständig homomorpher Verschlüsselung (FHE), bietet aber auch Möglichkeiten für Verbraucher, einige analytische Funktionen mit den Daten durchzuführen (Enveil, 2021). Wibson bietet einen auf intelligenten Verträgen basierenden Marktplatz, der sich auf verschiedene Datenschutzaspekte konzentriert, insbesondere auf den Schutz der Identität von Verkäufern und Käufern (Fernandez et al., 2020)[4].

Das H2020-Projekt des KRAKEN-Konsortiums (KRAKEN, 2020), bei dem das AIT Partner ist, entwickelt einen Datenmarkt für datenschutzsensible Daten. Um dies zu erreichen, zielt das Projekt darauf ab, "den Austausch, die Vermittlung und den Handel von potenziell sensiblen persönlichen Daten zu ermöglichen, indem die Kontrolle über diese Daten während des gesamten Lebenszyklus der Daten an die Bürger (Datenanbieter) zurückgegeben wird". KRAKEN stützt sich hauptsächlich auf drei Säulen: (i) einem Datenmarktplatz, (ii) einer selbstsouveränen Identität (SSI) (Der et al., 2017) und (iii) einer Toolbox mit kryptografischen Primitiven für datenschutzfreundliche Berechnungen. Der Marktplatz fungiert als Vermittler zwischen Datenanbietern und Datenkonsumenten. SSI wird verwendet, um die Authentifizierung, Autorisierung und z.B. die Schlüsselverwaltung zwischen Datenkonsumenten und -produzenten zu verwalten. Um datenschutzfreundliche Analysen zu ermöglichen, werden datenschutzfreundliche kryptografische Protokolle und Primitive, einschliesslich sicherer Mehrparteienberechnungen (Multi Party Computation), verwendet.

Die Entwicklung von Datenmärkten, die den Schutz der Privatsphäre garantieren wie z.B. Bitsaboutme[5], ist ein laufender Prozess und noch nicht zufriedenstellend gelöst. Insbesondere bleibt die Erforschung der erforderlichen Algorithmen und Protokolle für eine Plattform für intelligente Mobilität notwendig.

Bei Strassenfahrzeugen, die sich untereinander und mit der Infrastruktur vernetzen, spielt die Data Governance ebenfalls eine grosse Rolle. Diese Fahrzeuge tauschen über die Vernetzung untereinander Daten aus, um den Komfort oder in kritischen Situationen die Sicherheit zu erhöhen. Über die Vernetzung finden over-the-air Softwareupdates statt, um z.B. das Fahrverhalten des Fahrzeugs oder die in-Vehicle-Infotainment-Umgebung zu beeinflussen. Damit dabei die Sicherheit stets gewährleistet werden kann, sind Standardisierungen zur Governance des ITS Datenmanagements in den Bereichen Sicherheit, Architektur, Kommunikationsprotokolle, Anwendungen und Policy zur Entscheidungsfindung aktuell in der Entstehung (ISO 5616).

1.4 Europäische Dateninfrastrukturen

Neue Mobilitätsdienste stützen sich auf die Verfügbarkeit von und den einfachen Zugriff auf Mobilitäts- und Verkehrsdaten. Sowohl die Nutzer des öffentlichen und des Individualverkehrs als auch die Mobilitätsdienstleister benötigen Daten über die Verkehrsnetze, die Zugänge, Tarife, die Reisezeiten oder die Verkehrssituation. Die Durchgängigkeit von Informationsdiensten zwischen Verkehrsträgern, aber auch zwischen Regionen und Ländern, wird beeinträchtigt, wenn Daten nicht frei verfügbar sind oder wenn sie in nicht austauschbaren, proprietären Formaten vorliegen. Die Wirkungen können dabei sichtbar und unerwünscht ausfallen. Ein Land mit abweichenden Regelungen kann entweder gemieden werden oder umgekehrt Verkehr anziehen (wie bei unterschiedlichen Strassengebühren).

Die Europäische Union adressiert diese Problemstellung mit einer Rahmenrichtlinie, der "ITS-Richtlinie" sowie untergeordneten delegierten Verordnungen, die detailliertere

[4] Eine Übersicht über weitere Datenmärkte findet sich unter: https://about.datarade.ai/data-marketplaces
[5] Siehe: https://bitsabout.me/de/

Anforderungen enthalten. Die Verordnungen enthalten Bestimmungen bezüglich der EU-weiten Bereitstellung von[6]:

- Echtzeit-Verkehrsinformationsdiensten
- unentgeltlichen Verkehrsmeldungen mit Relevanz für die Verkehrssicherheit,
- multimodalen Reise-Informationsdiensten und
- Informations- und Reservierungsdiensten für sichere Parkplätze für Lastwagen.

Diese Verordnungen befassen sich mit der Bereitstellung verschiedener Informationsdienste für den Strassenverkehr und für die Mobilität. Die europäische ITS-Gesetzgebung verpflichtet die Mitgliedstaaten im Wesentlichen dazu, sicherzustellen, dass alle nationalen Akteure, wie öffentliche und private Infrastrukturbetreiber, Verkehrsdienstleister oder Kartenhersteller, die folgenden Anforderungen erfüllen:

- Bei der Bereitstellung von ITS-Diensten müssen die geltenden Standards verwendet werden.
- Jeder Mitgliedstaat muss einen "Nationalen Zugangspunkt" einrichten (National Access Point, NAP[7]). Dieser Zugangspunkt soll als singuläre Anlaufstelle dienen, über die private oder gewerbliche Nutzer auf Strassen-, Verkehrs- und Mobilitätsdaten des jeweiligen Mitgliedstaates zugreifen können.
- Jeder Mitgliedstaat muss in seinem Hoheitsgebiet sicherstellen, dass alle relevanten Akteure die Daten innerhalb der EU diskriminierungsfrei zur Verfügung stellen.
- Jeder Mitgliedstaat muss überprüfen, ob die nationalen Akteure die Bestimmungen der Verordnungen einhalten. Für jeden Rechtsakt muss der Europäischen Kommission periodisch ein Bericht über die Aktivitäten und Fortschritte bei der Umsetzung vorgelegt werden.

Es sei darauf hingewiesen, dass die europäische ITS-Gesetzgebung keine Verpflichtung für die Mitgliedstaaten vorsieht, irgendwelche physische Infrastruktur zu errichten[8]. Hauptziel der Gesetzgebung ist es, schon vorhandene Daten in einer harmonisierten, standardisierten, freien und nichtdiskriminierenden Weise zugänglich zu machen.

Die grundsätzliche Idee der europäischen ITS-Gesetzgebung lässt sich in zwei Hauptaspekte zusammenfassen, nämlich:

1) **Daten auf offenen Plattformen** verfügbar zu machen, und

2) die einschlägigen **Normen anzuwenden** sowie proprietäre Lösungen zu vermeiden.

In **Deutschland** übernimmt der **Mobilitätsdatenmarktplatz** (MDM) die Rolle des NAP, um die Zugänglichkeit, den Austausch und die Aktualisierung von standardisierten Reise- und Verkehrsdaten zu ermöglichen (BMVI, 2019).

Der MDM funktioniert anhand von zwei Ebenen. Die erste Ebene beinhaltet über eine Portalfunktion das Metadatenverzeichnis, das in der Form einer interaktiven Webseite angeboten wird. Damit werden das Anbieten, Recherchieren, Beziehen und Abonnieren von Daten, die auf dem MDM verfügbar sind, ermöglicht. Die zweite Ebene in der Form einer Broker-Funktion übernimmt die Rolle des Datenverteilers. Diese Funktion stellt sicher, dass der Online-Datenfluss vom Datenanbieter über den MDM zum Datenabnehmer geregelt abläuft.

Die Aufgaben, die der MDM erfüllt, beinhalten:

- Die Erstellung eines zentralen Portals mit strukturierten Informationen über verfügbare Verkehrsdaten einzelner Organisationen;
- die Funktionen zum Anbieten, Suchen und Abonnieren von verkehrsrelevanten Daten;

[6] Aus (Engdahl & Oehry, 2020).
[7] Die Schweiz ist diesbezüglich keine Verpflichtungen eingegangen, richtet jedoch analog einen NAP über die Verkehrsdatenplattform (VDP) des ASTRA ein.
[8] Mit Ausnahme des e-Call Notrufdienstes, der zwar ebenfalls in der ITS-Richtlinie als verpflichtende Einrichtung definiert wird, aber nicht mit den nationalen Datenzugängen in Zusammenhang steht.

- die Abwicklung des Datenaustauschs zwischen den Partnern über standardisierte Schnittstellen und Kommunikationsverfahren;
- die Vereinfachung der Geschäftsprozesse für alle Beteiligten, insbesondere Verringerung der technischen und organisatorischen Aufwände der Datenanbieter und Datenabnehmer und damit Erschliessung der Potentiale vorhandener Datenquellen (Rittershaus, 2021).

Um den künftigen Herausforderungen wie dem Zugang zu sensiblen Daten, dem direkten Zugriff von Endgeräten, den Massendaten in Echtzeit und dem Cloud Computing gerecht zu werden, wird die MDM mit dem **Mobility Data Space** ergänzt und in die neue Plattform mobilithek integriert (Rittershaus, 2021). Dies soll erlauben, den Interessen der Privatwirtschaft gerecht zu werden und deren Daten, unter Berücksichtigung ihrer Interessen, an die Dateninfrastruktur anzubinden.

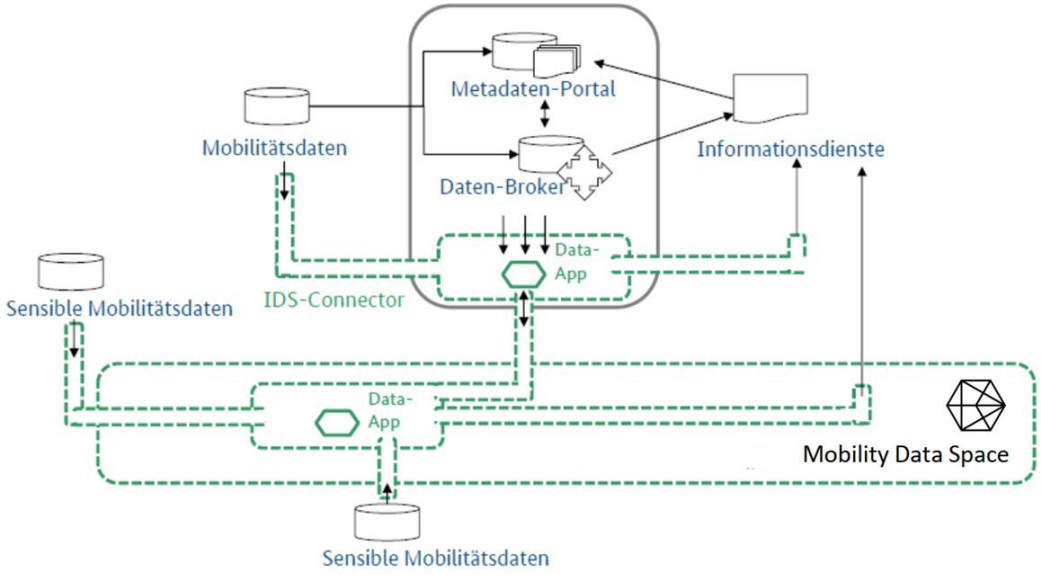


Abb. 4 *Systemarchitektur zur Einbindung des Mobilitity Data Space, des Metadaten-Portals und des Daten-Brokers in die künftige mobilithek.*
Quelle: (Rittershaus, 2021)

Für die Umsetzung der mobilithek ist es notwendig, das Mobilitätsökosystem anhand eines Mobilitätsdatenraums (Shared Digital Twin), der die einzelnen Services des Ökosystems als Datenobjekte integriert, abzubilden. Um die Daten nicht physisch einzubinden, basiert der Datenraum auf einer verteilten Datenhaltungsarchitektur ohne gemeinsames Datenbankschema. Die Daten werden über das Linked-Data Konzept anhand von eindeutigen Identifikatoren miteinander vernetzt. Die open-source verfügbare IDS-Software-Infrastruktur[9] bietet dazu eine informationstechnische Basis für Datenräume. Wie diese drei Komponenten zusammenhängen ist in *Abb.* 5 ersichtlich und wurde in der Grundlagenarbeit von Otto & Burmann (2021) entwickelt.

[9]Verfügbar unter: https://github.com/International-Data-Spaces-Association

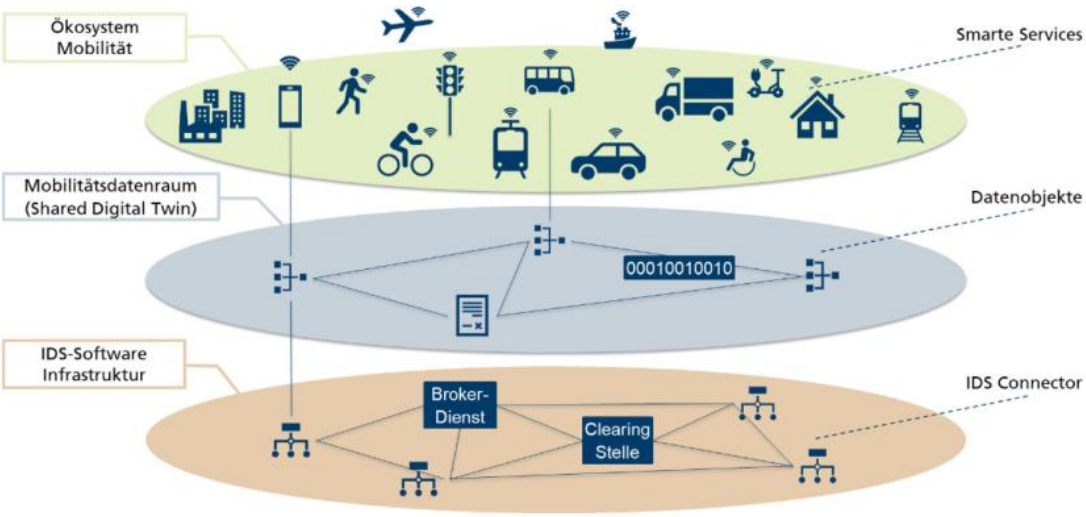


Abb. 5 *Integrationsarchitektur zu Dateninfrastrukturen, Datenräumen und Datenökosystemen für die Mobilität*
Quelle: (Otto & Burmann, 2021)

Zur Umsetzung eines intermodalen Mobilitätsdatenraums, der die europäischen Werte wie Datenschutz und Datensouveränität berücksichtigt, besteht noch Handlungs- und Forschungsbedarf. Noch ist bspw. unklar wie die Abbildung der verschiedenen Interessen der Stakeholder anhand von Governance-Modellen berücksichtigt und technologisch umgesetzt werden kann. Die Grundlagen dazu, z.B. die Instrumente der Hierarchie, Prozessdefinition und API-Vorgaben, wie sie aus unternehmensinternen Anwendungen bekannt sind, stehen noch nicht zur Verfügung (Otto & Burmann, 2021).

Aktuell sind viele weitere Initiativen mit europäischen Dateninfrastrukturen mit Bezug zur Mobilität befasst (Gaia X, 2022; IDS, 2022; Nordic Innovation, 2022).

1.5 Schweizer Dateninfrastrukturen

Für die Schweiz ist eine direkte Übernahme der EU-Bestimmungen nicht vorgesehen. Mit der fortschreitenden Digitalisierung soll die Mobilität zunehmend intermodaler, durchgängiger und internationaler werden. Die bisherige Strassenmobilität war mit wenigen Grenzen versehen, da es nur ein paar wenige physische Parameter (Gewicht, Ausmasse Fahrzeuge) zu regulieren gab. Es gilt die Gefahr zu minimieren, mit der Digitalisierung Grenzen der Mobilität zu schaffen, die es vorher nicht gab. Unter diesem Gesichtspunkt ist es eine Anforderung, den schweizerischen Ansatz mit den Nachbarländern und somit mit der EU zu harmonisieren (Engdahl & Oehry, 2020). Im autonomen Nachvollzug der EU-Bestimmungen plant die Schweiz ebenfalls einen Nationalen Zugangspunkt (NAP) einzurichten. Damit kann Kompatibilität mit den Dateninfrastrukturen der umliegenden europäischen Ländern gewährleistet werden und gleichzeitig eine Dateninfrastruktur im Bereich Mobilität geschaffen werden, die den schweizerischen Bedürfnissen entspricht (BAV, 2021a).

Den Bedarf nach offenen Plattformen auf nationaler Ebene hat die Schweiz erkannt. Mehrere Datenaustauschplattformen befinden sich in konzeptioneller Entwicklung, in funktionalen Pilotbetrieben beziehungsweise sind bereits umgesetzt.

Mit der **NOVA**-Plattform, die seit 2016 operativ ist, hat die SBB im Mandat der Branche ein zentrales Preis- und Vertriebs-Basissystem für den öffentlichen Verkehr der Schweiz umgesetzt. Sie enthält neben den Tarifdaten die zentralen Kundendaten, die Verkehrsdienstleistungen der öV-Unternehmen, die Netztopologie sowie Funktionen zur Kontrolle der Fahrausweise und Abrechnung der Einnahmen. Die Transportunternehmen haben ihre Vertriebskanäle an die NOVA-Schnittstelle angeschlossen und es können durchgängige Fahrausweise für den öV erstellt werden. Die NOVA-Plattform ist jedoch ein geschlossenes System, das nur für die konzessionierten Verkehrsunternehmen zugänglich ist (ITS CH, 2021).

Die SBB ist vom BAV mit den **Systemaufgaben der Kundeninformation** (SKI) beauftragt. Die SKI sammelt, konsolidiert und publiziert Fahrgastinformationsdaten des öffentlichen Verkehrs der Schweiz. Gemäss Art. 13 Abs. 3 PBG i.V.m. Art. 10 Abs. 2 Fahrplanverordnung unterstehen alle konzessionierten Transportunternehmen der Fahrplanpublikationspflicht. Das Gesamtsystem beinhaltet neben dem Stammdatensystem der Dienststellendokumentation (DiDok) die Fahrpläne und Echtzeitdaten über die Betriebslage. Über die Open-Data-Plattform **Mobilität Schweiz**[10] können Mobilitätsdaten eingesehen und bezogen werden. Zusätzlich stehen weitere Dienste wie z.B. der Open Journey Planner zur Verfügung.

Ergänzend zu den Daten im öffentlichen Verkehr wird die **Verkehrsdatenplattform** (VDP) aufgebaut und in die Open-Data-Plattform Mobilität Schweiz integriert. Unter der Federführung des ASTRA laufen Bestrebungen, Daten des individuellen Strassenverkehrs einzubinden. Dazu gehören neben den Daten, die durch Zählstellen, Verkehrsüberwachungskameras und Sensoren auf den Nationalstrassen generiert werden, auch Daten, die auf dem untergeordneten Strassennetz anfallen. In freiwilliger Kooperation mit Kantonen und Gemeinden sollen sämtliche für den Strassenverkehr relevanten dynamischen Echtzeit-Verkehrsdaten zentral zugänglich gemacht und deren Austausch und Bereitstellung gefördert werden. Der Zugang zur Plattform basiert auf dem Prinzip des gegenseitigen Informationsaustauschs (sog. " Mutual Data Sharing"). Die Verkehrsdatenplattform wird im Rahmen eines Pilotprojekts seit April 2020 schrittweise ausgebaut.

Als weitere öffentliche Dateninfrastruktur soll das **Verkehrsnetz CH** (VnCH) das gesamte nationale Verkehrssystem der Verkehrsträger Strasse, Schiene, Seil und Wasser digital abbilden und in einem Bezugsrahmen örtlich referenzieren. Über standardisierte Prozesse sollen die Änderungen an der physischen Infrastruktur auch in der digitalen Abbildung mit hohen Qualitätsstandards sichergestellt werden. Die Daten sowie deren Bereitstellung sollen frei von kommerziellen Interessen sein, diskriminierungsfrei zugänglich sowie für alle Nutzenden einfach und in einem einheitlichen Format abrufbar sein. Im Rahmen der Förderung der vernetzten Mobilität durch den Bund ist unter der Leitung von swisstopo ein Realisierungskonzept erstellt und die Machbarkeit im Jahr 2021 geprüft worden. Bis zur operativen Umsetzung wird ein Pilotbetrieb aufgebaut und betrieben. Ein digital vernetztes, örtlich referenziertes Abbild der Strasseninfrastruktur ist unter anderem eine Grundvoraussetzung für automatisiertes Fahren.

Der Bundesrat beauftragte das UVEK im Juli 2020, eine "**Nationale Datenvernetzungsinfrastruktur Mobilität**" (NADIM) für den Austausch von Mobilitätsdaten im Sinne eines Service Public aufzubauen und die entsprechenden gesetzlichen Grundlagen zu schaffen. NADIM soll unabhängig, verlässlich, offen, nichtdiskriminierend, transparent, nicht gewinnorientiert, von hoher Qualität und technisch flexibel ausgestaltet werden. (Engdahl & Oehry, 2020). Damit kann eine staatliche Daten- und Schnittstelleninfrastruktur bezüglich IT, Prozessen und Verträgen zur Förderung der Verfügbarkeit und des standardisierten Austauschs von Mobilitätsdaten sowie für die Vernetzung von Mobilitätsangeboten zwischen Mobilitätsanbietern und Mobilitätsvermittlern errichtet werden. Die Anforderungen an einen NAP gemäss Vorgaben der EU im Hinblick auf Vorgaben zu Datenumfang, Normen und Standards werden damit erfüllt (BAV, 2021a). Die Leitung des Projekts liegt beim BAV, in Zusammenarbeit mit weiteren Bundesämtern. NADIM befindet sich aktuell in konzeptioneller Entwicklung und soll die vorgängig erwähnten Plattformen mit einbinden.

Neben den erwähnten digitalen Infrastrukturen des Bundes sollen Daten aus öffentlichen und privaten Quellen integriert werden. NADIM ermöglicht den standardisierten Austausch von Mobilitätsdaten und damit die Vernetzung von öffentlicher Hand, Mobilitätsanbietern, Entwicklern und Betreibern von digitalen Kundenlösungen (z.B. Apps) sowie weiteren Akteuren wie Wissenschaft und Forschung. Um ihren Aufgaben gerecht zu werden, muss sie die unterschiedlichen Governance-Anforderungen der beteiligten privaten und öffentlichen Akteure berücksichtigen. Es ist nach dem Gesagten offensichtlich, dass eine neutrale Organisationsstruktur und entsprechende Governance-Modelle zentral für eine erfolgreiche Umsetzung dieser nationalen digitalen Infrastruktur sind. Die Systemübersicht der NADIM ist in Abb. 6. dargestellt.

[10] Verfügbar unter: https://opentransportdata.swiss/de/.

Abb. 6 Systemübersicht NADIM.
Quelle: (BAV, 2021b)

Für den Aufbau einer umfassenden digitalen Infrastruktur als Service Public ist eine Gesetzesgrundlage notwendig. Dazu wird im Auftrag des Bundesrates von der Bundesverwaltung das Bundesgesetz über die Mobilitätsdateninfrastruktur (MODIG) ausgearbeitet, um zukünftige Anwendungen in den Bereichen des Verkehrsmanagements, der Logistik, oder des automatisierten Fahrens a priori zu regeln. Die neue Dateninfrastruktur besteht aus zwei Hauptelementen: NADIM und Verkehrsnetz CH (VnCH). Das VnCH ist eine einheitliche, digitale Abbildung des gesamten Verkehrssystems der Schweiz. Hier sollen alle Daten zu den Verkehrsnetzen und der zugehörigen Infrastrukturen der öffentlichen Hand zentral durch den Bund synchronisiert, erweitert und optimiert werden. Damit bildet es das zentrale räumliche Referenzsystem für die Verknüpfung von Mobilitätsdaten über die NADIM. Das Gesetz regelt den Aufbau und Betrieb der NADIM und des VnCH. Weiter bildet es die Grundlage zur Errichtung und Organisation der Mobilitätsdatenanstalt (MDA) des Bundes, die für den Betrieb und Aufbau der NADIM zuständig sein wird. Damit wird der Grundstein für ein digital vernetztes, effizientes und europäisch interoperables Mobilitätssystem der Schweiz gelegt.

1.6 Industrielle Dateninfrastrukturen

Neben Mobilitätsdienstleistern und MaaS-Anbietern hat auch die Fahrzeugindustrie den Mehrwert von Kommunikationsdienstleistungen um das Fahrzeug erkannt. Dabei wurde das Konzept des **Extended Vehicle** (ISO 20077; ISO 20078) entwickelt (siehe Abb. 7).

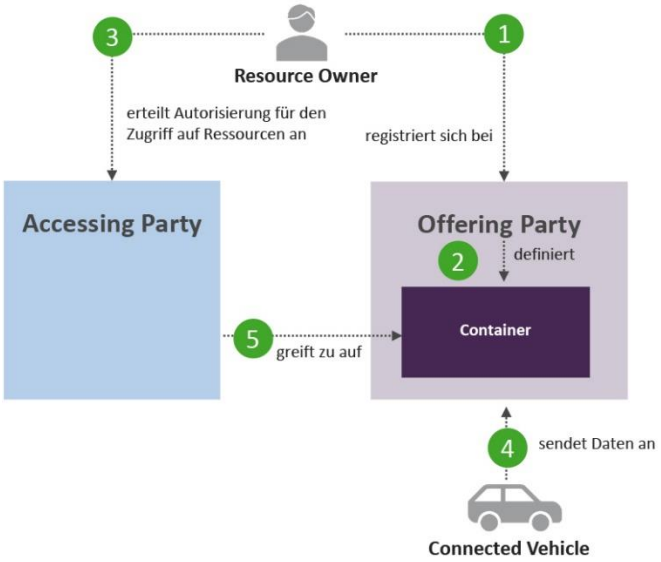


***Abb. 7** Extended Vehicle Konzept (ISO 20077; ISO 20078)*

Ziel ist es, hier eine Schnittstelle anzubieten, um auf Daten und Funktionen eines Fahrzeuges zuzugreifen. Derzeit wird ein solcher Zugriff oft über sogenannte OBD-II Dongles implementiert (Christensen & Dannberg, 2019). Dabei wird ein nach aussen sendendes Element an die in jedem Fahrzeug zu Diagnosezwecken vorhandene OBD-II Schnittstelle angeschlossen. Herausforderungen entstehen durch die Konzipierung von OBD-II als Diagnoseschnittstelle: Die verfügbaren Daten und Funktionen sind beschränkt, die OBD-II Schnittstelle ist nicht dafür ausgelegt, dauerhaft und während der Fahrt benutzt zu werden, und zeitgleich kann jeweils nur ein Nutzer kann auf die Schnittstelle zugreifen.

Aufgrund dieser Limitierungen wurde hier über ein neues Konzept nachgedacht (siehe ***Abb. 8***)

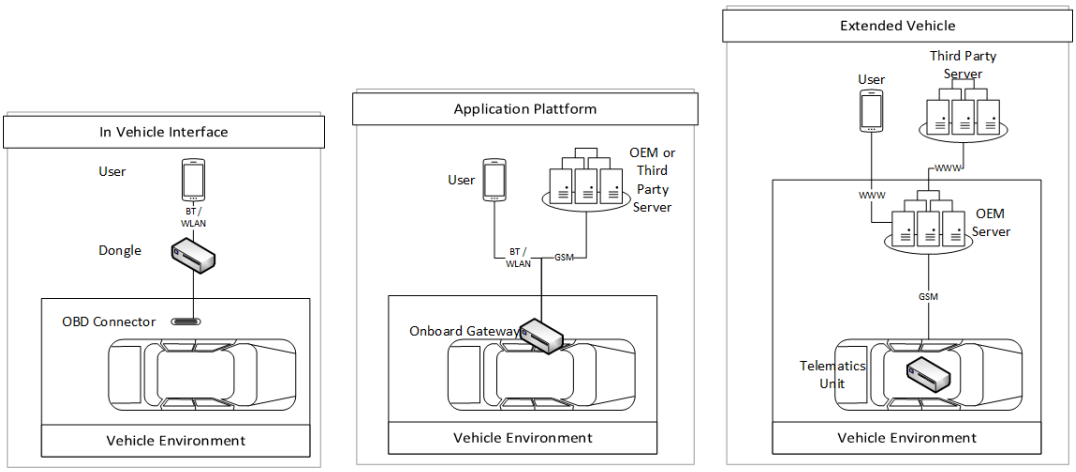


Abb. 8 *Vernetzung des Fahrzeuges - mögliche technische Lösungen (ISO 20077; ISO 20078)*

Startpunkt war der Zugriff über den OBD-II Dongle. Darauf aufbauend wurde ein Zugang über ein spezifisches Gateway angedacht, auf das Fahrzeugnutzer und Fahrzeughersteller direkt Zugriff haben. Herausforderung ist die Implementierung einer nach aussen geöffneter Schnittstelle auf das Fahrzeugsystem. Um hier hohe Zugriffssicherheit zu gewährleisten, wurde dann das in Abb. 9 dargestellte Konzept entwickelt. Das Fahrzeug kommuniziert hierbei nur mit einer einzigen externen Infrastruktur und alle weiteren Zugriffe erfolgen nur auf die Infrastruktur, ohne direkte Zugriffe auf das Fahrzeug. Die Schnittstellen nach aussen sollen ein standardisiertes Format anbieten und neutral für alle Dienstleistungen verfügbar sein. Die Kontrolle über den Zugriff, also Freigabe, soll durch den Fahrzeugbesitzer erfolgen.

Im Extended Vehicle Concept wird diese neu definierte Schnittstelle genutzt und die Daten werden für externen Services zur Verfügung gestellt. Was die Ausgestaltung der Infrastruktur betrifft, bestehen die Alternativen im Betrieb einer Infrastruktur durch den Fahrzeughersteller oder im Betrieb durch eine dritte, neutrale Organisation. Aus kartellrechtlichen Bedenken wird inzwischen die dritte, neutrale Organisation allgemein bevorzugt. Derzeit wird angedacht, dass ein grundlegender Satz von Daten und Services von aussen her zugänglich ist und ein beschränkter Satz von Daten und Services nur für den Fahrzeughersteller zugänglich ist (Kerber, 2018).

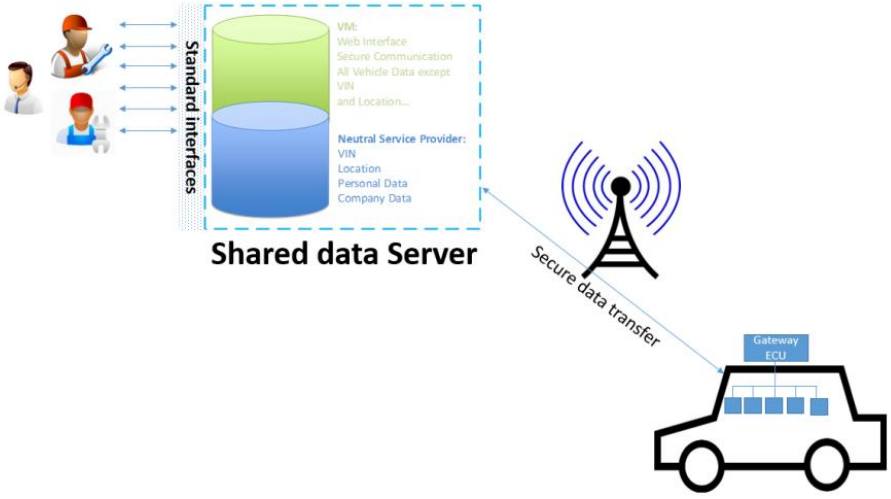


Abb. 9 *Shared data Server (Reich et al., 2018)*

2 Systematisierung der Mobilitätsangebote, Akteure und Datenflüsse

2.1 Generische Smart Mobility-Anwendungen

Mit der zunehmenden Digitalisierung in vielen Lebensbereichen und dem Wachstum von Anwendungen des Internet of Things (IoT) werden physische und virtuelle Objekte immer umfangreicher miteinander vernetzt. Diese Vernetzung findet auch in der Mobilität statt.

Zu den physischen Objekten der Mobilität gehören insbesondere sämtliche Fortbewegungsmittel. Seit 2018 werden nur noch Fahrzeuge zugelassen, die über ein eCall-System verfügen. Damit haben die Technologien GSM (Global System for Mobile Communications) und GNSS (Global Navigation Satellite System), die für die Vernetzung und Positionierung notwendig sind, Einzug in die Fahrzeuge gefunden. Auch bei anderen Fortbewegungsmitteln, wie z.B. E-Bikes, werden diese Technologien zunehmend öfters eingesetzt. Dies erlaubt es den Nutzern oder Diensteanbietern, die Fortbewegungsmittel aus der Ferne zu sperren, zu lokalisieren sowie die Software zu aktualisieren. Neben den Fortbewegungsmitteln werden auch die damit verbundenen Mobilitätsdienstleistungen immer digitaler, vernetzter und intelligenter.

Im Projekt soll ein Werkzeugkasten entwickelt werden, um Governancefragen digitaler Mobilitätsangebote zu adressieren. Um angesichts der Vielfalt und Marktdynamik bei neuen Mobilitätsangeboten möglichst allgemeingültige Aussagen zu Governancefragen machen zu können, haben wir als ersten Schritt in einem methodischen Vorgehen generische Elemente herausgearbeitet.

Im Rahmen des Projekts wurde deshalb eine Systematik entwickelt, um den Mobilitätsangeboten einzelne Smart Mobility-Anwendungen zuzuordnen und die resultierenden Datenflüsse zwischen den Akteuren zu identifizieren. Die Systematik gliedert sich in drei Ebenen. Die ersten zwei Ebenen (Level 1 und 2), "Mobilitätsangebote" und "Smart Mobility-Anwendungen", werden in diesem Kapitel eingeführt. Um den bei Smart Mobility-Anwendungen involvierten Akteuren generische Rollen zuzuordnen, wird in Kapitel 2.2 das dazu verwendete Rollenmodell eingeführt. Die Inhalte der dritten Ebene (Level 3), "Datentypen, Datenflüsse und die involvierten Akteure", werden mittels einer Prozessanalyse identifiziert und in Kapitel 2.3 erläutert.

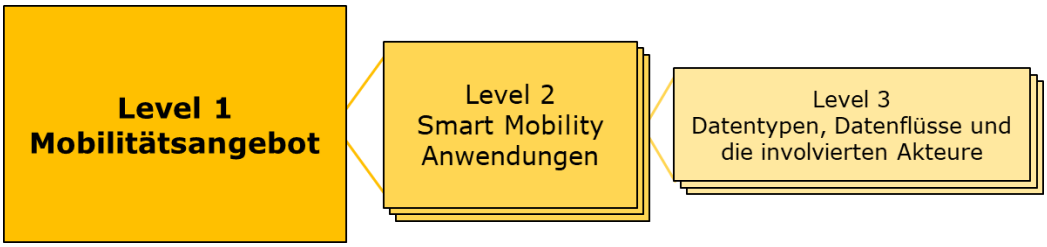


***Abb. 10**: Die drei Ebenen zur Identifikation von generischen Datenflüssen bei Smart Mobility-Anwendungen.*

Um diese Zuteilungen vorzunehmen und die relevanten Mobilitätsangebote und Anwendungen zu detektieren, wurde die hierzu einschlägige Literatur analysiert.

Im Forschungsbericht *Verkehr der Zukunft 2060: Neue Angebotsformen – Organisation und Diffusion* (ASTRA, 2020) werden zukunftsträchtige Angebotsformen in generische Angebotstypen eingeteilt und den dazugehörigen Geschäftsmodellen zugeordnet, wie in *Abb. 11* dargestellt.

So lassen sich dem Mobilitätsangebot "Individuelle Fahrzeugnutzung" beispielsweise die Anwendungen "privates vernetztes Fahrzeug" sowie "Riding (On Demand)" und "Sharing (On Demand)" zuordnen. Durch die zukünftige Automatisierung des Fahrens kann davon ausgegangen werden, dass die Angebotstypen Sharing und Riding zunehmend miteinander verschmelzen werden (ASTRA, 2019). Dem Mobilitätsangebot "kollektive

Fahrzeugnutzung" kann sowohl der öV in der klassischen Form wie auch On-Demand zugeordnet werden.

Plattformen übernehmen immer mehr die Vermittlung von Mobilitätsdienstleistungen samt deren Planung, Buchung, Bezahlung und der Informationsassistenz während der Reise. Diesem Angebot wird u.a. die Anwendung Mobility as a Service (MaaS) zugeordnet.

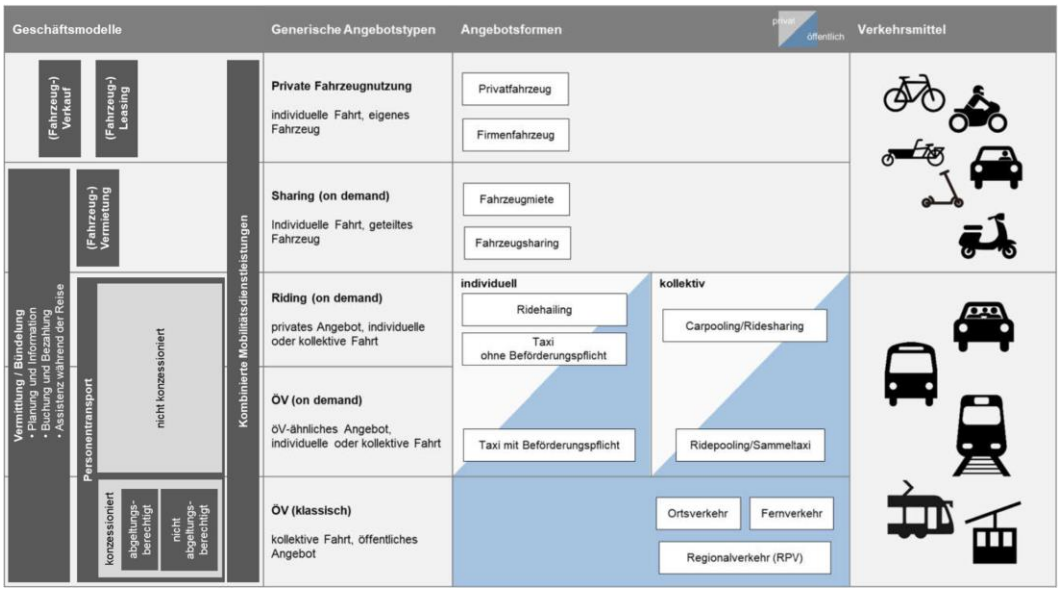


Abb. 11 *Begriffsstruktur Angebotsformen und Geschäftsmodelle,* Quelle: (ASTRA, 2020)

Die Analyse der grundlegenden Geschäftsprozesse entlang der gesamten Wertschöpfungskette der Angebote aus den Forschungsarbeiten (ASTRA, 2019, 2020) zeigt, dass neben dem Personentransport noch weitere Mobilitätsangebote und Anwendungen in der Praxis vorkommen. Diese lassen sich aus der Systematik der Norm *ITS service domains, groups und services* (ISO 14813-1, 2015) herleiten und ergänzen. Für ein funktionierendes Mobilitätsystem ist das Mobilitätsangebot "Verkehrsmanagement & Steuerung" genauso notwendig wie Versicherungsangebote und Notfalldienste.

Neben Personen werden auch Güter, abgebildet im Mobilitätsangebot Logistik, auf den Strassen transportiert. Damit Personen und Güter, die das Mobilitätssystem für den Transport in Anspruch nehmen, für die Benutzung entsprechenden bepreist werden können, braucht es noch das Mobilitätsangebot "Gebührenerhebung / Ticketing".

Für diese Forschungsarbeit wurden somit folgende **generische Mobilitätsangebote** identifiziert, die der Betrachtung zugrunde gelegt werden:

• individuelle Fahrzeugnutzung	• Notfalldienst
• kollektive Fahrzeugnutzung	• Verkehrsmanagement und Steuerung
• Plattformen (Vermittlung Mobilitätsangebote)	• Logistik
• Versicherungen	• Gebührenerhebung / Ticketing

Abb. 12 *Die acht generischen Mobilitätsangebote des Level 1*

Um sicherzustellen, dass die identifizierten generischen Mobilitätsangebote sämtliche Geschäftsbereiche abdecken, wurden ihnen Geschäftsmodelle von Smart Mobility-Anwendungen von etablierten Unternehmen, von derzeit entstehenden Start-ups sowie von Quellen aus der Literatur zugeordnet. In Abb. 13 ist diese Zuordnung dargestellt.

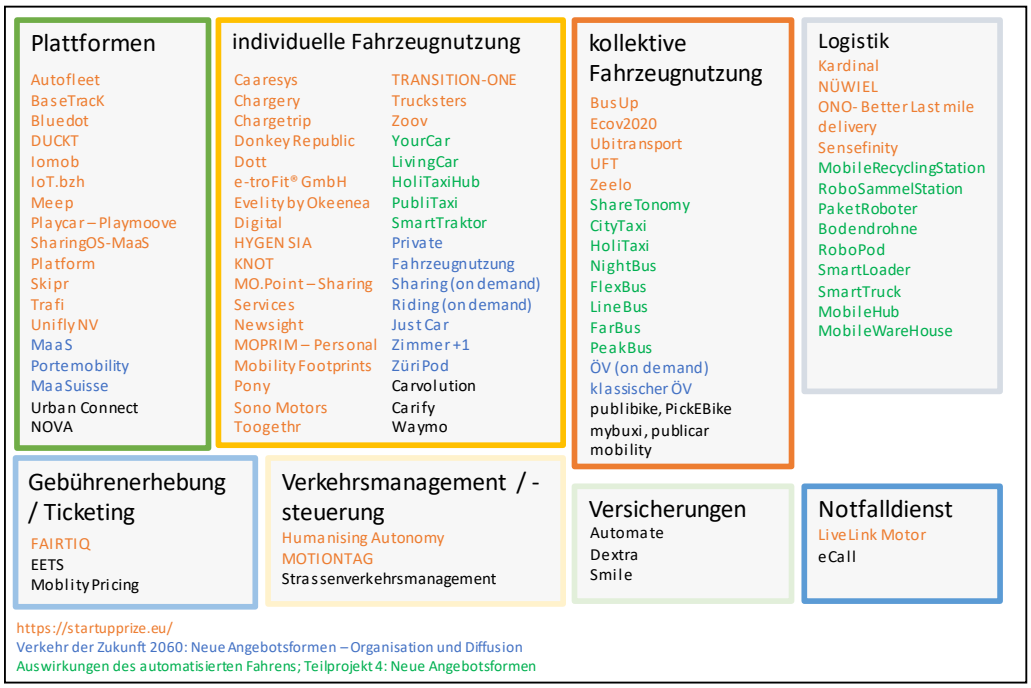


***Abb. 13** Zuteilung der verschiedenen Geschäftsmodelle von Smart Mobility-Anwendungen zu den acht generischen Mobilitätsangeboten. (Beispiele)*

Es ist gelungen, alle aufgefundenen Geschäftsmodelle den von uns identifizierten generischen Mobilitätsangeboten zuzuordnen[11]. Es ist somit zur Systematisierung unserer Arbeit möglich, von der Unzahl individueller Angebote zu abstrahieren und den Betrachtungen die acht generischen Mobilitätsangebote zugrunde zu legen.

Für die weitere Arbeit der Identifikation der relevanten Datentypen und Datenflüsse (Level 3), wird auf der Ebene der individuellen Angebote (Level 2) eine Liste typischer, beispielhafter und allgemeiner Mobilitätsdienstleistungen herangezogen. Dabei wurde darauf geachtet, dass alle relevanten Arten von Angeboten und Anwendung ohne übermässige Doppelungen und Überschneidungen erfasst sind. Diese sind in Abb. 14 dargestellt und werden zur Identifikation der Datenflüsse zwischen den beteiligten Akteuren verwendet.

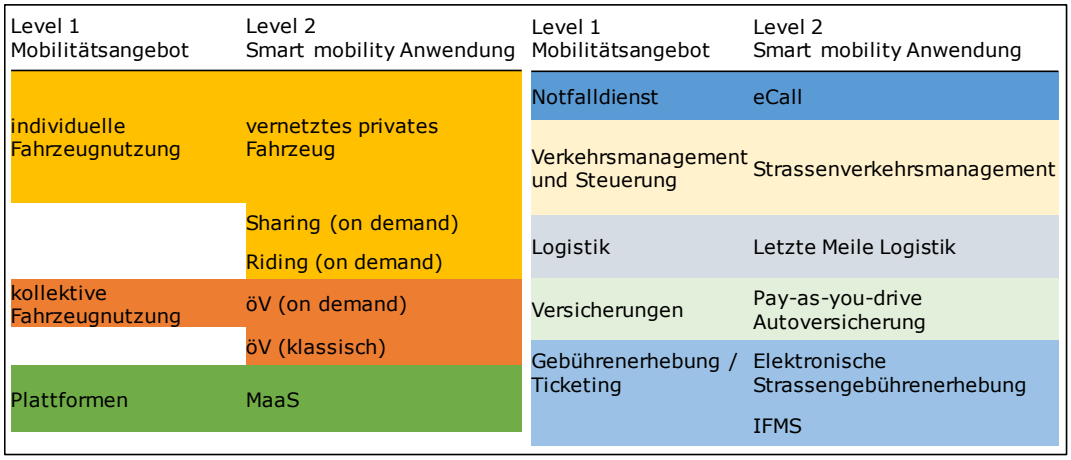


***Abb. 14** Zuordnung von Smart Mobility-Anwendungen zu den generischen Typen von Mobilitätsangeboten.*

[11] Es ist selbstverständlich möglich, dass es weitere Geschäftsmodelle gibt, die sich diesen acht Mobilitätsangeboten nicht zuordnen lassen. Im Hinblick auf die Zielsetzung von DAGSAM, ein möglichst generisches Governance-Modell zu entwickeln, wäre dies jedoch ein tragbarer Mangel.

2.2 Generisches Rollenmodell der beteiligten Akteure

Auch für die Datenflüsse zwischen den Akteuren, die jeweils bei den einzelnen Smart Mobility-Anwendungen als Datenlieferanten, Datenbezieher oder Datenverarbeiter agieren, müssen generische Elemente gefunden werden, damit wesentliche und zentrale Aspekte herausgearbeitet werden können.

Als generisches Modell für die in den Smart Mobility-Anwendungen beteiligten Akteure haben wir eines der ersten Modelle geprüft, das im Bereich der digitalen Mobilität zur Anwendung kam. Das Modell wurde in einem europäischen Forschungsprojekt entwickelt (B. Oehry et.al., 2002), um die Interoperabilität in der Europäischen Gebührenerhebung im Schwerverkehr zu fördern und von den jeweiligen nationalen Verhältnissen bezüglich der beteiligten Akteure (öffentliche Institutionen, private Firmen, Endkunden, etc.) zu abstrahieren.

Das Modell findet seit 2004 Anwendung beim EETS (European Electronic Tolling Service). Das Ziel von EETS ist die Erschaffung eines Systems, das den Nutzern des Systems ermöglicht, von einem zugelassenen Dienstanbieter (EETS-Provider) ein Mautgerät zu beziehen, welches mit allen konformen europäischen Gebührenerhebungssystemen kompatibel ist und es dem Nutzer erlaubt, mit nur einem Vertrag und nur einem Gerät Strassenverkehrsgebühren in ganz Europa elektronisch und automatisiert zu bezahlen. Das EETS-System basiert auf einer vom Europäischen Parlament und dem Rat der Europäischen Union erlassenen Richtlinie, in der vertragliche, prozedurale und technische Grundsätze für ein internationales Abkommen zur Schaffung eines europäischen elektronischen Mautdienstes beschrieben werden (EU, 2004, 2019).

Das EETS-Modell, Abb. 15, beinhaltet die generischen Rollen des EETS Dienstanbieters (englisch EETS Provider), des Gebührenerhebers (Toll Charger) und des Nutzers (User). Die Akteure in diesen drei Rollen stehen untereinander in vertraglicher Beziehung sowie im Leistungs- und Bezahlungsaustausch. Die übergeordneten Rahmenbedingungen werden von einer vierten Rolle, dem Regulator, z.B. über Gesetze und Verordnungen vorgegeben.

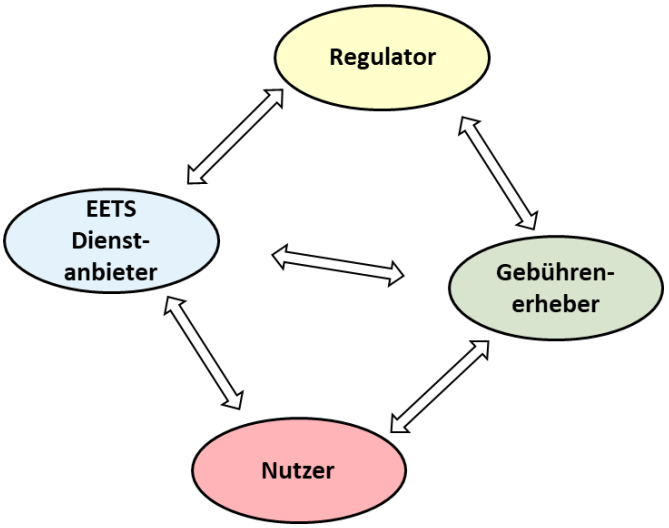


Abb. 15 *Rollenmodell des EETS*

Es stellt sich heraus, dass sich dieses einfache Modell auf alle untersuchten Smart Mobility-Anwendungen anwenden lässt, wenn die Bezeichnungen der Rollen der Akteure verallgemeinert werden.

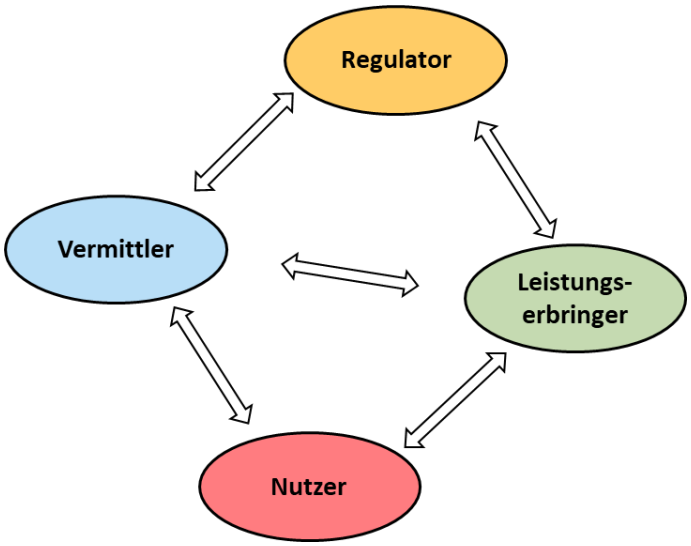


Abb. 16 *Generisches Rollenmodell von DAGSAM mit den generischen Akteuren Vermittler, Leistungserbringer, Nutzer und Regulator.*

Den Akteuren fallen im Rollenmodell dabei die folgenden Aufgaben zu:

- **Leistungserbringer**: Anbieter der zugrundeliegenden einzelnen Dienstleistung (Transport von Gütern oder Personen, Versicherung, Gebührenerhebung, Bereitstellung und Unterhalt der Infrastruktur etc.), die er gegenüber dem Nutzer erbringt.
- **Vermittler**: Hat die primäre vertragliche Beziehung zum Nutzer. Er führt Angebot und Nachfrage zusammen, bündelt Angebote und bietet so dem Nutzer Mobilitätsprodukte an. Der Vermittler bucht und vergütet die Leistung beim Leistungserbringer. Der Nutzer bezahlt die bezogenen Leistungen beim Vermittler, der seinerseits die entsprechenden Leistungserbringer vergütet.
- **Nutzer**: Die Konsumentin oder der Konsument von mobilitätsbezogenen Dienstleistungen.
- **Regulator**: Instanz, die die allgemeinen Rahmenbedingungen festlegt, sei es mittels verbindlicher Normen, Branchenübereinkünften, best-practice guidelines, o.ä. Eine weitere Aufgabe des Regulators ist die Durchsetzung dieser Rahmenbedingungen und das Anordnen von Massnahmen, sollten diese verletzt werden.

Es ist zu betonen, dass die Rollen im von DAGSAM entwickelten generischen Modell durchaus von mehreren realen Akteuren gemeinsam ausgefüllt werden können. So finden sich – um beim Beispiel der Gebührenerhebung zu bleiben – in der Rolle des Leistungserbringers der Eigner und Betreiber der Strasseninfrastruktur, der Gläubiger der Gebühr und die Kontrollorgane. Ebenso kann ein Akteur mehr als eine Rolle einnehmen, dies ist insbesondere der Fall, wenn Angebote nicht gebündelt werden, sondern direkt beim Leistungserbringer bezogen werden (zum Beispiel die Buchung eines Tickets direkt beim Bahnunternehmen).

2.3 Generische Prozesse zur Identifikation von Datenflüssen

Um die Datenflüsse bei Smart Mobility-Anwendungen zu identifizieren und sie generischen Datentypen zuzuordnen, wurden für die in Abb. 14 aufgezeigten Anwendungen systematisch die involvierten Prozesse analysiert.

Die Identifikation der einzelnen Prozesse stützte sich dabei einerseits auf den ITS Standard (ISO 14813-1, 2015), sowie die Datenschutzerklärungen und die allgemeinen Geschäftsbedingungen einzelner Anwendungen. Für diese Prozesse sind die bei jedem Prozessschritt anfallenden Datenflüsse zwischen den Akteuren identifiziert worden. In einem iterativen Verfahren sind die Datenflüsse dann generischen Datentypen zugeordnet und die Prozesse mit diesen Datentypen erneut durchgespielt worden.

Für jeden Prozessschritt wurde der Event, der Prozess, der ausgetauschte generische Datentyp, die Datenaustauschfrequenz und die am Prozess beteiligten Akteure benannt. In

der folgenden Darstellung werden die Instrumente und Auswahlmöglichkeiten zur Prozessbeschreibung aufgeführt.

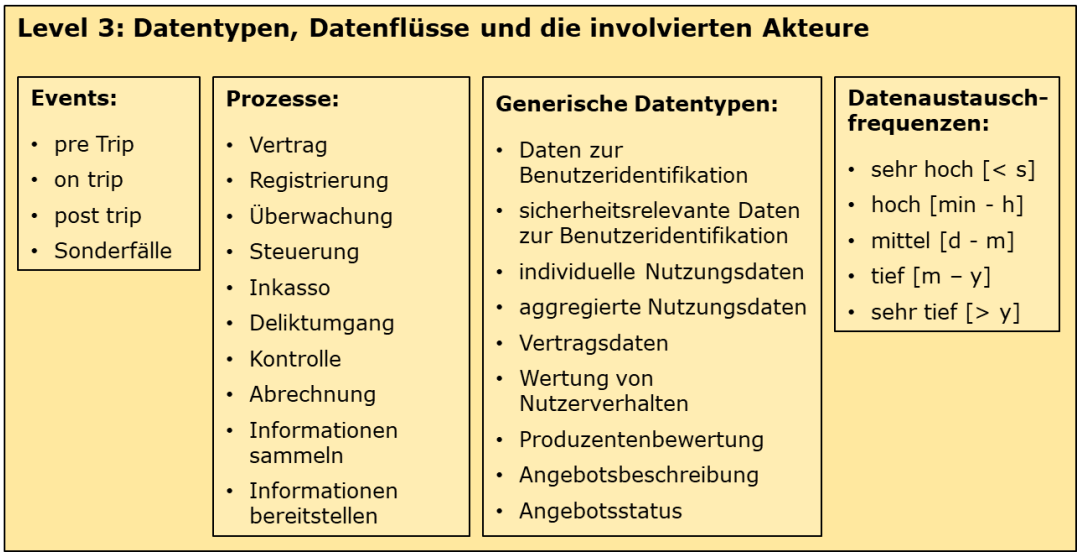


Abb. 17 *Instrumente und Auswahlmöglichkeiten zur Prozessbeschreibung.*

Die detaillierten Informationen, welche die generischen Datentypen beinhalten, werden in Kapitel 2.4 beschrieben.

Um die Inhalte der einzelnen generischen Datentypen zu verstehen, die Methodik zur Herleitung der anfallenden Datenflüsse aufzuzeigen und das Verständnis zu schärfen, wird das Vorgehen anhand der Anwendungen MaaS (Mobility-as-a-Service) und der elektronischen Strassengebührenerhebung (Road User Charge, RUC) beschrieben. Detaillierte Analysen für die weiteren in Abb. 14 angeführten Anwendungen können dem Anhang I entnommen werden.

2.3.1 Prozessanalyse der Smart Mobility-Anwendung MaaS

Unter MaaS werden Plattformen oder Mobilitätsökosysteme verstanden, die Smart Mobility-Anwendungen der verschiedene Mobilitätsdienstleister integral verbinden und koordinieren. MaaS ermöglicht den Nutzern die Planung, Buchung und Abrechnung von Fahrten auf einer einzelnen Plattform, welche von einem einzigen Dienstleister, dem MaaS Anbieter, betrieben wird. Dadurch wird dem Nutzer ein nahtloser Übergang von einem Verkehrsmittel zum anderen ermöglicht. Es entsteht ein Paradigmenwechsel, denn Reisende buchen nicht mehr die Reise mit einem oder mehreren Verkehrsmitteln um ein bestimmtes Ziel zu erreichen. Stattdessen steht für den Kunden das Ziel oder der Zweck im Vordergrund. Die Reise ist nur ein Mittel zur Zielerreichung und wird als Dienstleistung konsumiert.

Die Prozessanalyse stützt sich auf die Datenschutzerklärung einer MaaS-Anwendung (Whim Global, 2019), sowie einer darauf angewendeten Prüfung der EU-Datenschutzgrundverordnung (DSGVO) (Cottrill, 2020). Darin wird ein konzeptionelles MaaS-Datenökosystem hergeleitet, welches in Abb. 18 dargestellt ist. Unterschieden werden jeweils die Daten aus der Angebots- und Nachfrageseite, welche über eine Plattform miteinander verknüpft sind.

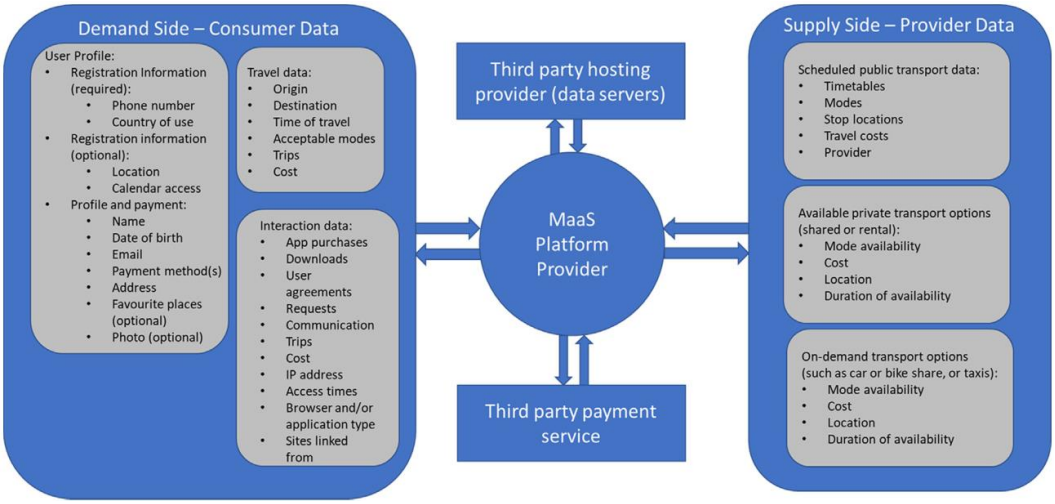


***Abb. 18** Konzeptionelles MaaS Datenökosystem (Cottrill, 2020)*

Das grundlegende Ziel jedes MaaS-Anbieters, der Angebot und Nachfrage auf einer digitalen Infrastruktur vermittelt, ist es, dass sowohl die Mobilitätsnachfrager als auch die Mobilitätsdienstleister mit dem MaaS-Anbieter Verträge eingehen und die Vertriebsabläufe über seine Plattform ermöglicht.

Die involvierten Akteure werden wie folgt in das im Kapitel 2.2 dargestellte Rollenmodell eingeteilt:

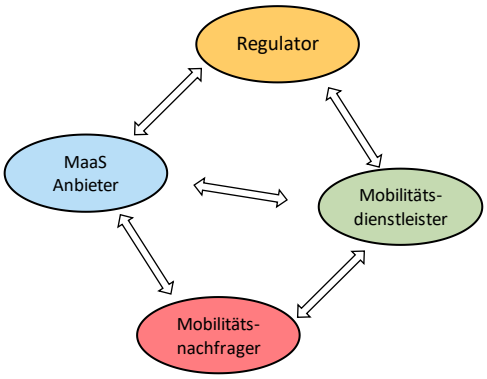
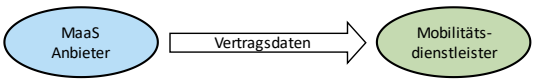


***Abb. 19** Rollenmodell bei MaaS*

- **Leistungserbringer:**
  Die Mobilitätsdienstleister stellen ihr Angebot auf der Plattform des MaaS-Anbieters zur Verfügung. Ihnen dient die Plattform als Marktplatz, um ihre Produkte zu bewerben und mehr Fahrgäste zu akquirieren. Der Infrastrukturbereitsteller ist in diesem Zusammenhang ebenfalls ein Leistungserbringer, da ohne die bereitgestellte Infrastruktur keine Mobilitätsdienstleistungen möglich sind.
- **Vermittler:**
  Der MaaS-Anbieter ist in der Rolle des Vermittlers, der die Angebote verschiedener Leistungserbringer bündelt, auf seiner Plattform zur Verfügung stellt und die Mobilitätsnachfrager mit dem Angebot verknüpft.
- **Nutzer:**
  Die Mobilitätsnachfrager und Mobilitätsnachfragerinnen nehmen die Mobilitätsdienstleistungen in Anspruch, die vom MaaS-Anbieter zur Verfügung gestellt werden.
- **Regulator:**
  In der Rolle des Regulators sind der Gesetzgeber, die Zertifizierungs- und Zulassungsstellen aber auch alle verbindlichen Rahmenbedingungen, wie Normen, zusammengefasst.

Im Folgenden werden die einzelnen Prozessschritte, die jeweils einen Datenfluss zwischen den Akteuren generieren, anhand der eingeführten Methodik erläutert.



Beim **pre trip-Prozess "Vertrag"** schliesst der MaaS-Anbieter mit verschiedenen Mobilitätsdienstleistern Verträge ab. Dabei

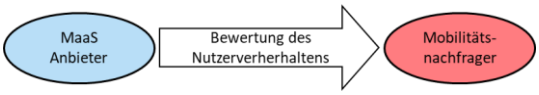
fliessen Vertragsdaten zwischen den beiden Akteuren und regeln die geschäftlichen Gegebenheiten. Unter diesen geschäftlichen Gegebenheiten kann auch geregelt werden, mit welchen anderen Mobilitätsdienstleiser das Angebot verknüpft oder ausgeschlossen werden kann. Dieser Datenaustausch erfolgt mit einer sehr tiefen Frequenz, da die Verträge üblicherweise über mehrere Jahre laufen.

Nach erfolgreichem Vertragsabschluss erhält der Mobilitätsdienstleister beim **pre Trip-Prozess "Registrierung"** vom MaaS-Anbieter die Identifikationsmerkmale, um sich bei ihm eindeutig und in einer gesicherten Art und Weise zu identifizieren. Dieser Datenaustausch erfolgt mit einer sehr tiefen Frequenz.

Beim **pre Trip-Prozess "Registrierung"** geben die Mobilitätsnachfrager dem Vermittler Daten zur Benutzeridentifikation preis. Dieser Austausch von persönlichen Daten wie z.B. Name, Rechnungsadresse, E-Mail-Adresse, Alter, Kreditkarteninformationen, Führerschein, Abonnemente erfolgt mit sehr tiefer Frequenz. Möglich ist auch die Übernahme von bereits bei einem Leistungserbringer registrierten Kunden.

Im Gegenzug erhält der Mobilitätsnachfrager beim **pre Trip-Prozess "Registrierung"** vom MaaS-Anbieter die Identifizierungsmerkmale, mit denen er sich bei Ihm sicher und eindeutig identifizieren bzw. authentifizieren kann. Dieser Datenaustausch erfolgt mit einer tiefen Frequenz.

Um den Dienst nutzen zu können, akzeptiert der Mobilitätsnachfrager beim **pre Trip-Prozess "Vertrag"** die AGB des MaaS-Anbieters. Dieser Datenaustausch erfolgt mit einer tiefen Frequenz. Darüber hinaus wählt der Mobilitätsnachfrager zwischen verschiedenen Angeboten und Modellen (i.d.R. Pay-as-you-go oder Abonnemente).

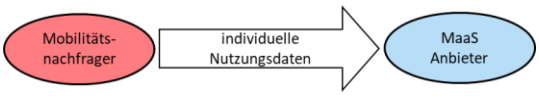


Der MaaS-Anbieter kann vom Mobilitätsnachfrager beim **pre Trip-Prozess "Informationen sammeln"** Daten für die Bewertung des Nutzerverhaltens anfragen. Dadurch kann er die persönlichen Präferenzen bezüglich der Verwendung von Mobilitätsangeboten bei der Vermittlung berücksichtigen. Dies erlaubt dem Mobilitätsnachfrager z.B. Anbieter zu priorisieren oder auszuschliessen.

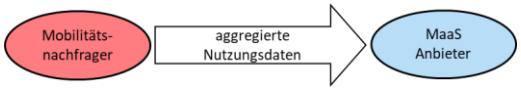
Der Mobilitätsdienstleister überliefert beim **pre Trip-Prozess "Informationen bereitstellen"** die Angebotsbeschreibung seiner Leistung wie z.B. die Fahrplaninformationen, die Verfügbarkeit, die geplanten Preise, etc. an den MaaS-Anbieter. Dieser Datenaustausch findet mit einer mittleren Frequenz statt.

Der Mobilitätsdienstleister überliefert beim **pre Trip-Prozess "Informationen bereitstellen"** den Angebotsstatus seiner aktuellen Leistung wie z.B. aktuelle Verfügbarkeit, Pünktlichkeit des Fahrplans an den MaaS-Anbieter und bringt damit das geplante Angebot in Relation zur aktuellen Betriebslage. Dieser Datenaustausch findet mit einer sehr hohen Frequenz statt.

Der MaaS-Anbieter stellt dem Mobilitätsdienstleister beim **pre Trip-Prozess "Informationen bereitstellen"** die notwendigen Daten über den Mobilitätsnachfrager zur Verfügung. Diese Daten umfassen die benutzeridentifikationsbezogenen Daten wie dessen Name, Abonnemente oder Führerscheine. Dieser Datenaustausch findet mit einer hohen Frequenz statt.

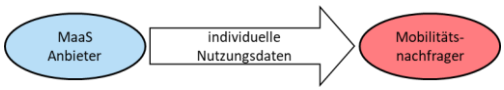


Durch die Nutzung der Dienste können Mobilitätsnachfrager, bei entsprechender Zustimmung, dem MaaS Anbieter Daten beim **on Trip-Prozess "Informationen sammeln"** Daten wie Fahrrouten (Geo-Positionsdaten, Zeit, Start & Ziel, Verkehrsmittel) zur Verfügung stellen. Dieser Datenaustausch erfolgt mit einer hohen Frequenz. Anhand einer Benutzer-ID können die Daten direkt mit den Benutzeridentifikationsdaten in Verbindung gebracht werden. Daraus können persönliche (Mobilitäts-)Präferenzen abgeleitet werden.



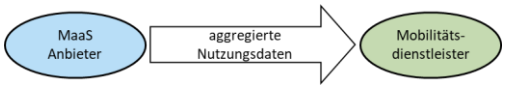
Durch die Nutzung der Dienste kann, bei entsprechender Zustimmung, der Mobilitätsnachfrager dem MaaS-Anbieter beim **on trip-Prozess "Informationen sammeln"** aggregierte, nicht-personenbezogene Nutzungsdaten wie die genutzten Verkehrsmittel, die gefahrene Distanz, die Fahrzeit etc. zur Verfügung. Dieser Datenaustausch findet mit einer mittleren Frequenz statt.

Der Mobilitätsdienstleister kontrolliert die Mobilitätsnachfrager während der Fahrt, ob sie mit gültigen Fahrscheinen unterwegs sind. Der Mobilitätsnachfrager muss dazu beim **on Trip-Prozess "Kontrolle"** seine Abonnemente (z.B. Halbtax, GA) oder das von der MaaS-Plattform bereitgestellte Ticket vorweisen. Die digitalen Tickets sind i.d.R. direkt mit der Identität des Nutzers verknüpft. Dieser Datenaustausch findet mit einer mittleren Frequenz statt.

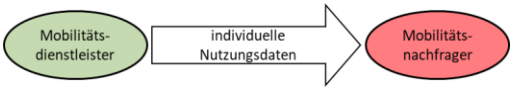


Der Mobilitätsnachfrager erhält beim **post Trip-Prozess "Abrechnung"** gemäss seiner zurückgelegten Distanz, der gewählten Verkehrsmittel und der Intensität der Inanspruchnahme von Transportdienstleistungen seine Rechnung. Dieser Datenaustausch findet mit einer mittleren Frequenz statt.

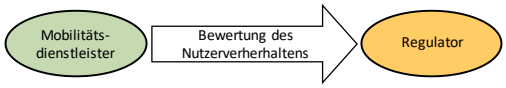
Die Begleichung der Rechnung durch den Mobilitätsnachfrager gegenüber dem MaaS-Anbieter erfolgt beim **post Trip-Prozess "Inkasso"**. Je nach Abrechnungsmodell variiert dieser Datenaustausch zwischen einer tiefen und hohen Frequenz.



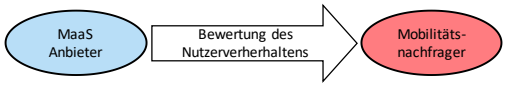
Der MaaS-Anbieter überweist beim **post trip-Prozess "Inkasso"** die mit den Verträgen geregelten und auf aggregierten Nutzungsdaten basierenden Beträge an die Mobilitätsdienstleister. Dieser Datenaustausch findet mit einer mittleren Frequenz statt.



Ergibt die Kontrolle durch den Mobilitätsdienstleister, dass eine Fahrt ohne gültigen Fahrschein gemacht wurde, so wird der Mobilitätsnachfrager beim **Sonderfall-Prozess "Deliktumgang"** anhand seiner individuellen Nutzungsdaten und seiner Nutzerbewertung gebüsst. Dieser Datenaustausch findet mit einer tiefen Frequenz statt.



Ergibt die Kontrolle des Mobilitätsnachfragers, dass eine Fahrt ohne einen gültigen Fahrschein gemacht wurde, so wird er im **Sonderfall-Prozess "Deliktumgang"** für eine bestimmte Zeitdauer in einer nationalen Datenbank, die vom Regulator betrieben wird, erfasst und bewertet. In der Schweiz werden fehlbare Nutzende des ÖV für mindestens zwei Jahre erfasst und im Wiederholungsfall wird die Busse erhöht, sowie die Zeitdauer bis zum Verfall des Eintrags entsprechend verlängert. Dieser Datenaustausch findet mit einer tiefen Frequenz statt.



Sollte der Mobilitätsnachfrager die Rechnungen nicht begleichen, so wird er im **Sonderfall Prozess-" Deliktumgang"** gebüsst und erfasst. Zusätzlich kann ihm der Zugang zur MaaS Plattform entzogen werden. In diesem Fall wird das Nutzerverhalten des Mobilitätsnachfragers durch den MaaS-Anbieter bewertet. Dieser Datenaustausch findet mit einer tiefen Frequenz statt.

2.3.2 Prozessanalyse der Smart Mobility-Anwendung Strassengebührenerhebung (RUC)

Bei der Strassengebührenerhebung, fortan mit RUC (Road User Charge) abgekürzt, wird für die Benutzung der Strasseninfrastruktur eine Abgabe erhoben. Grundsätzlich geht es darum, die zurückgelegte Distanz auf den Strassen zu messen und daraus die Abgabe zu berechnen.

RUC-Systeme beruhen auf einem Gebühren- und einem Erhebungskonzept. Im **Gebührenkonzept** wird die Abgabe rechtlich definiert. Insbesondere werden die abgabepflichtigen Fahrzeuge, das abgabepflichtige Netz und die Höhe der Abgabe je Fahrzeugtyp festgelegt. Das **Erhebungskonzept** beschreibt, wie die so definierte Gebühr umgesetzt wird. Relevante Governance-Fragen ergeben sich ausschliesslich aus dem Erhebungs-Aspekt, nicht aus der rechtlichen Definition der Gebühr. Für DAGSAM sind ist somit einzig die Aspekte des Erhebungskonzepts relevant. Die Nutzung der Verkehrsinfrastruktur soll effizient und somit möglichst automatisiert erfasst werden. Dieses umfasst im Kern alle Betriebsprozesse, d.h. die Registrierung der Fahrzeuge und der Abgabepflichtigen, die Erfassung der Nutzung, die Kundeninformation und Kundendienst, den Vertrieb, das Inkasso sowie die Kontrolle und Ahndung (INFRAS/Rapp/Ecoplan, 2021).

In den letzten 20 Jahren wurden im EU-CH-Raum hauptsächlich Gebührenkonzepte für den Schwerverkehr umgesetzt, mit unterschiedlichen Erhebungskonzepten. Während zu Beginn in den verschiedenen Ländern jeweils ein eigenes dezidiertes fahrzeugseitiges Erfassungsgerät, On Board Unit (OBU) genannt, eingebaut werden musste, ist es mittlerweile möglich, mit einem einzigen Gerät durch sämtliche Länder zu fahren. Die Europäische Gesetzgebung hat dazu die rechtlichen und normativen Grundlagen geschaffen[12]. Diese interoperable Dienstleistung "European Electronic Toll Service", EETS, muss von allen Ländern des europäischen Wirtschaftsraums (die Mitgliedstaaten der EU, Island, Liechtenstein und Norwegen), die über Gebührenerhebungssystem verfügen, angeboten werden. Auch die Schweiz folgt den Vorgaben des EETS.

Bei der Umsetzung der leistungsabhängigen Schwerverkehrsabgabe (LSVA) im Jahr 2001 mit der ersten Systemgeneration mussten die OBUs mit dem Tachographen in den Fahrzeugen verbunden werden und über eine spezifische Kurzstreckenkommunikationstechnologie, DSRC, kommunizieren können. Für die Umsetzung der 3. LSVA Systemgeneration, die ab 2024 eingeführt wird, ist weder die Verbindung mit dem Fahrzeug noch die DSRC-Kommunikation nötig. Das System wird einzig mittels der Technologien der Satellitennavigation (generische Bezeichnung GNSS – Global Navigation Satellite System, im spezifischen GPS, GALILEO und GLONASS) und des Mobilfunks (meist abgekürzt als CN - Cellular Network) betrieben.

Dies ermöglicht es in Zukunft, die Gebühr mit den bereits in den Fahrzeugen vorhandenen Systemen zu erheben. Seit der Einführung von e-Call sind in jedem neu zugelassenen Fahrzeug die Technologien **GNSS und CN** vorgeschrieben. Durch die Entwicklung der Standards zum Extended Vehicle (ISO 20077; ISO 20078) wird der Zugriff auf diese Daten zusätzlich vereinfacht und via Webservice ermöglicht (siehe die Ausführungen dazu in Kap. 5.3.4). Anhand der GNSS-Lokalisierung werden Lokalisierungspunkte im Fahrzeug aufgezeichnet und mittels Mobilfunk übermittelt. Auf einer zentral gehaltenen Karte wird mittels Map-Matching der Lokalisierungspunkte die tatsächlich gefahrene Distanz berechnet.

Die Machbarkeit einer flächendeckenden Abgabe mittels GNSS/CN-Ansatz ist durch mehrere operative Systeme nachgewiesen worden und angesichts der breiten Unterstützung der Technologieplattform im europäischen Recht und durch die europäische Normierung sowie durch unzählige Anwendungen, Geräte und Hersteller de facto die einzige realistische Umsetzungsoption (INFRAS/Rapp/Ecoplan, 2021). Aus diesen Gründen erfolgt die Prozessanalyse zur Identifikation der Datenflüsse auf dem Systemansatz der GNSS-Lokalisierung mit einer zentralen Kartenhaltung.

[12] Directive 2004/52/EC on the interoperability of electronic road toll systems in the Community und Commission Decision 2009/750/EC on the definition of the European Electronic Toll Service and its technical elements. Diese wurden anschliessend durch die aktualisierten EETS-Vorschriften (die Richtline 2019/520, die Delegierte Verordnung (EU) 2020/203 der Kommission und die Durchführungsverordnung (EU) 2020/204 der Kommission) ersetzt. (EG, 2009, 2020a, 2020b; EU, 2019)

Das Rollenmodell für RUC-Systeme wurde durch die Vorgaben des EETS de-facto festgeschrieben. Es stellt eine für die RUC-Anwendung spezifische Ausgestaltung des im Kapitel 2.2 dargestellten generischen Rollenmodells dar. Zudem beruht die Prozessanalyse auf dem Status Quo der Gebührenerhebung, in der die Fahrdaten der Infrastrukturbenutzer über den Maut-Dienstanbieter an den Gebührenerheber übermittelt werden. Dieser errechnet daraus die zu entrichtende Gebühr. Wie diese Fahrdaten der Infrastrukturbenutzer mittels einem Data-Governance-Modell geschützt werden können, wird in Kapitel 5.3 präsentiert.

Die involvierten Akteure des RUC-Rollenmodell bilden sich wie folgt auf das im Kapitel 2.2 dargestellten Rollenmodell ab:

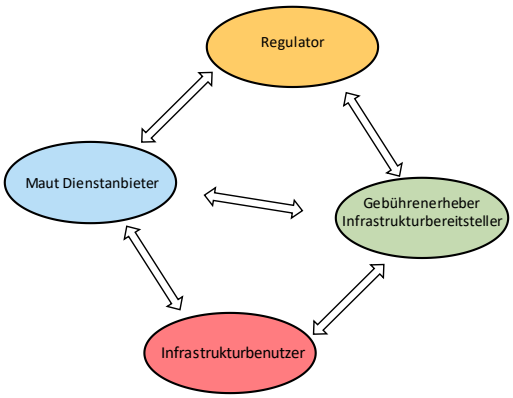


***Abb. 20** Rollenmodell bei RUC*

- **Leistungserbringer:**
  Der **Gebührenerheber**, als Leistungserbringer, ist verantwortlich für die Umsetzung der Erhebung, die Berechnung der Abgabenhöhe basierend auf der der übermittelten Fahrdistanz je Fahrzeugtyp und die Kontrolle der korrekten Entrichtung. Neben dem Gebührenerheber ist beim RUC ebenfalls der **Infrastrukturbereitsteller** ein Leistungserbringer, der das abgabepflichtige Netz zur Nutzung bereitstellt.
- **Vermittler:**
  Der **Maut-Dienstleister** ist in der Rolle des Vermittlers, der die Daten der Infrastrukturbenutzer sammelt und diese für die Berechnung der Abgabe dem Gebührenerheber zur Verfügung stellt. Er übernimmt zudem die Abrechnung zwischen dem Gebührenerheber und dem Infrastrukturbenutzer.
- **Nutzer:**
  Die Infrastrukturbenutzer, nehmen die vom Leistungserbringer bereitgestellte Infrastruktur mit ihren Fahrzeugen in Anspruch. Die Nutzer stehen hauptsächlich mit dem Maut-Dienstanbieter in Kontakt. Sie übermitteln mit den zur Verfügung gestellten Erfassungseinrichtungen im Fahrzeug die Geodaten ihrer Fahrstrecken an den Maut-Dienstanbieter und erhalten im Gegenzug die Rechnung für die Benutzung der Infrastruktur.
- **Regulator:**
  In der Rolle des Regulators sind der Gesetzgeber, Zertifizierungsstellen aber auch alle verbindlichen Rahmenbedingungen, wie Normen, zusammengefasst.

Im Folgenden werden die einzelnen Prozessschritte, die jeweils einen Datenfluss zwischen den Akteuren generieren, anhand der in Kap. 2.3 eingeführten Methodik erläutert. Die Prozessanalyse basiert auf den in EU-ICIP (2020) beschrieben Prozessen.

Beim **pre trip-Prozess "Vertrag"** geht der Maut-Dienstanbieter mit dem Gebührenerheber einen Vertrag ein, der die Erhebung und Bereitstellung von Pflichtdaten (GNSS Lokalisationen & Zeitpunkte, Fahrzeugtypen, gefahrene Distanzen, etc.) inkl. deren Genauigkeit, sowie die Abfuhr der vom Infrastrukturnutzer zu bezahlenden Abgaben an den Gebührenerheber regelt. Darüber hinaus wird im Vertrag geklärt, wie der Gebührenerheber den Mautbetreiber für die Dienstleistung entschädigt.

Beim **pre trip-Prozess "Registrierung"** werden Daten zur Benutzeridentifikation zwischen Maut-Dienstanbieter und

Gebührenerheber ausgetauscht. Bei diesen Daten handelt es sich um z.B. um Firmenamen, UID, Zahlungsadresse und Zahlungsdetails.

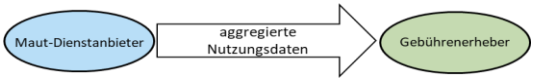
Beim **pre trip-Prozess "Registrierung"** werden sicherheitsrelevante Daten zur Benutzeridentifikation zwischen dem Gebührenerheber und dem Maut-Dienstanbieter ausgetauscht. Diese Identifizierungsmerkmale erlauben es dem Maut-Dienstanbieter, sich beim Gebührenerheber eindeutig zu identifizieren und gesichert zu kommunizieren.

Beim **pre trip-Prozess "Vertrag"** werden Vertragsdaten zwischen Infrastrukturbenutzer und Maut-Dienstanbieter ausgetauscht. Der Infrastrukturbenutzer akzeptiert die AGBs des Maut-Dienstanbieters und erhält im Gegenzug erhält den Service, mit der die Gebühr basierend auf seiner zurückgelegten Strecke je Fahrzeugtype berechnet werden kann.

Beim **pre trip-Prozess "Registrierung"** werden Daten zur Benutzeridentifikation zwischen Infrastrukturbenutzer und Maut-Dienstanbieter ausgetauscht. Der Infrastrukturbenutzer registriert sich bei einem Maut-Dienstanbieter mit Namen, VIN, Zahlungsadresse und Zahlungsdetails.

Beim **pre trip-Prozess "Registrierung"** werden sicherheitsrelevante Daten zur Benutzeridentifikation zwischen Maut-Dienstanbieter und Infrastrukturbenutzer ausgetauscht. Diese Identifizierungsmerkmale, erlauben es dem Infrastrukturbenutzer, sich beim Maut-Dienstanbieter eindeutig zu identifizieren und gesichert zu kommunizieren.

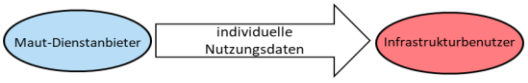
Beim **on trip-Prozess "Informationen sammeln"** werden **i**ndividuelle Nutzungsdaten zwischen Infrastrukturbenutzer und Maut-Dienstanbieter ausgetauscht. Während der Fahrt sammelt der Maut-Dienstanbieters mit seinem angebotenen Service die GNSS Lokalisationen des Infrastrukturbenutzers. Dieser Prozess hat als Grundanforderung, dass die gefahrenen Routen vollständig und korrekt abgebildet werden.



Beim **post trip-Prozess "Informationen bereitstellen"** werden individuelle Nutzungsdaten vom Maut-Dienstanbieter dem Gebührenerheber zur Verfügung gestellt, damit dieser die Höhe der Abgabe berechnen kann. Aus den GNSS Lokalisationen mit hoher Auflösung wird an einer zentralen Stelle mit Kartenabgleich die zurückgelegte Distanz pro Tarifzone berechnet. Der Maut-Dienstanbieter erhält im Gegenzug die Rechnung, die er anschliessend dem Infrastrukturbenutzer zur Begleichung vorlegt.

Beim **post trip-Prozess "Kontrolle"** werden individuelle Nutzungsdaten zwischen Maut-Dienstanbieter und Gebührenerheber ausgetauscht Der Gebührenerheber kontrolliert, ob die erhaltenen Fahrrouten plausibel und vollständig sind, in dem sie z.B. keine Lücken aufweisen.

Beim **on trip-Prozess "Kontrolle"** werden individuelle Nutzungsdaten zwischen Infrastrukturbenutzer und Gebührenerheber ausgetauscht. Der Gebührenerheber erhebt Bilder von Durchfahrtspassagen des Infrastrukturbenutzers, die mit einem Zeitstempel und dem Standort signiert sind. Anhand der Bilder wird die Korrektheit der Fahrtendeklaration überprüft. Der Abgleich mit den Fahrrouten muss innerhalb gegebener nützlicher Fristen stattfinden.



Beim **post trip-Prozess "Abrechnung"** werden individuelle Nutzungsdaten zwischen Maut-Dienstanbieter und

Infrastrukturbenutzer ausgetauscht. Der Infrastrukturbenutzer bekommt vom Maut-Dienstanbieter die Rechnung gemäss der zurückgelegten Distanz.

Beim **post trip-Prozess "Inkasso"** werden Daten zur Benutzeridentifikation zwischen Infrastrukturbenutzer und Maut-Dienstanbieter ausgetauscht, indem der Infrastrukturbenutzer die Rechnung begleicht.

Beim **post trip-Prozess "Inkasso"** werden Daten zur Benutzeridentifikation zwischen Gebührenerheber und Maut-Dienstanbieter ausgetauscht. Der Gebührenerheber begleicht die gemäss Vertrag anfallenden Beträge dem Maut-Dienstanbieter.

Beim **Sonderfall-Prozess "Deliktumgang"** werden **i**ndividuelle Nutzungsdaten zwischen Gebührenerheber und Infrastrukturbenutzer ausgetauscht. Falls bei den Kontrollen ein Vergehen festgestellt wird, eröffnet der Gebührenerheber ein Verfahren gegenüber dem Infrastrukturbenutzer, um ihn gemäss den rechtlichen Vorgaben zu ahnden.

Beim **Sonderfall-Prozess "Deliktumgang"** werden Daten zur Bewertung des Nutzerverhaltens zwischen dem Gebührenerheber und dem Maut-Dienstanbieter ausgetauscht. Bei Vergehen wird der Infrastrukturbenutzer von dem Maut-Dienstanbieter und dem Gebührenerheber bewertet (bspw. zur Feststellung wiederholter Widerhandlungen).

2.4 Generische Datentypen

Die Datenflüsse, die bei den einzelnen Anwendungen entstehen, konnten durch die detaillierten Prozessanalysen aller ausgewählten Anwendungen identifiziert und zu den folgenden generischen Datentypen zusammengefasst werden:

Daten zur Benutzeridentifikation:

Diese Daten ermöglichen die eindeutige Identifikation der Nutzer. Es handelt sich dabei um persönliche Daten wie z.B. Name, Nationalität, Geschlecht, Alter, Wohn-/Liefer-/Rechnungsadresse, E-Mail-Adresse. Zusätzlich fallen die Daten zur Abwicklung von Bezahlungen wie die Kreditkarteninformationen oder die Kontoangaben in diese Kategorie. Bei Fahrzeugen erlaubt die Fahrzeug-Identifikationsnummer (VIN) oder das Nummernschild eindeutige Rückschlüsse auf die Identifikation. Zudem gehören die bestehenden Abonnemente im öffentlichen Verkehr wie ein GA, Verbunds-Abo oder Halbtax sowie der Führerschein in diese Kategorie.

Sicherheitsrelevante Daten zur Benutzeridentifikation:

Merkmale wie Trust Objects und Keys werden zur sicheren und eindeutigen Identifizierung bzw. Authentifizierung zwischen Vertragspartner benötigt. Diese Informationen sind bei Zwei-Faktor-Authentifizierungen notwendig.

Individuelle Nutzungsdaten:

Diese Nutzungsdaten beinhalten z.B. die Fahrten und Routenverläufe über einen längeren Zeitraum (Geopositionsdaten, Uhrzeit, Start- und Zielort, Verkehrsmittel). Diese Routenverläufe und damit auch die zugrundeliegenden Daten erlauben die eindeutige Identifikation einer Person. Weitere Daten dieses Typs sind z.B. Ton- /Video- und Bildaufzeichnungen in nicht anonymisierter Form, Routenabfragen, die Bestellung von Lieferungen, Unterschriften auf Paketlieferscheinen etc. Eine User-ID verknüpft diese Daten direkt mit denjenigen zur Benutzeridentifikation. Diese Daten sind aus Sicht des Datenschutzes als Personendaten und gar oft als besonders schützenswerte Personendaten einzuordnen (s. dazu hinten Kap. 0).

Aggregierte Nutzungsdaten:

Die aggregierten Nutzungsdaten erlauben keine eindeutige Identifikation des Nutzenden. Die Anonymisierung findet entweder durch die Datenbearbeitung oder bereits bei der

Datenerhebung statt. Sie entstehen bei der Verwendung von Smart Mobility-Anwendungen und es handelt sich um Daten wie z.B. die Distanz der gefahrenen Strecke in einer bestimmten Tarifzone oder anonymisierte Video-/Bild-/Tonaufnahmen einer Nutzung.

Vertragsdaten:

Für die Nutzer entstehen Vertragsdaten in der Regel durch die Zustimmung zu den Bedingungen und Konditionen bzw. den allgemeinen Geschäftsbedingungen. Zwischen den Leistungserbringern und den Vermittlern handelt es um vertragliche Details, die die Preisgestaltung, die Bedingungen und die Leistungen (Lieferumfang) regeln. Zudem definieren sie, welche Daten in welcher Granularität und Auflösung zwischen den Akteuren fliessen.

Bewertung des Nutzerverhaltens:

Diese Daten enthalten Bewertungen der Nutzer durch den Leistungsanbieter oder Vermittler. Sie fallen bei der Nutzung der Mobilitätsangebote über einen längeren Zeitraum an und werden nutzerspezifisch gespeichert, sofern eine gesetzliche Grundlage dafür besteht oder der Nutzer seine Zustimmung zur Speicherung und Auswertung gegeben hat. Es handelt sich um eine Informationssammlung über das Nutzerverhalten. Diese beinhaltet neben den persönlichen Präferenzen wie die Bevorzugung von gewissen Verkehrsmitteln zusätzliche Merkmale wie z.B. Pünktlichkeit, Zahlungsbereitschaft, riskante Fahrweise. Verstösse und Delikte von Nutzern gegen die Geschäftsbedingungen oder das geltende Gesetz werden in Listen gespeichert wie z.B. im nationalen Register für Reisende ohne Fahrschein oder im Register für Mautpreller. Aus Datenschutzsicht kann es sich bei diesem Vorgehen um ein Profiling oder sogar um ein Profiling mit hohem Risiko handeln (s. dazu hinten in Kap. 3.2.2).

Produzentenbewertung:

Gleichzeitig werden auch die Leistungserbringer häufig durch die Nutzer bewertet. Vielfach handelt es sich bei diesen Bewertungen entweder um Störungsmeldungen, die den Komfort beeinträchtigen oder um Verbesserungsvorschläge bezüglich der genutzten Leistung.

Angebotsbeschreibung:

Dies sind statische, angebotsbeschreibende Daten, die unter anderem eine planbare Preisbildung erlauben. Dazu zählen die Fahrpläne des öffentlichen Verkehrs, die Verfügbarkeit von Angeboten wie die stationären Standorte von Sharing-Fahrzeugen, die geplanten Preise des Angebots oder die Kapazitäten von Strassen und öV-Angeboten. Daneben beschreiben sie auch das Angebot der Infrastruktur wie z.B. Geschwindigkeitsbegrenzungen und Fahrverbote. Die Infrastruktur wird anhand von digitalen topologischen Karten dargestellt. Weiter beschreiben diese Datentypen die Dimensionen der Logistikfahrzeuge (Ladevolumen, zugelassenes Gewicht) und deren Ausstattung (Kühlung, Flüssigkeitentanks, Gefahrguttransportfähigkeit) oder die Emissionsklassen.

Angebotsstatus:

Der aktuelle Status des Mobilitätsangebots verändert sich dynamisch. Dieser Datentyp setzt die aktuelle Betriebslage in das Verhältnis zur Angebotsbeschreibung und erlaubt damit die nachfrageorientierte Preisbildung. Zu diesem Datentyp zählen die aktuelle Verfügbarkeit von Sharing-Fahrzeugen und Sitzplätzen im öV, die Strassenauslastung und die freien Strassenkapazitäten, der Rückstau auf Strassen und an Knoten, die aktuelle Pünktlichkeit eines Fahrplans oder die zeitabhängigen Preise eines Angebots. In Bezug auf die Infrastruktur und deren digitale Abbildung können temporäre Strassensperren oder Baustellen in den Karten abgebildet werden. Weiter berücksichtigt dieser Datentyp für Fahrzeuge u.a. deren Tankfüllstand oder Reichweite, die transportierten Güter, Beschleunigungsdaten, Informationen über die Fahrzeugorientierung, den Airbag-Status sowie die aktuelle Positionierung der Fahrzeuge.

Die einzelnen Datentypen werden anhand der folgenden Abbildung in einen übergeordneten Kontext gestellt. Die Mobilität ist ein Träger der Schweizer Volkswirtschaft. Die Schweizer Volkswirtschaft lässt sich durch Strukturdaten beschreiben, welche eine der wichtigsten Grundlagen für die Planung von Mobilitätsangeboten bilden und mehrheitlich öffentlich zugänglich sind. Sie werden nicht weiter berücksichtigt, da sie für Smart Mobility-Anwendungen in der Angebotsplanung berücksichtigt werden und dem täglichen operativen Geschäft vorgelagert sind. Innerhalb der Mobilität sind Smart Mobility-Anwendungen ein Mittel, um

den Mobilitätsbedürfnissen und den Beweggründen für die Mobilitätsnachfrage der Bevölkerung gerecht zu werden.

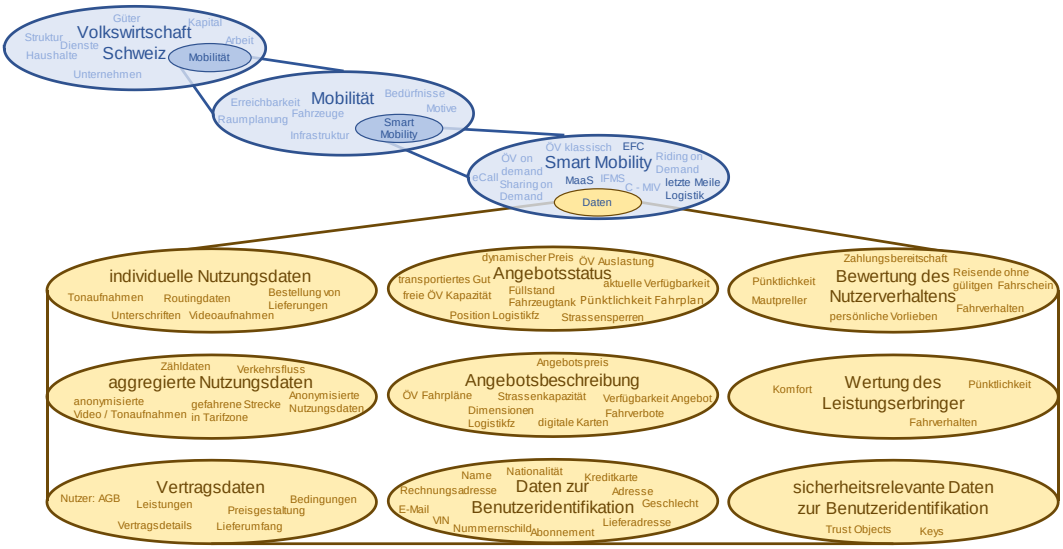


Abb. 21 *Generische Datentypen von Smart Mobility-Anwendungen im Kontext der Schweizer Volkswirtschaft.*
Quelle: Grundlage von (ITS CH, 2021), durch eigene Überlegungen ergänzt.

2.5 Einbezug der Stakeholder

Neben der Ermittlung der Datentypen und Datenflüsse sagen auch die Beobachtungen, Vorstellungen und Ansprüche der Stakeholder etwas über das Funktionieren der Märkte für Mobilität aus und zeigen, wohin sich eine Data Governance für Mobilitätsdienste bewegen könnte.

2.5.1 Interviews

Im Rahmen des Forschungsprojekts wurden Interviews mit ausgewählten Stakeholdern geführt. Die Interviews dienten dazu, die Erkenntnisse aus der Prozessanalyse zu überprüfen und verschiedene Sichtweisen auf die schützenswerten Assets eines Unternehmens, die Anforderungen an die Konzeption einer digitalen Infrastruktur und deren Governance-Anforderungen zu gewinnen. Es wurde darauf geachtet, relevante und repräsentative Mobilitätsdienstleister aus dem öffentlichen und konzessionierten Bereich sowie der Privatwirtschaft einzubinden und gleichzeitig die verschiedene Mobilitätsformen wie Bus, Bahn, Velo, MIV und Sharing zu berücksichtigen. Die relevanten Erkenntnisse aus den Interviews werden im Folgenden jeweils danach gegliedert, welche Assets die Stakeholder als schützenswert erachten, welche Erwartungen sie an die Dateninfrastruktur haben und welche Governance-Anforderungen sie sich wünschen:

AMAG

Die AMAG-Gruppe ist das grösste Schweizer Automobil Import- und Handelsunternehmen und tätig im Bereich von Mobilitätsdienstleistungen wie Leasing, Valet Parking, Chauffeurdienste, digitale Vernetzung von Fahrzeugen (autoSense) und Automobil-Abonnemente (Clyde). Zudem ist sie eine Partnerin der Swiss Startup Factory und entwickelt mit dem AMAG Innovation & Venture LAB neue Geschäftsmodelle im Bereich der Mobilität.

Schützenswerte Assets: Besonders wertvoll ist der Kundenstamm. Er soll nicht von jemand anderem übernommen werden können. Die Bewegungsprofile der Kundinnen und Kunden stellen einen Mehrwert für die Privatwirtschaft dar. Zudem sind das Angebot und die monetäre Wirksamkeit des Angebots zu schützen.

Dateninfrastruktur: Die AMAG stellt sich die Dateninfrastruktur als einen Marktplatz vor, um die Reichweite des Angebots zu erhöhen und zusätzliches Vertriebspotential zu schaffen. Sichergestellt werden soll eine immer gleichbleibende User Experience. Dazu soll es möglich sein, Nutzerprofile anzulegen, um die Mobilitätsbedürfnisse der Kundschaft besser zu verstehen. Die Vermittlungen der Angebote und Nachfrage auf der Plattform darf nicht viel kosten.

Governance-Anforderungen: Eine Dateninfrastruktur mit öffentlichen und privatwirtschaftlichen Angeboten muss zwingend durch eine treuhänderisch agierende Institution (Custodian) betrieben werden, der gleichberechtigt alle Player bedient, nicht mit den Daten hantiert und kein Leistungserbringer für das Mobilitätsökosystem ist. Diese Institution ist für die Kundenverwaltung zuständig und ein Routing muss fair und transparent über ihn funktionieren. Die Datenhoheit soll beim Leistungserbringer der Mobilität liegen und die Nutzer sollen im Sinne eines "opt in" der Verwendung ihrer Daten zustimmen können. Die Angebote des Leistungserbringers sollen nicht komplett offengelegt, sondern über Anfragen beantwortet werden. Die Leistungserbringer stellen die Angebote und diese müssen für den Custodian unsichtbar bleiben. Zudem soll über vertragliche Kontrolle und selektive Freigabe der Angebote ermöglicht werden, Angebotskombination mit Konkurrenzunternehmen zu unterbinden.

MyBuxi

MyBuxi ist ein Start-up-Unternehmen für On-Demand-Transporte in ländlichen Gebieten mit einem schlanken und effektiven digitalen Auftritt. Zukünftig möchte das Unternehmen gesamte Mobilitätsketten zusammenstellen und sieht sich als Vermittler und Transportdienstleister. Es ist Gründungsmitglieder der Genossenschaft openmobility.

Schützenswerte Assets: Die Kundendaten und deren Profile sind schützenswert und die Kundschaft soll selbst bestimmen können, was mit ihren Daten geschieht. Der aktuelle Betriebszustand des MyBuxi Angebots kann nicht offengelegt werden, weil dies aufgrund der dynamischen Veränderlichkeit gar nicht möglich ist. Während die Vertragsinhalte als schützenswert betrachtet werden, stellt die Offenlegung der Vertragspartner kein Problem dar.

Dateninfrastruktur: Kooperationen mit Dritten und die Kombination von Angeboten sollen einfach und kostengünstig möglich sein. Dafür ist ein Datenaustausch notwendig. Über ein smart contract-Verwaltungssystem soll die Zusammenarbeit mit Partnern ermöglicht und über Standardverträge die Partnerschaften geregelt werden. Die Dateninfrastruktur soll die Visibilität der Angebote erhöhen und die Angebote müssen über Bestellschnittstellen verfügbar gemacht werden. Die Dateninfrastruktur soll ein variables Kernstreckenrouting ermöglichen. Dieses soll nicht von Punkt (z.B. Bahnhof) zu Punkt, sondern zwischen zwei regionalen Clustern mehrerer Punkte funktionieren und je nach Betriebszustand während der Reise dynamisch angepasst werden können. Der «Consent» der NutzerInnen zu wichtigen Fragen wie dem Datenaustausch persönlicher oder sogar besonders schützenswerter Daten zwischen Unternehmen soll einfach hinterlegt und verwaltet werden können. Eine eindeutige Identifikation von NutzerInnen ist nötig für Reiseketten, die personalisierte Angebote enthalten. Es braucht einen Mechanismus, damit geblockte Personen nicht über Umwege wieder Dienste in Anspruch nehmen können.

Governance-Anforderungen: Wenn eine Gesamtdienstleistung von A nach D angeboten werden soll, ist der Dienstleister unmittelbar für Haftungsfragen verantwortlich. Dies kann entsprechend geregelt werden, z.B. über smart contracts. Bei dynamischen Angeboten ist wichtig, dass zu viele Anfragen (von der gleichen Quelle) unterbunden werden können, um das System vor Überlast zu schützen.

Pick-e-Bike

Pick-e-Bike ist ein Anbieter von Velo-Verleihsystemen in der Region Basel und verfügt neuerdings auch über ein Franchising Modell in Freiburg i. Üe. Pick-e-Bike befindet sich im Besitz der BLT, der Primeo energy und der Basler Kantonalbank.

Schützenswerte Assets: Die Kundendaten sind schützenswert, auch um die Kunden vor Angeboten oder Werbung zu schützen. Ansonsten gibt es wenig Schützenswertes bei Pick-e-Bike und der BLT im Allgemeinen. Da Pick-e-Bike aus drei Unternehmen besteht, ist eine hohe Transparenz erforderlich. Als Teil der Öffentlichkeit und des öffentlichen Verkehrs werden ihre Zahlen entsprechend offengelegt.

Dateninfrastruktur: Die Dateninfrastruktur soll ein Art Warenhaus sein, wo alle ihre Angebote einstellen können und diese verknüpfbar gemacht werden sollen, zum Wohle der Kunden. Bei Mietsachen ist es gesetzlich vorgeschrieben, Personendaten wie z.B. Adressen zu erfassen. Dies ist bei der Konzeption der Infrastruktur zu berücksichtigen. Eine digitale Plattform an sich ist kein technisches Problem, sondern ein vertragliches.

Governance-Anforderungen: Die Kunden sollten nicht von der Konkurrenz angeschrieben werden können, um sie abzuwerben oder ihnen Angebote zu unterbreiten.

Postauto

Die Postauto AG ist mit über 900 Buslinien, einer Netzlänge von über 16'000 Kilometern und 13'000 Haltestellen das grösste Schweizer Unternehmen des öffentlichen Strassentransports. Sie entwickelt sich zudem in den Bereichen On-Demand und Sharing, wie die jüngsten Beispiele aus dem Appenzellerland und dem Verzascatal zeigen.

Schützenswerte Assets: Das Angebot kann ohne Bedenken offengelegt werden, aber nicht im Detail. Betriebsgeheimnisse, zu denen die Gestehungskosten gehören, sollen entsprechend geschützt werden.

Dateninfrastruktur: Die Dateninfrastruktur soll das Interesse befriedigen, dass möglichst viele Personen über die Angebote Bescheid wissen. Die Dateninfrastruktur sollte zur Förderung der Flexibilisierung eine Reservations- und Prognosefähigkeit haben.

Governance-Anforderungen: Die Dateninfrastruktur benötigt einen unabhängigen Orchestrator und einen diskriminierungsfreien Zugang. Zudem soll sie ein transparentes Routing zur Verfügung stellen. Die Dateninfrastruktur benötigt einen Schutzmechanismus, um maschinelle Abfragen zu identifizieren. Bei Verdacht auf Handlungen, welche die Offenlegung von Betriebsgeheimnissen zum Ziel haben, sind diese zu unterbinden. Der Transportdienstleister bedient die Schnittstelle zur Infrastruktur, um seine Produkte anzubieten, er soll aber die weiterhin Möglichkeit haben, jemanden abzulehnen.

SOB

Die Schweizerische Südostbahn AG (SOB) ist ein Schweizer Eisenbahnunternehmen, das sich mit digitalen Innovationen wie dem elektronischen Ticketing und den digitalen Mobilitätslösungen beschäftigt. Die SOB engagiert sich für den Aufbau von Partnernetzwerken, um neue integrierte Mobilitäts-Ökosysteme einzuführen und ist Gründungsmitglied der openmobility Genossenschaft. Die SOB nimmt vier Perspektiven ein: Transportunternehmen, Tourismusplattform mit dem Kernziel, Züge zu füllen, Engagement für eine nachhaltige Mobilität sowie Unterhalt und Betrieb von Eisenbahninfrastruktur.

Schützenswerte Assets: Die Kundendaten inkl. ihrer Customer Journeys und Kundenprofile sind schützenswert und sollen beim Unternehmen bleiben. Aus betrieblicher Sicht sind dies die Auslastung und die Passagierfrequenzen, die Personal- Betriebsstunden und die internen Kostensätze. Grundsätzlich kann alles, was keine Kundendaten oder Daten, die Schlussfolgerungen auf Gestehungskosten, Produktionskosten und Einsatz der Fahrzeuge erlauben, offengelegt werden.

Dateninfrastruktur: Die Dateninfrastruktur soll einen Marktplatz bieten, der erlaubt, ihr Kernangebot zu erweitern. Die Dateninfrastruktur befindet sich in der Mitte zwischen den Lieferanten (Mobilitätsdienstleister) und den Händlern. Die Händler haben den Kontakt mit der Kundschaft und stellen ihnen spezifische Angebote von Mobilitätsdienstleistern (die gleichzeitig auch Händler sein können) zusammen. Der Marktplatz soll sich selbst tragen ist aber nicht gewinnorientiert. Er ist Mittel zum Zweck, damit sich insgesamt für die Kundschaft ein ideales Angebot entwickelt.

Governance-Anforderungen: Aufgrund des Pauschalreisegesetzes wird der Händler sehr schnell zum Leistungserbringer und haftbar für die Leistungen Dritter. Die Dateninfrastruktur soll die Daten zum Buchen, Zusammenstellen der Reise und Abrechnen verarbeiten. Dies muss neutral und diskriminierungsfrei erfolgen. Der Zugang muss von jedem Mobilitätanbieter einzeln angeschlossen werden und die Dateninfrastruktur sollte dies technisch einheitlich zur Verfügung stellen. Der Datenschutz ist ein Nebenthema, wenn sensible Kundendaten beim Anbieter bleiben. Um den Kunden Gesamtpakete anzubieten, wären passgenaue Kundenprofile ideal. Kunden mit Kundenprofilen könnte während der Reise, unter Berücksichtigung geltender Datenschutzbestimmungen und dem Einverständnis der Kundschaft (opt in), Zusatzangebote gemacht werden.

2.5.2 Anforderungen der Stakeholder

Zusammenfassend lassen sich die Interessen der Stakeholder in Bezug auf deren schützenswerte Assets, die operativen Anforderungen an eine Dateninfrastruktur und die Anforderungen an die Governance wie folgt unterteilen:

Schützenswerte Assets

Die Kundendaten und deren Profile müssen in der Hoheit der Stakeholder beziehungsweise deren Kunden bleiben. Zudem muss dem Kunde eine gleichbleibende und qualitativ hochwertige Customer Journey angeboten werden. Während die Namen der Vertragspartner – zumindest teilweise – offengelegt werden können, sind die Vertragsinhalte schützenswert und müssen dementsprechend im Verborgenen bleiben. Die Betriebszustände der Smart Mobility-Anwendungen verändern sich dynamisch. Demzufolge soll zwar das Angebot eine hohe Visibilität erfahren, jedoch sind die Auslastung, die Passagierfrequenzen, die Personal-/ Betriebsstunden, die internen Kostensätze und die monetäre Wirksamkeit des Angebots zu schützen.

Grundsätzlich kann alles offengelegt werden, sofern es sich nicht um Kundendaten oder Daten handelt, die Schlussfolgerungen auf Gestehungskosten, Produktionskosten und Einsatz der Fahrzeuge erlauben.

Operative Anforderungen an eine Dateninfrastruktur

Die Dateninfrastruktur wird als unabhängiger Marktplatz verstanden, der die Reichweite des Angebots, zusätzliches Vertriebspotential, verknüpfbare Angebote, kostengünstige Vermittlung von Angebot & Nachfrage und den Datenaustausch bereitstellt. Nutzerprofile sollen dazu dienen, Mobilitätsbedürfnisse besser zu verstehen. Zusätzlich werden bei Mietsachen zwingend Personendaten erhoben. Die Leistungserbringer, die auch Vermittler sein können, sollen den Kontakt mit den Kunden pflegen und ihnen spezifische Angebote von verschiedenen Mobilitätsdienstleistern zusammenstellen können. Weiter soll die Dateninfrastruktur eine Reservations- und Prognosefähigkeit besitzen.

Über ein intelligentes Vertrags-Verwaltungssystem soll die Zusammenarbeit mit Partnern über Standardverträge ermöglicht werden. Die Dateninfrastruktur soll ein dynamisches Routing zur Verfügung stellen, dessen Nutzung freiwillig sein sollte. Zur Erhöhung der Effizienz des Gesamtverkehrssystems soll das Routing kontextualisiert und personalisiert arbeiten, damit im jeweiligen Fall optimale Routen angeboten werden können. Nach welchen Kriterien und mit welchen Algorithmen dieses Routing funktioniert, muss offengelegt werden (Transparenz) und so die Fairness gewährleistet werden. Zudem sollen die Leistungserbringer und/oder Vermittler dieses Routing für ihre Zwecke adaptieren können, z.B. Kombinationen ihrer Angebote mit denjenigen der Konkurrenz zu unterbinden. Insbesondere muss eine gleichbleibende User Experience sichergestellt werden und dabei die Performanz, Skalierbarkeit und den Datenschutz bei verteilten Systemen mitberücksichtigen.

Governance Anforderungen an eine Dateninfrastruktur

Eine treuhänderisch agierende Institution hat die Dateninfrastruktur zu betreiben und bietet einen diskriminierungsfreien Zugang. Über die Governance sollen Haftungsfragen in Bezug auf Garantieleistungen geregelt sein. Die Angebote der Leistungserbringer dürfen nicht komplett offengelegt, sondern nur auf Anfrage hin beantwortet werden (selektive Freigabe einzelner Angebote). Ein Schutzmechanismus ist nötig, um maschinelle Abfragen zu identifizieren, beziehungsweise zu unterbinden. Die Datenhoheit muss beim Leistungserbringer bleiben und die Nutzer stimmen per opt in der Verwendung ihrer Daten zu.

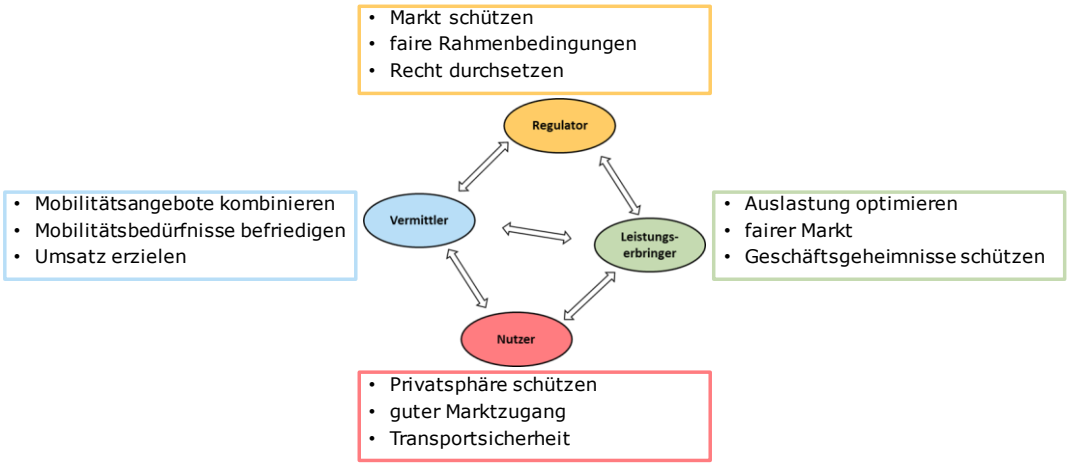


Abb. 22 *Zu schützende Interessen der Stakeholder in der Mobilitätslandschaft Schweiz.*

3 Juristische Instrumente

3.1 Daten als Gegenstand des Rechts

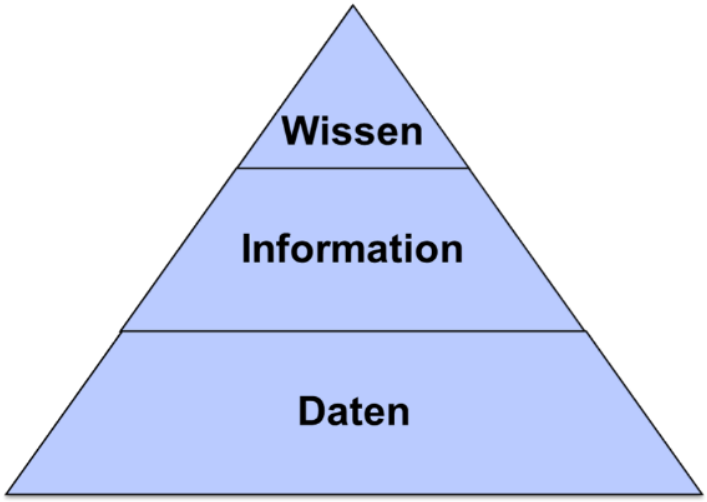


Abb. 23 *Informationspyramide*
Quelle: Thouvenin & Früh, 2020

Bevor auf die wesentlichen rechtlichen Fragen im Zusammenhang mit Mobilitätsdaten eingegangen werden kann, ist zu klären, was das Recht überhaupt unter dem Begriff "Daten" versteht. Das lässt sich anhand der sog. *Informationspyramide* (Thouvenin & Früh, 2020; Weber & Thouvenin, 2018) und eines praktischen Beispiels mit Nutzerdaten aus dem Mobilitätsbereich erläutern. Je nachdem auf welcher Stufe der Informationspyramide die Daten vorliegen, spricht man von *Daten*, *Information* oder *Wissen*:

- Sensoren, welche im Inneren eines Fahrzeugs dessen Position laufend aufzeichnen, sammeln *Daten* auf der *syntaktischen Ebene* (engl. Code Layer). Es handelt sich um eine Folge von Zeichen, die bei digitalen Daten oftmals in einer endlichen Folge von Nullen und Einsen besteht. Andere mögliche Formen der Repräsentation sind Gruben (pits) und Flächen (lands) in der Spiralspur einer CD. Daten sind auf der syntaktischen Ebene maschinenlesbar. Diese Daten sind für Menschen zunächst einmal unverständlich.
- Liegen die Daten, ausgegeben von der entsprechenden Software, aber in einer Form (etwa als geografische Koordinaten) vor, welche als geografischer Hinweis verstanden werden kann, spricht man von *Information* auf der *semantischen Ebene* (engl. Content Layer). Jemand der über diese Information verfügt, weiss, wann sich das Auto an welchen Orten befand. Ein zentrales Merkmal von Information ist, dass diese durch menschliche Sinne wahrgenommen werden kann. Der Übergang von der syntaktischen Ebene zur semantischen Ebene erfordert deshalb eine Maschine, welche die Informationen aus den Daten extrahiert und in eine für den Menschen wahrnehmbare Form überführt.
- Ein Car-Sharing-Unternehmen kann nun diese Informationen über die Aufenthaltsorte eines Fahrzeugs mit anderen Nutzerinformationen zusammenführen und daraus beispielsweise ableiten, wo sich der Wohn- oder Arbeitsort eines Nutzers befindet. Durch dieses Zusammenführen von Informationen entsteht *Wissen* auf der *pragmatischen Ebene.*

Manchmal wird in der Lehre auch noch eine vierte Ebene, nämlich die *strukturelle Ebene* (engl. Physical Layer), unterschieden. Sie bezieht sich aber auf die physikalische Festlegung der Daten auf einem physischen Träger und ist deswegen nicht in der Informationspyramide abgebildet, welche sich ausschliesslich auf unkörperliche (d.h. immaterielle) Gegenstände bezieht.

Für die Frage der rechtlichen Zuordnung von Daten ist wesentlich, auf welcher dieser Ebenen die Rechtsordnung anknüpft. Die in der Folge dargestellten rechtlichen Instrumente wie die Immaterialgüterrechte, der Geheimnisschutz und das Datenschutzrecht knüpfen auf der semantischen Ebene an, d.h. dort, wo Daten als Informationen auftreten und damit in einer Form, die vom Menschen sinnlich wahrgenommen werden kann. Einzig der Schutz durch das Sacheigentum knüpft auf der strukturellen Ebene an. Rechtlich geschützt werden dadurch allerdings bloss die Datenträger, nicht die Daten als solche.

3.2 Instrumente für die Zuordnung von Daten

3.2.1 Rechtslage

Obwohl es in der Schweizer Rechtsordnung an einem eigentlichen Eigentumsrecht an Daten fehlt, gibt es einige Instrumente, welche eine Zuordnung von Daten bewirken können. Dabei lassen sich *Zuordnungsnormen, Schutznormen,* die *vertragliche Zuordnung* von Daten und die Zuordnung aufgrund des *Datenschutzrechts* unterscheiden.

Als ***Zuordnungsnormen*** können jene Instrumente bezeichnet werden, welche einer natürlichen oder juristischen Person *Ausschliesslichkeitsrechte (absolute Rechte)* an Daten gewähren. Sie vermitteln der jeweiligen Person eine Rechtsposition, die gegenüber jedermann gilt und gerichtlich durchgesetzt werden kann. Als mögliche absolute Rechte an Daten kommen in der Schweiz die Immaterialgüterrechte (Urheberrecht, Patentrecht, Designrecht, Markenrecht) und die im Urheberrecht geregelten so genannten Leistungsschutzrechte in Frage. Ein wie in der EU existierendes sui generis-Recht an Datenbanken (Richtlinie 96/9/EG) besteht in der Schweiz hingegen nicht. Die *rechtliche (Schutz-)Wirkung* von Immaterialgüter- und Leistungsschutzrechten besteht darin, dass der jeweilige Rechtsinhaber jede fremde, unerlaubte Nutzung der geschützten immateriellen Güter bzw. eine Vervielfältigung des geschützten Werks oder ein Zugänglichmachen der geschützten Leistung (gerichtlich) verbieten lassen kann. Daneben kann der jeweilige Inhaber von Immaterialgüter- und Leistungsschutzrechten positiv über seine Rechte verfügen, indem er diese belastet (z.B. mit Pfandrechten), auf Dritte überträgt oder Dritten Lizenzrechte zu deren Nutzung erteilt.

Als ***Schutznormen*** können jene Instrumente bezeichnet werden, die einer natürlichen oder juristischen Person einen rechtlichen Schutz an Daten einräumen, die von der jeweiligen Person faktisch kontrolliert werden. In den Genuss des Schutzes kommt also, wer die tatsächliche Herrschaft über die Daten ausübt.

Eine solche Bestimmung findet sich beispielsweise im *wettbewerbsrechtlichen Schutz von Fabrikations- und Geschäftsgeheimnissen* (Art. 6 UWG). Daneben gewährt das Bundesgesetz über den unlauteren Wettbewerb mit einem gegen die *Verwertung fremder Leistungen* gerichteten Tatbestand (Art. 5 lit. c UWG) eine Rechtsposition, welche die faktische Kontrolle der Berechtigten über Daten stärkt. Diese Schutznormen gewähren der jeweiligen Person wie bei den Ausschliesslichkeitsrechten einen *Unterlassungs- und Beseitigungsanspruch*, den diese gegen potentielle Rechtsverletzer geltend machen kann. Zudem kann die berechtigte Person vom Verletzer *Schadenersatz* verlangen oder mittels Strafantrag dessen *strafrechtliche Verfolgung* veranlassen. Allerdings wirken diese Ansprüche nur gegen vom Gesetz bezeichnete *bestimmte* Verletzer und nicht gegenüber jedermann wie bei den Ausschliesslichkeitsrechten. Geben die Verletzter die erlangten Daten beispielsweise an Dritte weiter, versagen die Ansprüche.

Weitere Schutznormen finden sich im *strafrechtlichen Geheimnisschutz* (Art. 162 StGB) und im Schutz von *Amts- bzw. Berufsgeheimnissen* (Art. 320 f. StGB), die im Zusammenhang mit bestimmten Daten zur Anwendung kommen. Die faktische Herrschaft über Daten wird zudem durch die *Strafbarkeit gewisser Handlungen* geschützt, wozu die unbefugte Datenbeschaffung (Art. 143 StGB; sog. "Datendiebstahl"), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB; sog. "Hacking"), die Datenbeschädigung (Art. 144bis StGB) und der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB; sog. "Automatenbetrug") gehören. Diese Schutznormen gewähren den Berechtigten aber keinen Unterlassungs- und Beseitigungsanspruch, sondern lediglich ein *Strafantragsrecht*. Mit dem strafrechtlichen Rechtsschutz kann also im Unterschied zum

Unterlassungs- und Beseitigungsanspruch die Verwendung fremder Daten nicht verboten werden, wenn diese einmal den Herrschaftsbereich des Rechtsträgers verlassen haben.

Daten können auch mittels ***vertraglicher Vereinbarungen*** einem Rechtsträger zugeordnet werden. Zwar wirken solche Verträge im Gegensatz zu den gegenüber jedermann wirkenden Ausschliesslichkeitsrechten nur zwischen den Vertragsparteien. Die Vertragsfreiheit gewährt den Parteien jedoch die Möglichkeit, eine Rechtslage zu schaffen, die einem Ausschliesslichkeitsrecht recht nahekommt.

Schliesslich sorgt auch das ***Datenschutzrecht*** für eine gewisse Zuordnung von Daten, welche einen Bezug zu einer oder mehreren Personen aufweisen. Es stützt sich dabei auf den Persönlichkeitsschutz (Art. 13 Abs. 2 BV; Art. 28 ZGB). Das Schweizer Datenschutzgesetz (DSG) wurde jüngst revidiert und wird am 1. September 2023 in revidierter Fassung in Kraft treten (nDSG). Es regelt den Umgang mit *Personendaten* und definiert diese als "alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen" (Art. 3 lit. a DSG). Im EU-Recht gilt dieselbe Definition (vgl. Art. 4 Abs. 1 VO Nr. 2016/679, DSGVO). Die Bestimmbarkeit von Personen wird weit ausgelegt. Es genügt nach Auffassung des Bundesgerichts bereits, dass die Identifikation einer bestimmten Person ohne unverhältnismässigen Aufwand möglich ist (BGE 138 II 346 E. 6.1). Alle Daten, die keine Personendaten sind, werden Sachdaten genannt und unterstehen nicht dem Datenschutzrecht. Allerdings kann nicht leichthin angenommen werden, dass es sich um Sachdaten handelt. Denn durch die Kombination und Verknüpfung verschiedener Daten können auch scheinbare Sachdaten, die für sich allein keinen Personenbezug (mehr) aufweisen, einer bestimmten Person zugewiesen werden und somit (wieder) zu personenbezogenen Daten werden. Die zunehmende Digitalisierung und Sammlung grosser Datenmengen (Big Data) hat zur Folge, dass immer mehr Daten einen Personenbezug aufweisen (vgl. Thouvenin & Früh, 2020).

Gewisse Personendaten werden besonders geschützt. Beinhalten die Daten Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen, dann gelten diese als *besonders schützenswerte Daten* (Art. 3 lit. c DSG). Liegt eine Zusammenstellung von bestimmten Daten vor, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben, so sind diese Daten Gegenstand eines sog. *Persönlichkeitsprofils* (Art. 3 lit. d DSG; *"Profiling"* und *Profiling mit hohem Risiko"* im Art. 35 lit. f und g nDSG). An besonders schützenswerte Personendaten oder an das Profiling knüpfen strengere Regeln an, namentlich in Bezug auf die Bekanntgabe an Dritte (s. Art. 12 Abs. 2 lit. c DSG, leicht anders künftig Art. 30 Abs. 1 lit. c nDSG), die Anforderungen an die Einwilligung (Art. 4 Abs. 5 DSG; Art. 6 Abs. 7 lit. a und b nDSG).

3.2.2 Anwendung und Methodik

Welche der vorstehend dargestellten Instrumente auf die einzelnen generischen Datentypen aus Kapitel 2.4 anwendbar sind, muss jeweils im Einzelfall geprüft werden. Die für den Mobilitätsbereich massgeblichen Fragen lassen sich in zwei Flussdiagrammen vereinfacht darstellen und können schematisch geprüft werden. Daraus ergibt sich, wem welche Daten in einem konkreten Sachverhalt – bspw. bei einem bestimmten Mobilitätsangebot – mit welchen Instrumenten zugeordnet sind. Die Instrumente können auch kumulativ wirken, wenn deren jeweilige Voraussetzungen erfüllt sind. Welche Instrumente in einem bestimmten Einzelfall eine Zuordnung der Daten bewirken, ergibt sich aus dem untenstehenden Flussdiagramm "Datenzuordnung".

- Zuallererst kann geklärt werden, ob an den fraglichen Daten *Urheberrechte* bestehen. Dies ist dann der Fall, wenn die Daten Bilder, kreative Texte oder kreative Film- oder Tonaufnahmen beinhalten (Art. 2 Abs. 2 lit. a und g sowie Abs. 3bis URG). Damit Rechte an Texten, Film- oder Tonaufnahmen entstehen, müssen diese gewisse Voraussetzungen erfüllen, namentlich eine *geistige Schöpfung* darstellen (Äusserung gedanklicher Tätigkeit eines Menschen) und einen *individuellen Charakter* haben. An Bilder werden insofern weniger hohe Anforderungen gestellt, als sie auch dann als Werk gelten, wenn sie keinen individuellen Charakter haben und damit nicht kreativ sind (Art. 2 Abs. 3bis URG). Aufgrund der genannten Voraussetzung der geistigen

Schöpfung entstehen keine Urheberechte an vollautomatisierten Bild- oder Videoaufnahmen von Verkehrsüberwachungskameras oder Radarkontrollgeräten. Besteht indes ein Urheberrecht an den Daten, wirkt dies gegenüber jedermann.

- Weiter ist der Frage nachzugehen, ob die betroffenen Daten *Gegenstand eines Fabrikations- oder Geschäftsgeheimnisses* sind (Art. 6 UWG; Art. 162 StGB). Die Voraussetzungen für den wettbewerbsrechtlichen und den strafrechtlichen Geheimnisschutz sind weitgehend deckungsgleich: Die fraglichen Daten müssen Gegenstand von Tatsachen sein, die weder offenkundig noch allgemein zugänglich sind. Dann handelt es sich um Geheimnisse. In Bezug auf die Geheimhaltung dieser Tatsachen muss der Geheimnisherr oder die Geheimnisherrin zudem ein Geheimhaltungsinteresse und einen Geheimhaltungswillen haben. Gegenstand des Geheimnisschutzes sind typischerweise Daten über die Nutzung einer Mobilitätsdienstleistung, über Preismodelle oder über Auslastungen.
- Zuletzt können Daten durch das Wettbewerbsrecht vor fremder Verwertung geschützt sein (Art. 5 lit. c UWG). Der Schutz dieser Norm greift, wenn die fraglichen Daten *marktreif* sind und von Dritten *ohne angemessenen eigenen Aufwand* und durch *technische Reproduktionsverfahren* übernommen und *verwertet* wurden. Auch wenn die Rechtsprechung diesen Schutz nur selten gewährt, kann er beispielsweise gegen die Übernahme einer Datenbank mit nutzer- bzw. kundenbezogenen Daten (individuellen Nutzerdaten und Bewertung des Nutzerverhaltens) durch einen Konkurrenten oder Wettbewerber greifen.
- Greift keines der genannten Instrumente, d.h. wurden alle Fragen im Flussdiagramm "Datenzuordnung" mit "Nein" beantwortet, so können die Daten grundsätzlich frei genutzt werden. Zu beachten sind jedoch allfällige datenschutzrechtliche Aspekte (siehe sogleich in Kap. 3.3) sowie vertragliche Verpflichtungen, die allerdings nur in den seltensten Fällen offenkundig sind.

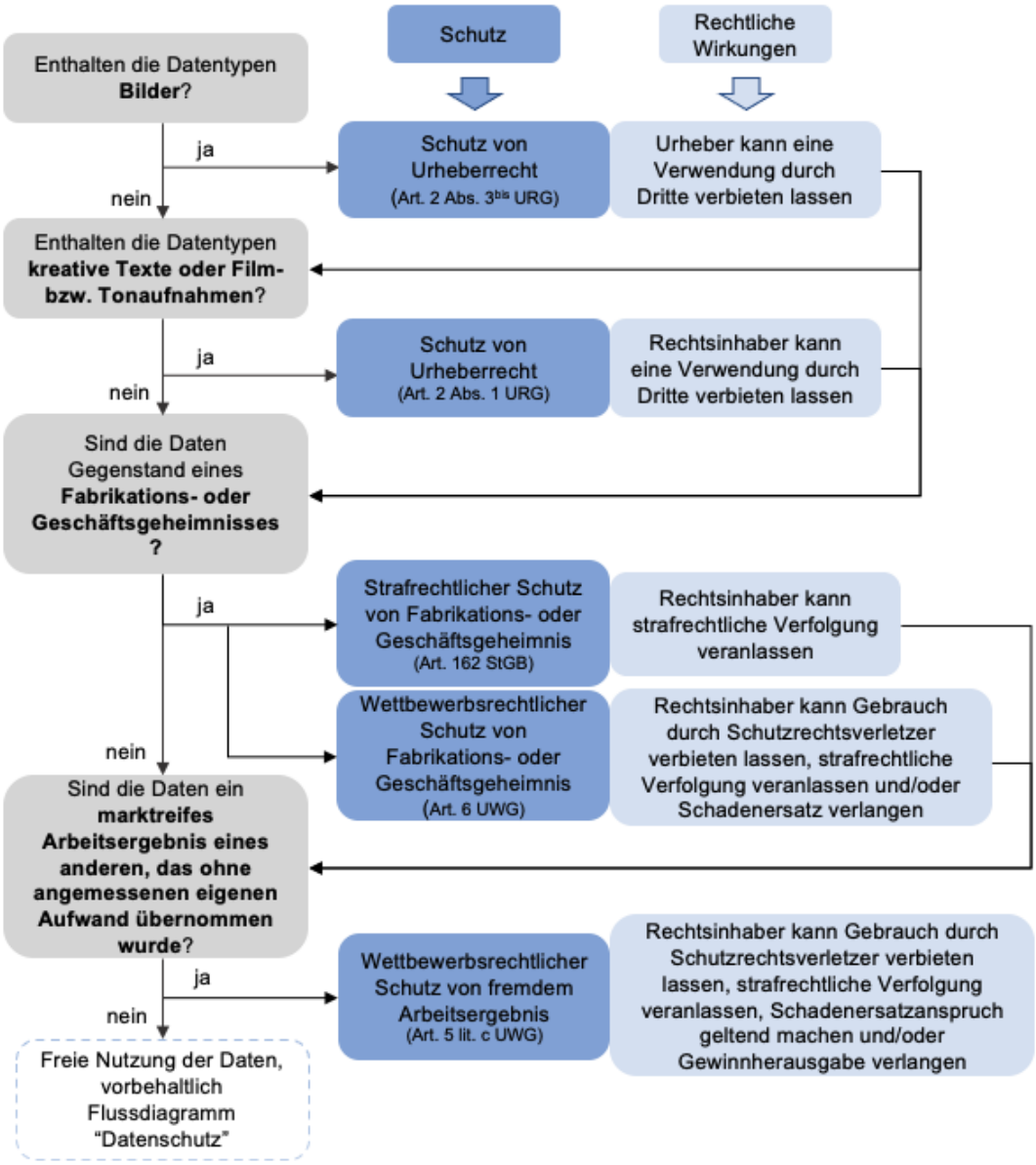


***Abb. 24** Flussdiagramm "Datenzuordnung*"

Inwiefern das Datenschutzrecht greift, lässt sich ebenfalls anhand einer Reihe von Fragen beantworten, die im untenstehenden Flussdiagramm "Datenschutz" abgebildet sind.

- Eingangs ist zu klären, ob eine natürliche Person durch die fraglichen Daten ohne unverhältnismässigen Aufwand **identifiziert** werden kann. Ist die Frage zu verneinen, handelt es sich um Sachdaten, für deren Bearbeitung die Grundsätze des Datenschutzgesetzes nicht anwendbar sind. Im Einzelfall kann es jedoch sein, dass durch die Kombination und Verknüpfung weiterer Informationen oder Daten solche Sachdaten dennoch einen Personenbezug erhalten können, womit diese dennoch als Personendaten zu qualifizieren sind.
- Kommt man zum Schluss, dass es sich bei den fraglichen Daten um Personendaten handelt, muss als Folgefrage geklärt werden, ob diese spezifische sensible Informationen über die betroffenen Personen beinhalten und somit als **besonders schützenswerte Personendaten** gelten. Im gleichen Schritt ist zu klären, ob die fraglichen Daten im Zusammenhang mit dem **Profiling** einer Person stehen.

Die Unterscheidung von Personen- und Sachdaten ist deshalb von grosser Relevanz, da die *Bearbeitung von Personendaten den strengen Regelungen des Datenschutzrechts des Bundes oder eines Kantons untersteht*. Die für die Bearbeitung von Personendaten anwendbaren Bestimmungen des Datenschutzgesetzes bringen diverse *Pflichten des Datenbearbeiters* und *diverse Rechte der betroffenen Person* mit sich. Wie diese strengen

Regelungen für die Bearbeitung von Personendaten aussehen, kann anhand des Datenschutzgesetzes des Bundes dargestellt werden:

Das Datenschutzgesetz auferlegt Datenbearbeitern die *Pflicht*, die Grundsätze der *Rechtmässigkeit* (Art. 4 Abs. 1 DSG; Art. 6 Abs. 1 nDSG), *Verhältnismässigkeit* (Art. 4 Abs. 2 DSG; Art. 6 Abs. 2 nDSG), *Zweckbindung* (Art. 4 Abs. 3 DSG; Art. 6 Abs. 3 nDSG), *Erkennbarkeit* (Art. 4 Abs. 4 DSG; Art. 6 Abs. 3 nDSG) und der *Bearbeitung nach Treu und Glauben* (Art. 4 Abs. 2 DSG; Art. 6 Abs. 2 nDSG), zu wahren. Daten bearbeitende Personen müssen sich zudem über die *Richtigkeit* der Daten vergewissern (Art. 5 DSG; Art. 6 Abs. 5 nDSG) und haben die zur Bearbeitung von Personendaten genutzten Systeme technisch von Anfang an so auszugestalten, dass der Datenschutz eingehalten wird und datenschutzfreundlich voreingestellt sind (sog. "privacy by design and default", Art. 7 nDSG). Die Verletzung dieser Pflichten führt zu einer Persönlichkeitsverletzung zulasten der betroffenen Person und entsprechenden Ansprüchen (Art. 12 Abs. 2 DSG und Art. 15 DSG bzw. Art. 30 nDSG und Art. 32 nDSG i.V.m. Art. 28 ff. ZGB). Die Widerrechtlichkeit einer Persönlichkeitsverletzung kann jedoch gerechtfertigt werden. Mögliche Rechtfertigungsgründe können sich aus der Einwilligung einer Person in die Datenbearbeitung, durch überwiegende private oder öffentliche Interessen oder aus dem Gesetz ergeben (Art. 13 DSG; Art. 31 nDSG).

Der betroffenen Person gewährt das Datenschutzgesetz verschiedene *Rechte*, namentlich das Recht auf *Auskunft*, ob Daten über sie bearbeitet werden (Art. 8 DSG; Art. 25 nDSG), das Recht in die Bearbeitung ihrer Daten *einzuwilligen* (Art. 13 Abs. 1 DSG; Art. 31 Abs. 1 nDSG) oder das Recht, die Übertragung oder Herausgabe ihrer Daten zu verlangen (sog. Datenportabilitätsrecht; Art. 28 f. nDSG). Das Datenschutzrecht erlaubt es der betroffenen Person also bis zu einem bestimmten Grad, die Bearbeitung ihrer Daten zu kontrollieren. Kommt es zu einer widerrechtlichen Persönlichkeitsverletzung durch die Datenbearbeitung, kann die betroffene Person insbesondere die *Sperrung* der Datenbearbeitung, die *Untersagung der Bekanntgabe von Daten an Dritte*, die *Berichtigung* der Personendaten oder deren *Löschung bzw. Vernichtung* verlangen (Art. 15 DSG; Art. 28 und 32 nDSG).

Handelt es sich bei den fraglichen Daten um besonders *schützenswerte Personendaten oder um Daten im Zusammenhang mit Profiling*, können weitergehende Pflichten anfallen, wie die Pflicht von Inhabern von Datensammlungen, betroffene Personen über die Beschaffung ihrer besonders schützenswerten Personendaten oder Profiling-Daten zu *informieren* (s. unter noch geltendem Recht Art. 14 DSG; Art. 18a DSG; s. unter dem revidierten Recht die weiteren Pflichten unter Art. 4 und 5 nDSG). Ist für die Datenbearbeitung eine Einwilligung erforderlich, so hat diese bei besonders schützenswerten Personendaten oder Profiling-Daten ausdrücklich zu erfolgen (Art. 4 Abs. 3 DSG; Art. 6 Abs. 7 nDSG). Ferner muss die Bearbeitung von besonders schützenswerten Personendaten und Profiling-Daten *durch Bundesorgane* grundsätzlich auf einer *formellgesetzlichen Grundlage* beruhen (Art. 17 Abs. 2 DSG; Art. 34 Abs. 2 nDSG).

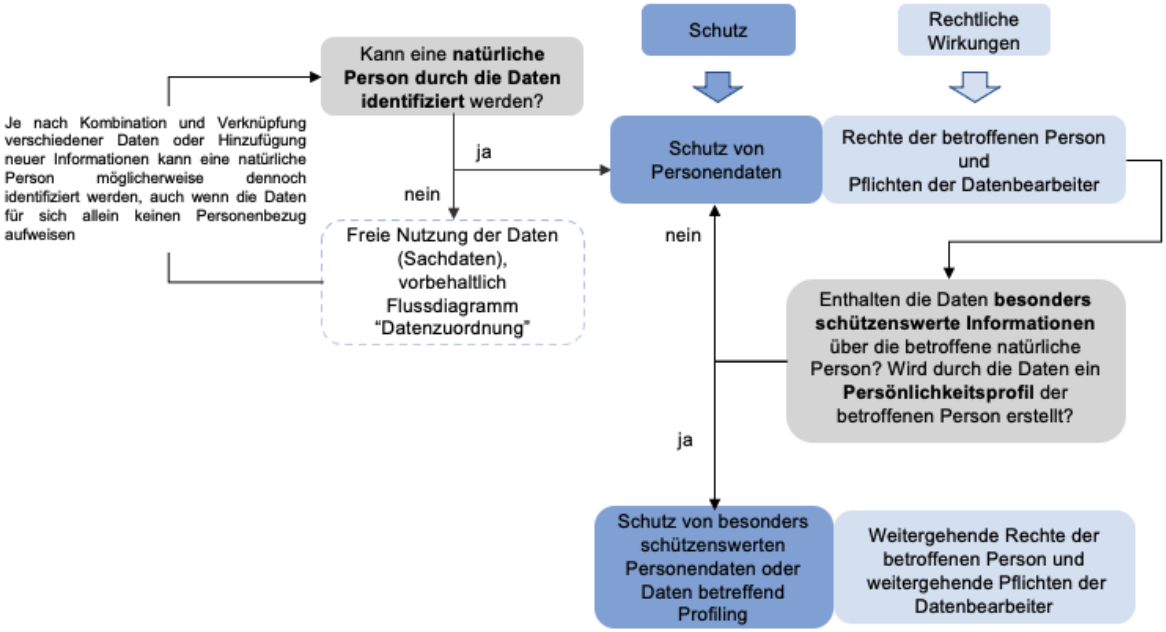


Abb. 25 Flussdiagramm "Datenschutz"

3.3 Instrumente für den Zugang zu Daten

Die Kehrseite zur Zuordnung von Daten bildet die Diskussion, ob und unter welchen Umständen *Datenzugangsrechte* bestehen. Es geht mithin darum, wann staatliche Behörden oder Private verpflichtet werden, bestimmte Daten im Kontext der Mobilität anderen zur Verfügung zu stellen. Diese Frage stellt sich kaum, solange Mobilitätsdaten von Zuordnungsnormen erfasst und damit mit absoluten Rechten geschützt sind. In solchen Zuordnungsnormen, wie sie sich beispielsweise aus dem Urheberrecht ergeben, sind nämlich typischerweise auch Ausnahmeregeln enthalten, um den Zugang zum geschützten Gut zugunsten anderer Interessen zu gewähren. Man spricht von so genannten Schranken (Beispiele sind die Zitatfreiheit im Urheberrecht oder im Patentrecht das Recht, an einer geschützten Erfindung zu forschen). Solche spezifischen Schranken zugunsten der Nutzung von Mobilitätsdaten existieren heute nicht und ein Bedürfnis nach ebensolchen ist bislang auch nicht erkennbar. Die Frage stellt sich ebenfalls nicht, wenn und solange Unternehmen "ihre" (Mobilitäts-)Daten Dritten oder der Allgemeinheit frei zur Verfügung stellen. Dafür hat sich der Begriff der Datenphilanthropie etabliert (Hofheinz & Osimo, 2017).

Schliesst die faktische Kontrolle der Dateninhaber allerdings Dritte grundsätzlich von der Nutzung der Daten aus, können Datenzugangsrechte ein Instrument darstellen, um diese faktische Kontrolle aufzubrechen. Allgemeine Datenzugangsrechte, welche unabhängig von Mobilitätssektor beim Vorliegen allgemeingültiger Voraussetzungen zum Schutz öffentlicher oder privater Interessen greifen, gibt es im geltenden Recht grundsätzlich nicht. Einzige Ausnahme ist die auf das kartellrechtliche Missbrauchsverbot gestützte Pflicht zur Offenlegung bestimmter Informationen oder Daten, wenn dadurch Dritte im Wettbewerb behindert werden (Art. 7 Abs. 2 lit. a KG) (siehe hierzu Früh, 2018, S. 536, jedoch mit Vorbehalten zur Anwendbarkeit des Kartellrechts).

In Bezug auf Mobilitätsdaten ergeben sich aus dem öffentlichen Recht indes durchaus vereinzelte Bestimmungen, welche deren Offenlegung oder eine allgemeine Zugangsgewähr vorschreiben. Wie bei der Datenzuordnung und dem Datenschutzrecht kann wiederum in einem vereinfachten Flussdiagramm schematisch mithilfe einer Reihe aufeinander folgender Fragen geprüft werden, zu welchen Daten im Mobilitätsbereich Zugang erwirkt werden kann. Der Fokus liegt hierbei nicht auf Rechten, die gewissen Individuen gestützt auf deren Persönlichkeit oder persönlicher Betroffenheit zustehen (z.B. beim datenschutzrechtlichen Auskunftsanspruch i.S.v. Art. 8 DSG bzw. Art. 25 nDSG, siehe vorne Kap. 3.2.2). Vielmehr geht es um Zugangsrechte, die unabhängig von der jeweiligen Person und aus übergeordneten Interessen gewährt werden:

- Handelt es sich um Daten der öffentlichen Verwaltung, müssen diese grundsätzlich aufgrund des Öffentlichkeitsprinzips der Verwaltung der Allgemeinheit zugänglich gemacht werden. Dies wird durch verschiedene Open-Government Data-Initiativen unterstützt, im Mobilitätsbereich beispielsweise mit der Open-Data-Plattform Mobilität Schweiz (BAV, 2021c). Andere Beispiele sind die öffentliche Erhältlichkeit von Geobasisdaten (swisstopo, 2021a) und Daten über das Verkehrsnetz Schweiz (swisstopo, 2021b), welche beide durch das Bundesamt für Landestopografie swisstopo zur Verfügung gestellt werden. Ausgenommen sind Mobilitätsdaten, die – vorbehaltlich allfälliger spezialgesetzlicher Auskunftsrechte von betroffenen Personen oder spezialgesetzlich vorgesehener Zugangsrechte Dritter in Bezug auf anonymisierte Personendaten oder Sachdaten – grundsätzlich nur für den behördeninternen Gebrauch vorgesehen sind, etwa aus sicherheitspolizeilichen, datenschutzrechtlichen oder anderen dem Öffentlichkeitsprinzip entgegenstehenden Interessen (siehe für den Bund Art. 7 ff. BGÖ). Beispiele hierfür sind die Daten in den Informationssystemen Strassenverkehrskontrollen (Art. 89o ff. SVG [SR 741.01]; Art. 47 f. Strassenverkehrskontrollverordnung [SR 741.013]), Strassenverkehrsunfälle (ISU) (Art. 89i ff. SVG; Art. 1 ff. Verordnung über das Informationssystem Strassenverkehrsunfälle [SR 741.57]) und Strassenverkehrszulassung (IVZ) (Art. 89 a-h SVG; Art. 1 ff. Verordnung über das Informationssystem Verkehrszulassung [SR 741.58]).
- Befinden sich die fraglichen Daten im Herrschaftsbereich eines Transportunternehmens (privat oder mit staatlicher Beteiligung), so kann dieses allenfalls gesetzlich dazu verpflichtet sein, gewisse Daten der Allgemeinheit oder einer staatlichen Behörde zugänglich zu machen. Dabei fällt auf, dass mehrheitlich Transportunternehmen mit einer Personenbeförderungskonzession von solchen Datenoffenlegungspflichten betroffen sind. So haben beispielsweise konzessionierte Transportunternehmen oder Transportunternehmen, die sich freiwillig der Fahrplanverordnung unterstellen, ihre Fahrplandaten jedermann zur Verfügung zu stellen (Art. 10 Abs. 2 Fahrplanverordnung [SR 745.13]). Beispiele für weitere Offenlegungspflichten zugunsten staatlicher Behörden sind die Offenlegung streckenbezogener Daten von konzessionierten Transportunternehmen (Art. 53 Abs. 3 Personenbeförderungsgesetz [SR 745.1]) und konzessionierten Eisenbahnunternehmen (Art. 12b Eisenbahnverordnung [SR 742.141.1]) an das Bundesamt für Verkehr.
- Daten, welche nicht Gegenstand einer der genannten Zugangsrechte oder Offenlegungspflichten sind, können von den Dateninhabern ohne Einschränkung kontrolliert werden. Vorbehalten bleiben – wie bereits erwähnt – kartellrechtliche Ansprüche.

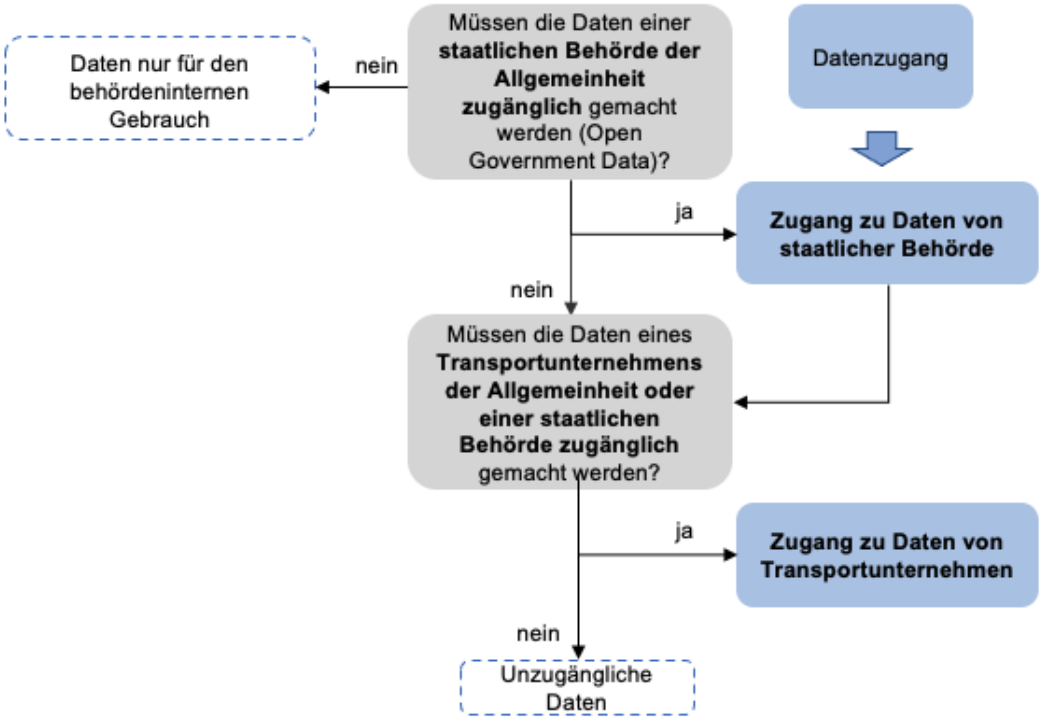


Abb. 26 *Flussdiagramm "Datenzugang"*

4 Technologische Instrumente

4.1 Grundlagen

Um die Privatheit, Vertraulichkeit, Integrität oder Authentizität sensitiver Daten zu schützen, müssen diese Eigenschaften während des gesamten Lebenszyklus der Daten sichergestellt werden. Grundlegend unterscheidet man hier drei Phasen, welche im Lebenszyklus von Daten jeweils mehrfach auftreten können, und unterschiedliche Anforderungen bezüglich Effizienz und Sicherheitsgarantien haben.

- **Data at Rest**: Mit diesem Term werden Daten beschrieben, auf welche aktuell nicht zugegriffen wird, und welche in einer physischen oder logischen Speichereinheit abgelegt sind. Beispiele für derartige Medien reichen von Datenbanken über USB-Sticks zu cloudbasierten Datenservern. Die Herausforderungen für Data at Rest sind vielfältig und reichen von der fehlenden Kontrolle über cloudbasierte Speicheranbieter, über Speichern auf physisch ungeschützten Geräten wie USB-Sticks, hin zu langfristigen Verfügbarkeits- und Sicherheitsanforderungen.
- **Data in Transit** oder **Data in Motion**: Hiermit werden Daten während ihrer Übertragung bezeichnet, unabhängig vom gewählten Medium. Die Herausforderungen zur Wahrung von Vertraulichkeit und Integrität während der Datenübertragung umfassen die Vielzahl an möglichen Übertragungswegen, die fehlende Kontrolle über die Sicherheit am Endpunkt der Übertragung, sowie Limitierungen bei der zur Verfügung stehenden Rechenkapazität und Bandbreite.
- **Data in Use**: In dieser Phase wird auf Daten zugegriffen, beispielsweise um sie zu lesen, zu löschen, zu aktualisieren, oder weiterzuverarbeiten. Relevante Herausforderung ist unter anderem die Kontrolle, dass die Verarbeitung nur im Einvernehmen mit Vereinbarungen und relevanten rechtlichen Auflagen stattfindet. Des Weiteren müssen in den meisten bestehenden Systemen Daten während der Verarbeitung im Klartext vorliegen, wodurch im Falle eines Angriffs während der Verarbeitung die Vertraulichkeit der Daten nicht garantiert werden kann. Zudem bestehen während der Datenverarbeitung auch hohe Effizienzanforderungen.

Die ersten beiden genannten Phasen sind wohlverstanden, und es existieren viele Richtlinien und hocheffiziente kryptographische und technische Lösungen, sodass im Folgenden nicht weiter auf diese Phasen eingegangen wird. Zur Sicherung von Data in Use werden unter anderem starke Authentifizierungslösungen, fein-granulare Zugriffskontrollen, sowie die Protokollierung von Datenzugriffen eingesetzt.

Um die verbleibenden Limitierungen, insbesondere bezüglich des notwendigen Vertrauens in zentrale verarbeitende Stellen mit Klartextzugriff während der Verarbeitung, zu reduzieren, findet derzeit aktive Forschung an fortgeschrittenen technologischen und kryptographischen Methoden statt. Dabei wird einerseits die Flexibilität und Funktionalität innovativer Lösungen erweitert, und andererseits ein Schwerpunkt auf die Erhöhung der Effizienz und Skalierbarkeit bestehender Lösungen und deren Implementierungen gelegt.

4.2 Technologieübersicht

Im Folgenden wird eine Übersicht ausgewählter Technologien gegeben, welche bei der Entwicklung eines Data Governance-Modells berücksichtigt werden. Die nachfolgende Beschreibung ist weitgehend anwendungsagnostisch. Aufgrund spezifischer Anforderungen und Limitierungen der einzelnen Technologien in Bezug auf Vertrauensannahmen und Sicherheitsgarantien, Funktionalität und Einsetzbarkeit, sowie Effizienz und Skalierbarkeit erfolgt eine Zuordnung der Technologien auf einzelne Anwendungsszenarien unter Berücksichtigung der jeweiligen Anforderungen anschliessend in den Kapiteln 5.2 und 5.3.

4.2.1 Multi-Party Computation

Secure Multi-Party Computation (MPC) beschreibt eine Klasse von kryptographischen Protokollen, die es mehreren Parteien erlaubt, gemeinsame Berechnungen auf vertraulichen Eingabedaten durchzuführen. Dabei wird sichergestellt, dass jede Partei nur das definierte

Ergebnis der Berechnung lernt, nicht jedoch weitere Informationen über die Eingabedaten der anderen Teilnehmer, vgl. auch die folgende Abbildung.

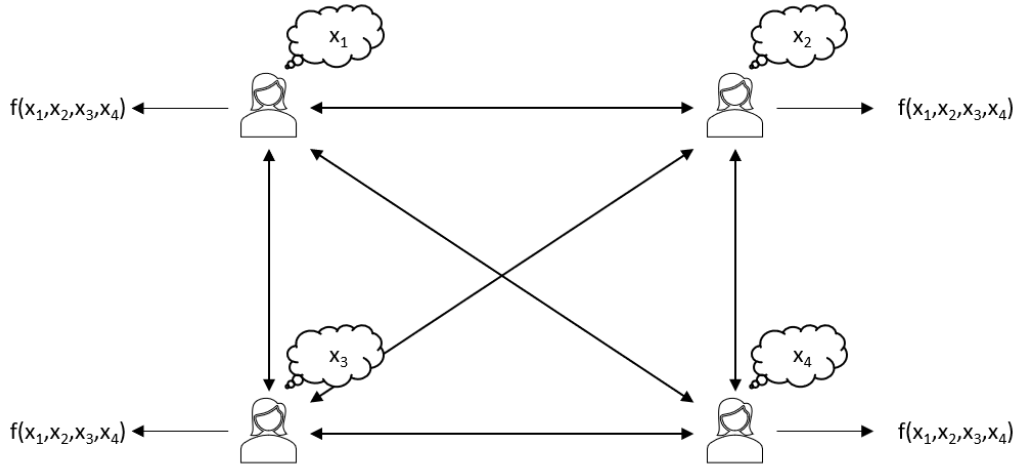


***Abb. 27** Übersichtsbild Multi-Party Computation*

Als illustratives Szenario kann hier beispielsweise an eine Auktion gedacht werden, bei der jeder Bieter ein Gebot macht. Am Ende der Berechnung soll das höchste Gebot gegenüber einem Auktionator offengelegt werden, wohingegen die Vertraulichkeit aller anderen Gebote während der gesamten Berechnung allen Mitbietenden und dem Auktionator gegenüber gewahrt werden soll.

Basierend auf vorherigen Arbeiten wurde Multi-Party Computation für allgemeine Berechnungen von Yao (Yao, 1982) sowie Goldreich, Micali und Wigderson (Goldreich et al., 1987) eingeführt, und seither laufend weiterentwickelt. Die Berechnungen basieren dabei meist auf Secret Sharing Methoden, bei denen die Eingabedaten in Fragmente zerlegt werden, sodass nur a priori definierte Teilmengen der Fragmente dazu verwendet werden können, die Eingabedaten wieder zu rekonstruieren, während jede andere Teilmenge nichts über die Eingabedaten lernt. Durch Verteilen der Fragmente an die einzelnen MPC Teilnehmer (sogenannte Nodes) wird nun, durch Ausnützung bestimmter strukturerhaltender Eigenschaften des Secret Sharing, eine verteilte Berechnung ermöglicht. Dabei erfolgt die Berechnung in Runden, sodass jeweils nach der Durchführung lokaler Berechnungen Zwischenergebnisse wieder in fragmentierter Weise verteilt werden.

Aus dieser nötigen Interaktivität bei Multi-Party Computation entsteht ein hoher Kommunikationsoverhead, welcher die Effizienz der Berechnungen signifikant reduziert. In den meisten Anwendungsszenarien werden daher Systeme mit lediglich drei MPC Nodes betrachtet, welche die Berechnungen durchführen. Im Fall einer Auktion könnten beispielsweise die MPC Nodes von Notaren betrieben werden, welche die bereits fragmentierten Gebote der Bietenden entgegennehmen, und anschliessend die eigentliche Auktion durchführen. Auf diese Weise wird die Vertraulichkeit der Gebote weiterhin gewährleistet, und gleichzeitig die Anzahl der nötigen Parteien während der Berechnung auf drei reduziert. Des weiteren hat dieser Ansatz den Vorteil, dass Asynchronität in dem Sinn erreicht werden kann, dass nicht alle Bietenden zum Zeitpunkt der Auktion online sein müssen, um selbst in der Berechnung teilzunehmen. Dieser Ansatz wurde beispielsweise in der ersten grossflächigen Anwendung von MPC bei der landesweiten Versteigerung von Zuckerrübenanbauflächen (Bogetoft et al., 2009) gewählt.

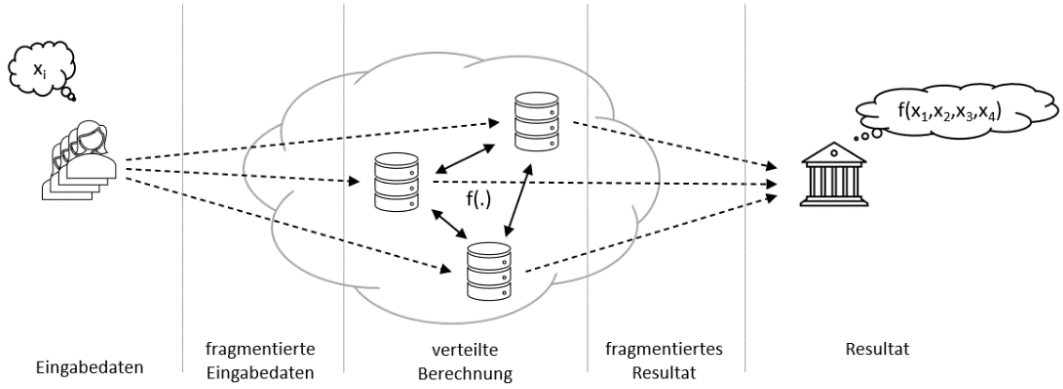


***Abb. 28** Typisches Setting in MPC Anwendungen*

Sicherheitseigenschaften

Die zentralen Sicherheitseigenschaften von Multi-Party Computation sind Vertraulichkeit der Daten und Integrität des Ergebnisses. Vertraulichkeit bedeutet, dass während der gesamten Berechnung keine Partei mehr Informationen über die Eingabedaten lernt, als vom für diese Partei vorgesehenen Ergebnis abgeleitet werden können. Andererseits bedeutet Integrität, dass dem Empfänger des Ergebnisses die korrekte Berechnung garantiert wird.

In der wissenschaftlichen Literatur können unterschiedliche formale Definitionen dieser Eigenschaften gefunden werden, welche durch Protokolle mit teils signifikant unterschiedlichen Laufzeiten instanziiert werden können. Dabei wird jeweils davon ausgegangen, dass höchstens ein definierter Anteil von MPC Nodes korrumpiert wird, und diese Nodes anschliessend kollaborieren. Dabei ist es unerheblich, ob die Korrumpierung bewusst (z.B. durch einen Systemadministrator) oder unbewusst (z.B. durch die Ausnützung einer Sicherheitslücke durch einen externen Angreifer oder ein Datenleck) zustande kommt. Ein korrumpierter Node wird als vollständig unter Kontrolle eines Angreifers stehend betrachtet, um höchstmögliche Sicherheitsgarantien geben zu können. Durch die Annahme der Kollaboration wird weiters insbesondere auch Sicherheit gegenüber unabhängig agierenden, korrumpierten Nodes gewährleistet.

In der Praxis erfordert die Annahme eines begrenzten Anteils korrumpierter Nodes, dass die Betreibenden der einzelnen MPC Nodes sorgfältig gewählt werden müssen, um Sicherheit zu erzielen. Insbesondere dürfen die einzelnen Nodes nicht von ein und derselben Entität kontrolliert werden.

Üblicherweise werden insbesondere die folgenden Eigenschaften in Angreifermodellen unterschieden:

- **Anzahl unehrlicher Nodes**: Wie erwähnt, können die Sicherheitseigenschaften von MPC nur garantiert werden, solange höchstens ein vordefinierter Anteil der MPC Nodes korrumpiert wird. Insbesondere die Unterscheidung, ob eine ehrliche Mehrheit an MPC Nodes angenommen wird oder nicht, führt zu unterschiedlichen Protokollen.
- **Passive vs aktive Angreifer**: Im passiven Angreifermodell wird davon ausgegangen, dass alle Parteien der Protokollspezifikation folgen, jedoch versuchen, aus den erhaltenen Daten möglichst viel Information über die Eingabedaten anderer Parteien zu folgern. Im Falle aktiver Angreifer wird davon ausgegangen, dass die kollaborierenden Nodes aktiv von der Protokollspezifikation abweichen, um dadurch die Vertraulichkeit und Integrität zu verletzen. Insbesondere muss im Fall einer unehrlichen Mehrheit sichergestellt werden, dass die Korrektheit jeglicher Ausgabe, die eine ehrliche Partei erhält, sichergestellt wird.
- **Informationstheoretische vs berechenmässige Sicherheit**: Die meisten kryptographischen Primitiven beruhen auf Annahmen, dass gewisse mathematische Probleme nicht effizient gelöst werden können, und bieten daher nur berechenmässige Sicherheit: sollte sich die Annahme als inkorrekt herausstellen und, z.B. mittels eines Quantencomputers oder durch neue Algorithmen effizient gelöst werden können, kollaboriert auch die Sicherheit des Verfahrens. Für MPC ist es dahingegen möglich, auch informationstheoretisch sichere Protokolle zu definieren, welche

unabhängig von den Möglichkeiten des Angreifers beweisbare Sicherheit garantieren, solange die definierte Anzahl unehrlicher Nodes nicht überschritten wird.

Es ist wichtig zu betonen, dass die Sicherheitsgarantien für MPC sich jeweils nur auf die Berechnungen innerhalb des MPC-Netzwerks beziehen. Insbesondere im Fall der Integrität bedeutet das, dass der Empfänger eines Ergebnisses die Authentizität und Integrität der Eingabedaten nicht überprüfen kann, sondern lediglich die Korrektheit der Berechnungen.

Einen möglichen Ausweg bietet hier die Kombination mit weiteren kryptographischen Methoden wie beispielsweise digitalen Signaturen und sogenannten Zero-Knowledge Proofs of Knowledge. Bei letzteren handelt es sich um Protokolle, welche es einer Partei erlauben, einer anderen Partei die Kenntnis über ein (kryptographisches) Geheimnis zu beweisen, ohne das Geheimnis selbst preiszugeben. Im Falle von MPC kann dies so eingesetzt werden, dass die Eingabedaten an der Quelle (z.B. auf Fahrzeugseite) signiert werden, und das MPC Netzwerk verifiziert die Signaturen in verteilter Form. Gemeinsam mit dem Resultat der Berechnung (z.B. zurückgelegte Distanz) berechnen die MPC Nodes einen Zero-Knowledge Proof, dass das Ergebnis von authentischen Daten korrekt abgeleitet wurde. Dadurch bekommt der Empfänger Ende-zu-Ende-Authentizitätsgarantien, ohne die Vertraulichkeit der Eingabedaten zu reduzieren.

Anwendungsmöglichkeiten

Aufgrund der Fortschritte insbesondere bezüglich der Effizienz von Multi-Party Computation wurden in den letzten Jahren zahlreiche Anwendungen vorgeschlagen und auch umgesetzt. Diese reichen von sogenannten Schlüsselzeremonien zum Erstellen von Parametern für Kryptowährungen, Auktionen, verteilter Datenanalyse, oder im Bereich der Shared Economy. Weitere geplante Anwendungen umfassen beispielsweise das Management von Slots im Flugverkehr.

In der Literatur wurden Konzepte für viele weitere Anwendungsszenarien hergeleitet wie beispielsweise vernetzte autonome Fahrzeuge (Li et al., 2019).

Standardisierung

Multi-Party Computation wird auf Grund seines Potentials derzeit in mehreren internationalen Gremien standardisiert. Nennenswerte Initiativen umfassen unter anderem die folgenden:

- Die Internationale Organisation für Normung (ISO) sowie die Internationale Elektrotechnische Kommission (IEC) erarbeiten derzeit eine Normenreihe zu MPC:
  - ISO/IEC 4922-2 Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing
  - ISO/IEC 4922-1 Information security — Secure multiparty computation — Part 1: General
- Die IEEE Standards Association veröffentlichte kürzlich Richtlinien zur Verwendung von MPC:
  - IEEE 2842-2021 - IEEE Recommended Practice for Secure Multi-Party Computation
- ITU Telecommunication Standardization Sector (ITU-T) veröffentlichte ebenfalls kürzlich aktualisierte Richtlinien zur Verwendung von MPC:
  - Technical Guidelines for Secure Multi-party Computation

4.2.2 Trusted Execution Environments

Das Ziel einer Trusted Execution Environment (TEE) oder sicheren Enklave ist das Schaffen einer Umgebung, welche sensitive Daten und Code vor Zugriff durch aussenstehende Prozesse, inklusive des Betriebssystems, schützt. Es handelt sich dabei um eine Hardwareerweiterung, welche das vertrauenswürdige Ausführen von Berechnungen innerhalb einer ansonsten potentiell nicht vertrauenswürdigen Umgebung erlaubt. In einer Trusted Execution Environment werden die Vertraulichkeit, die Authentizität des ausgeführten Programmcodes sowie die Integrität der ausgeführten Berechnungen garantiert. Um diese Ziele zu erreichen, ist eine strikte Isolierung aller relevanten Teile eines Systems, inklusive der verwendeten Hardware, notwendig, welche durch kryptographische Methoden wie

digitale Signaturen sichergestellt wird. Die in einer TEE laufenden vertrauenswürdigen Anwendungen haben dabei Zugriff auf die volle Leistung eines Geräts, inklusive allfälliger Peripheriegeräte.

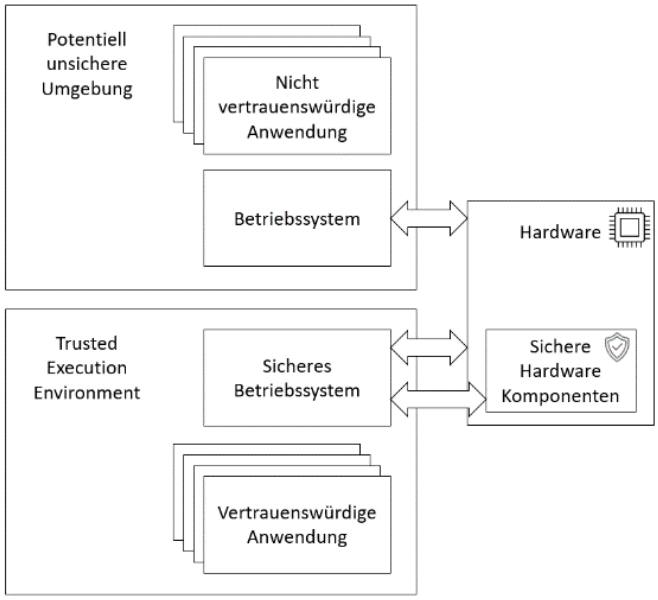


***Abb. 29** Übersichtsbild Trusted Execution Environments*

Um eine allfällige Simulation der sicheren Hardware durch von einem Angreifer kontrollierte Software zu vermeiden, basieren TEEs auf hardwaregebundenen Vertrauensankern. Diese enthalten geheime kryptographische Schlüssel, die bei der Produktion erstellt werden, und auch bei einer Hardware-Rücksetzung nicht mehr geändert werden können. Weiters enthalten die Vertrauensanker die öffentlichen Schlüssel einer vertrauenswürdigen Partei, welche die Firmware signieren muss, um eine sichere Umgebung garantieren zu können. Zum Beispiel wird durch die Verwendung von physisch nicht-klonbaren Funktionen (PUFs) meist sichergestellt, dass jedes Gerät über einzigartige kryptographische Schlüssel verfügt. Dadurch wird erreicht, dass selbst im unwahrscheinlichen und aufwendigen Fall des erfolgreichen Auslesens eines Vertrauensankers die Integrität und Vertraulichkeit anderer Geräte nicht betroffen sind.

Sicherheitseigenschaften

Trusted Execution Environments geben hohe Garantien bezüglich Integrität und Vertraulichkeit von Daten und Anwendungen. Dennoch wurde in den vergangenen Jahren eine Vielzahl von akademischen sowie praktischen Angriffen gegen spezifische Implementierungen entwickelt, welche ausserhalb des bei der Implementierung betrachteten Angreifermodells liegen. Beispielsweise können spekulative Ausführungen, bei denen aktuell untätige Prozessor-Ressourcen Ergebnisse für mögliche künftige Schritte eines Programmablaufs vorberechnen, um dadurch die Effizienz des Systems zu verbessern, dazu führen, dass durch sogenannte Seitenkanalangriffe Informationen über sensible verarbeitete Daten abgeleitet werden können. Bei derartigen Angriffen wird ausgenützt, dass sich ein physisches System, abhängig von den verarbeiteten Daten, unterschiedlich verhält, z.B. in Hinblick auf die Laufzeit oder Stromverbrauch. Zu den bekanntesten Vertretern dieser Klasse gehören unter anderem die unterschiedlichen Versionen des Spectre-Angriffs (Kocher et al., 2019) auf Intel SGX, z.B. SgxPectre und SgxSpectre. Andere Typen von Angriffen nützen Sprungvorhersagen oder das Cache-Verhalten von Prozessoren, um die Sicherheit durch Seitenkanäle zu unterminieren (Borrello et al., 2022; Nilsson et al., 2020).

Anwendungsmöglichkeiten

Die Anwendungsbereiche der durch diese strikte Trennung erhöhten Sicherheit sind vielseitig, und umfassen die Absicherung von Zahlungsprozessen, digitalen Identitäten, die Analyse, Übertragung, und Speicherung von IoT Anwendungen, oder die Absicherung von Premiuminhalten beim Management von digitalen Rechten.

Standardisierung

Die von GlobalPlatform entwickelten Standards für Trusted Execution Environments umfassen insbesondere die relevanten Schnittstellen, Schutzprofile, sowie Management Richtlinien:

- TEE Internal Core API Specification
- TEE Client API Specification
- TEE Protection Profile
- TEE Management Framework: Open Trust Protocol

Die meisten relevanten Chiphersteller bieten Hardwareunterstützung für Trusted Execution Environments an, und entsprechende sichere Betriebssysteme werden jeweils von unterschiedlichen Herstellern angeboten.

4.2.3 Vollhomomorphe Verschlüsselung

Viele in der Praxis eingesetzte Verschlüsselungsverfahren unterstützen, oft aufgrund anderer Sicherheitsanforderungen an das System, keine Berechnungen auf den verschlüsselten Daten. Sie eignen sich daher zur Absicherung für Data at Rest sowie Data in Transit, jedoch nicht für Data in Use.

Andererseits bietet eine Vielzahl an Verfahren die Möglichkeit, eine algebraische Operation auf verschlüsselten Daten durchzuführen. Bei diesen sogenannten partiell-homomorphen Verfahren ist es zum Beispiel möglich, durch Berechnungen auf verschlüsselten Daten (sogenannten Chiffraten) Zahlenwerte in den darin enthaltenen Klartexten zu addieren.

2009 wurde das erste vollhomomorphe Verschlüsselungsverfahren (Fully Homomorphic Encryption, FHE) vorgestellt (Gentry, 2009). Durch die Ermöglichung zweier algebraischer Operationen (z.B. Addition und Multiplikation) erlaubt FHE, beliebige Berechnungen in der verschlüsselten Domäne durchzuführen. Dies erlaubt insbesondere die Auslagerung von Berechnungen in nicht-vertrauenswürdige Cloudumgebungen, da die Vertraulichkeit der Daten nicht unterminiert wird.

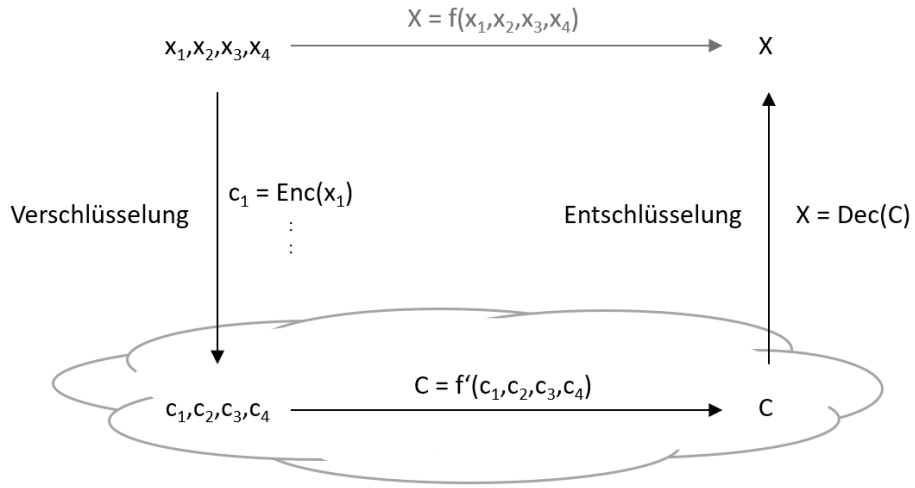


Abb. 30 *Übersichtsbild Vollhomomorphe Verschlüsselung*

Aufgrund des bekannten Designmusters für vollhomomorphe Verschlüsselung ist meist eine beliebige Anzahl einer algebraischen Operation (z.B. Addition) möglich, während jede Anwendung der zweiten Operation (z.B. Multiplikation) die Qualität des Chiffrats verschlechtert, und nach zu vielen Anwendungen eine Entschlüsselung verhindert. Um dieses Problem zu umgehen, muss in regelmässigen Abständen ein sogenannter Bootstrapping-Schritt durchgeführt werden, der die Qualität des Chiffrats wieder zurücksetzt, ohne dabei die Vertraulichkeit zu verletzen. Dieser Schritt hat stets hohe negative Auswirkungen auf die Gesamteffizienz des Verfahrens, sodass die in praktischen Anwendungen evaluierbaren Funktionen stark von deren Struktur abhängen, und die Einsatzbarkeit von FHE derzeit entsprechend noch auf einer Fall-zu-Fall Basis zu evaluieren ist.

Sicherheitseigenschaften

Vollhomomorphe Verschlüsselung bietet hohe Garantien bezüglich der Vertraulichkeit der Daten. Im Gegensatz zu MPC müssen keine Annahmen bezüglich der Anzahl möglicherweise korrumpierter Parteien gemacht werden, und es besteht kein Bedarf für Vertrauensanker wie bei TEEs.

Allerdings bietet FHE keine Garantien bezüglich der Integrität der Berechnung. Dieser Nachteil gegenüber den vorangegangenen Technologien wird in aktuellen Forschungsprojekten adressiert, welche das neue Konzept verifizierbarer FHE betrachten, jedoch noch nicht praktisch einsetzbar sind.

Anwendungsmöglichkeiten

Vollhomomorphe Verschlüsselung hat im Gegensatz zu den vorherigen Technologien den Nachteil, dass alle Klartexte unter einem zentralen Schlüssel verschlüsselt werden müssen.

Einerseits bedeutet dies, dass in einem kollaborativen Szenario alle Daten bereits für den späteren Empfänger verschlüsselt werden müssen und dieser nicht dynamisch gewählt werden kann. Dies wird durch sogenannte Multi-Key FHE Verfahren (López-Alt et al., 2012) adressiert, bei denen Chiffrate verschiedener Eigentümer kombiniert werden können, jedoch entsprechender Interaktion zur Entschlüsselung des Resultats bedürfen, sodass Asynchronität nur bedingt erreicht werden kann.

Um Vertraulichkeit in einem kollaborativen Szenario mit nur einem zentralen Schlüssel zu erreichen, muss weiters sichergestellt werden, dass der Empfänger keinen Zugriff auf die einzelnen Chiffrate erhält, sondern lediglich auf das Ergebnis der Berechnung.

Trotz vielversprechender Eigenschaften beschränken diese Limitierungen die Einsatzmöglichkeiten von FHE zum Sicherstellen der Vertraulichkeit im Kontext von Smart Mobility-Anwendungen auf spezifische Anwendungen.

Standardisierung

Vollhomomorphe Verschlüsselung ist ein aktives Forschungsgebiet. Während Implementierungen ausgewählter Verfahren öffentlich zugänglich sind, existieren derzeit noch keine Standards internationaler Standardisierungsgremien.

- Eine nennenswerte Ausnahme bildet die Homomorphic Encryption Standard Community-Standard Initiative, welche erste Schritte in Richtung Standardisierung von FHE gesetzt hat:
    - Homomorphic Encryption Security Standard

5 Design eines Governance-Modells

5.1 Governance-Modell

5.1.1 Vorbemerkungen

Hauptziel des Projekts ist es, ein **Governance-Modell** für den Mobilitätsbereich zu entwikkeln, aus dem sich Empfehlungen für den Umgang mit den für die Smart Mobility-Anwendungen notwendigen Daten ergeben. Die Vorarbeiten haben gezeigt, dass sich im Mobilitätsbereich vielfältige Mobilitätsangebote mit etlichen Smart Mobility-Anwendungen herausgebildet haben (siehe Abb. 13), die sich rasch weiterentwickeln und zahlreiche Gemeinsamkeiten aufweisen. Insbesondere nehmen die beteiligten Akteure in allen Smart Mobility-Anwendungen vergleichbare Aufgaben ein (siehe Kap. 2.2). Allerdings bestehen zwischen den Mobilitätsangeboten auch wesentliche Unterschiede. Der Markt ist zudem sehr zersplittert und gesamthaft der Marktanteil an Smart Mobility Anwendungen weiterhin sehr klein, hinzu kommt, dass mit den zugrundeliegenden eigentlichen Transportdienstleistungen kaum oder kleine Margen erzielt werden.

Aus der Literatur ergeben sich zahlreiche Anhaltspunkte, welche Prinzipien im Zusammenhang mit der multilateralen Governance zu berücksichtigen sind (EDRM, 2021; Kooper et al., 2011; UN, 2009; Wimmer et al., 2018). Im Bereich der Mobilität und für Smart Cities werden dabei weitere Prinzipien und Elemente, spezifisch auch für Data Governance und Management, genannt (EOSC, 2019; Michael et al., 2019; Paskaleva et al., 2017).

Entscheidend ist indes vor allem, dass Governance für Smart Mobility-Anwendungen drei ineinandergreifende und interagierende Aspekte, nämlich rechtliche, organisatorische, und technische umfasst (siehe Grafenstein, 2022, S. 16 ff.) zwischen denen sich Wechselwirkungen ergeben:

Rechtliche Aspekte der Governance

Aus rechtlicher Sicht umfasst ein Data Governance-Modell verschiedene *Regulierungsinstrumente*. Denkbar ist etwa der Einsatz von Behörden, die mit bestimmten Befugnissen (zur Aufsicht, Bewilligung oder Kontrolle) ausgestattet werden. Regulierungsinstrumente bilden aber auch Rechtsvorschriften im Sinne von Ge- oder Verboten. Darüber hinaus können auch Marktmechanismen verwendet werden, um bestimmte Ziele zu erreichen, wobei die Marktkräfte mit gezielten Anreizen beeinflusst werden können.

Weiter können die im Zusammenhang mit einem Data Governance-Modell stehenden Regeln auf verschiedenen *Regulierungsstufen* stehen. Unterschieden werden können zwingende Gesetzes- und/oder Verordnungsbestimmungen, regulierte Selbstregulierung, Selbstregulierung und blosse Empfehlungen.

Wo sich keine (starren) und eindeutigen rechtlichen Regeln aufstellen lassen, weil diese nicht alle Einzelfälle befriedigend lösen, können im Data Governance-Modell stattdessen *rechtliche Prinzipien* hilfreich sein, aus denen sich sachgerechte Lösungen entwickeln lassen. Unabhängig vom vorgeschlagenen Data Governance-Modell muss nach dessen Implementierung untersucht werden, wie es in der Praxis auf den Datenmarkt und das Mobilitätsökosystem auswirkt (*Wirkungskontrolle*).

Organisatorische Aspekte der Governance:

Die organisatorische Governance stellt innerhalb des vom Recht gesetzten Rahmens die Entscheidungsprozesse sicher und regelt die jeweiligen Zuständigkeiten und Verantwortlichkeiten. Um diese für Smart Mobility-Anwendungen zu definieren, braucht es eine passende Form der Organisation.

Unabdingbar ist ein Kontrollorgan welches die Interessen sämtlicher Stakeholder (siehe Kap. 2.5.2) berücksichtigt, die gesamte Mobilitätslandschaft der Schweiz widerspiegelt und die Regeln für die Partizipation festlegt und kontrolliert (z.B. betreffend Wahlen von Gremien oder Aufsichtsorganen). Diese Aufgabe kann durch einen anerkannten neutralen Custodian oder ein Multistakeholder-Forum (mehr hierzu im Kap. 5.2.4) wahrgenommen werden. In Bezug auf die Datennutzung und Datenweitergabe muss es die

organisatorische Governance ermöglichen, Berechtigungen für den Zugriff auf und die Verarbeitung von Daten zu erteilen oder abzulehnen. Dies stellt sicher, wer wann auf welche Daten zugreifen darf. Weiter regelt sie den Ort und die Bedingungen der Datenverarbeitung.

Technische Aspekte der Governance

Mit technischen Mitteln können Berechtigungen für Datenzugriff und Datenverarbeitung verwaltet werden, womit sich Schnittstellen zu organisatorischen und rechtlichen Aspekten ergeben. Über kryptographische Mechanismen kann zudem sichergestellt werden, dass Daten nur bestimmten Berechtigten zugänglich sind und diese auch nur insofern bearbeitbar sind, wie die Berechtigungen es erlauben. Überdies kann die technologische Nachvollziehbarkeit von Datenzugriffen und Datenbearbeitungen gewährleistet werden.

Mit technischen Standards kann die korrekte Umsetzung der Rechtslage garantiert werden und zugleich ein "Beweis/Nachweis" erbracht werden, dass die Technik rechtskonform arbeitet. Dazu gehört auch die Auditierbarkeit der Implementierung. In diesem Zusammenhang hat die technische Governance auch die Kompatibilität mit bestimmten Standards zu regeln.

Technische Governance bedeutet aber auch die Festlegung von Systemarchitekturen oder das Fällen von Grundsatzentscheiden, etwa zur zentralen oder dezentralen Speicherung oder Berechnung.

5.1.2 Generisches Modell

Unter Berücksichtigung dieser Vorgaben verstehen wir unter einem **Governance-Modell** die *Gesamtheit aller Normen und Bedingungen, die für das Funktionieren einer Smart Mobility-Anwendung massgebend sind*. Dabei können die Normen sowohl technischer als auch organisatorischer Natur sein, und sie können durch normative Verweisung Teil der Gesetzgebung werden. Zu den Bedingungen gehören die Wirtschaftlichkeit eines Mobilitätsangebots sowie als elementarer Aspekt das zwischen den Akteuren notwendige Vertrauen.

Das Governance-Modell identifiziert zunächst die bestehenden Akteure (1). Dies trägt zu organisatorischen Aspekten der Governance (Kap. 5.1.1) bei und erlaubt die notwendigen Zuständigkeiten und Verantwortlichkeiten zu regeln. Anschliessend thematisiert es die Verwendung der für den Datenaustausch notwendigen Infrastruktur (2), um die technischen Aspekte der Governance in Bezug auf Verwaltung von Datenzugriff und Datenverarbeitung zwischen den Akteuren sicherzustellen. In einem dritten Schritt wird der geltende rechtliche Rahmen untersucht, welcher die Mobilitätsanwendung möglicherweise einschränkt (3). Dadurch können sowohl bestehende Regulierungsinstrumente als auch potentielle Lücken und normativer Anpassungsbedarf identifiziert werden. Das schafft eine Grundlage, auf welcher sich die rechtlichen Aspekte der Governance abstützen. In einem letzten Schritt geht es dann um den eigentlichen Kern – die Data Governance – und damit um den konkreten Umgang mit Mobilitätsdaten. Mittels eines detaillierten Analyserasters kann ermittelt werden, welche technischen, rechtlichen oder organisatorischen Prinzipien bzw. Regeln in Bezug auf die konkrete Mobilitätsanwendung erforderlich sind (4. bzw. 4.1 – 4.4).

Die Akteure, die Infrastruktur und der geltende Rechtsrahmen bilden die Grundsätze im entwickelten Modell. Diese stehen untereinander in Abhängigkeit. Diese werden in den ersten drei Schritten des Governance-Modells geklärt und entsprechend abgegrenzt. Basierend darauf können im vierten Schritt die zusätzlichen Massnahmen festgelegt werden, um die Data Governance einer Smart Mobility-Anwendung sicherzustellen. Dieser Schritt spezifiziert folglich die Gesamtbetrachtung auf einer detaillierteren Ebene, ohne Anpassung der ersten drei Schritte.

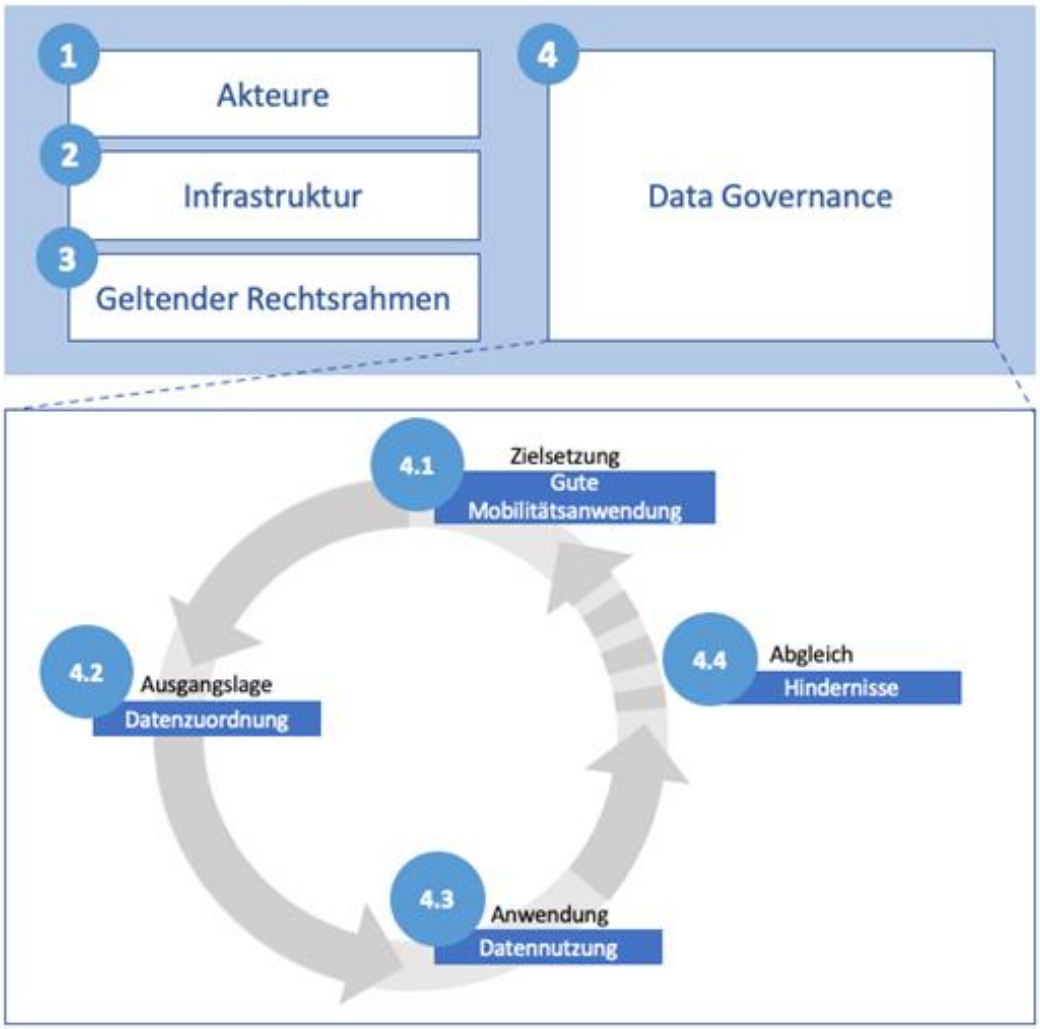


Abb. 31 *Schematische Darstellung des Governance-Modells*

5.1.3 Auswahl der Smart Mobility-Anwendungen

Dieses generische Governance-Modell wird im Rahmen des Projekts anhand zweier exemplarischer Smart Mobility-Anwendungen angewendet und damit gleichzeitig auf dessen Anwendbarkeit geprüft. Daraus ergibt sich, ob und inwieweit das Modell in Bezug auf alle Mobilitätsanwendungen verallgemeinerungsfähig ist. Die Auswahl der exemplarischen Mobilitätsanwendungen erfolgte anhand zweier Kriterien:

- **Zukunftspotential:** Untersucht werden sollen vor allem Mobilitätsanwendungen, die das Potenzial haben, die Mobilitätslandschaft in der Schweiz künftig nachhaltig zu beeinflussen.
- **Impulse durch DAGSAM:** Untersucht werden sollen vor allem Mobilitätsanwendungen, in Bezug auf welche dieses Projekt tatsächlich Impulse für die Data Governance liefern könnte. Für Mobilitätsanwendungen die international vorangetrieben werden, wie z.B. die Zulassung automatisierter Fahrzeuge, ist diese Beeinflussbarkeit gering. Für Anwendungen, die sich hauptsächlich im nationalen Kontext etablieren könnten wie z.B. MaaS oder RUC, ist die Beeinflussbarkeit gross, da es der Schweiz weitgehend freisteht, die Rahmenbedingungen eigenständig festzulegen.

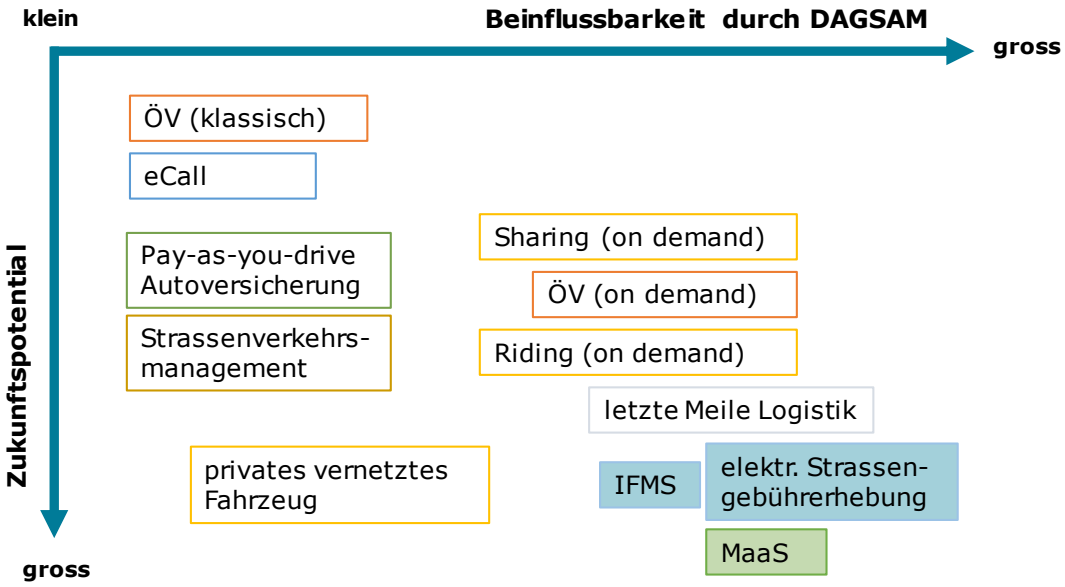


***Abb.* 32** Auswahlraster zur Vertiefung der Smart Mobility-Anwendungen im Rahmen von DAGSAM

Anhand dieser Kriterien hat das Projektteam – unterstützt durch die Begleitkommission – die Smart Mobility-Anwendungen "Mobility-as-a-Service (MaaS)" und "elektronische Strassengebührenerhebung (RUC)" gewählt und zwar in dieser Reihen- bzw. Prioritätenfolge.

MaaS deckt diesbezüglich viele Anwendungen aus den Mobilitätsangeboten der individuellen und der kollektiven Fahrzeugnutzung sowie der Plattformen (vgl. dazu die Einführung zu Mobilitätsangebote und Smart Mobility-Anwendungen in Kap. 2.1) ab.

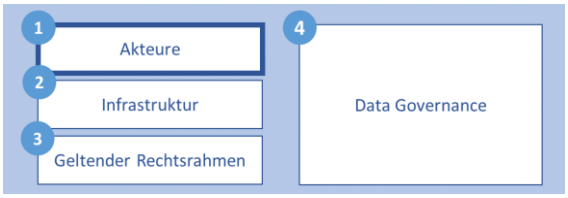
Die Smart Mobility-Anwendung Strassengebührenerhebung deckt ihrerseits zudem Aspekte der sog. die Integrated Fare Management Systeme (IFMS) bzw. des Mobility Pricing und somit der Gebührenerhebung im Allgemeinen ab. In sämtlichen Anwendungen werden anhand der satellitengestützten Geolokalisation (GNSS) Personen bzw. Fahrzeuge eindeutig identifizierbar.

Der grösste Unterschied zwischen diesen beiden Anwendungen liegt in der Rolle der öffentlichen Hand. Während bei MaaS-Angeboten die Rolle des Gemeinwesens nicht von vornherein festgelegt ist, agiert es bei der Gebührenerhebung zwingend als "Geldeintreiber" und verarbeitet dabei typischerweise personalisierte Nutzungsdaten.

Entsprechend wird in Kap. 5.2 ein Governance-Modell für Mobility-as-a-Service (MaaS) und in Kap. 5.3 für die Gebührenerhebung entwickelt. Aus beiden untersuchten Mobilitätsanwendungen lassen sich sodann gemeinsame Erkenntnisse gewinnen und das entwickelte Governance-Modell evaluieren.

5.2 Governance von Mobility-as-a-Service (MaaS)

5.2.1 Akteure



Am MaaS-Konzept sind mehrere Akteure beteiligt. Wie bei allen Mobilitätsanwendungen zählen der **Leistungserbringer** (hier: der Mobilitätsdienstleister), der **Nutzer** (hier: die Mobilitätsnachfrager) und der **Vermittler** (hier: der MaaS-Anbieter bzw. die MaaS-Plattform) (engl. MaaS service provider oder MaaS operator) dazu (Kamargianni & Matyas, 2017, S. 4). Die Rechtsnatur des MaaS-Anbieters kann dabei unterschiedlich ausgestaltet sein. Entweder handelt der Staat selbst bzw. eine Anbieterin des öffentlichen Verkehrs mit staatlicher Beteiligung oder eine Anbieterin aus der Privatwirtschaft ist tätig (Hensher et al., 2020, S. 99 f.; Kamargianni & Matyas, 2017, S. 4 f.).

Der **Regulator** als übergeordneter abstrakter Akteur hat die Aufgabe die Spielregeln und Rahmenbedingungen festzulegen, diese zu kontrollieren und allenfalls durchzusetzen. Für die Verkehrsplanung und -überwachung sowie Verkehrsgesetzgebung im Zusammenhang mit MaaS ist dies die jeweilige staatliche Behörde. Zudem können die MaaS-Anbieter und Mobilitätsdienstleister in Branchenübereinkünften im Sinne der Selbstregulierung tätig werden. Auch alle im MaaS-Kontext entwickelten Normen werden im Rollenmodell dem Regulator zugeordnet.

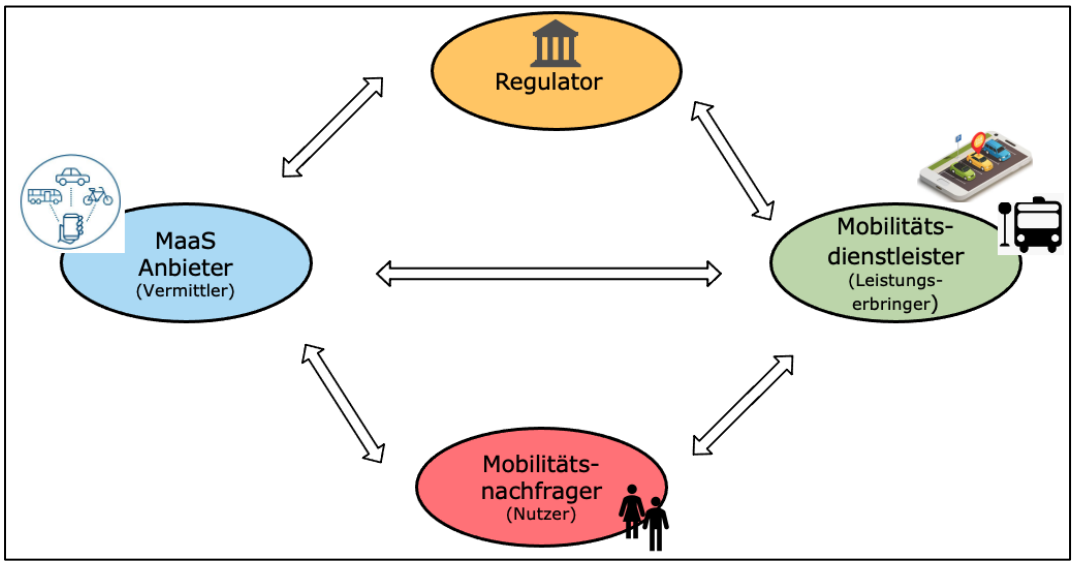
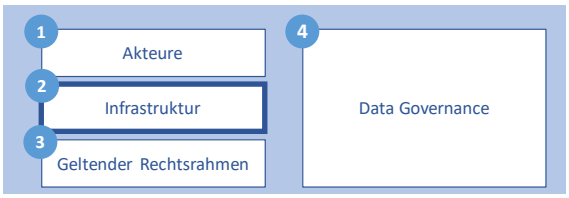


***Abb. 33** Rollenmodell bei MaaS*[13]

5.2.2 Dateninfrastruktur(en)



Maas benötigt eine sog. (Mobilitäts-)Dateninfrastruktur, in der Daten über die Smart Mobility-Anwendungen von Mobilitätsdienstleistern sowie weitere Daten (z.B. Geodaten) gesammelt werden, um so den Betrieb, die Entwicklung und das Management von MaaS durch MaaS-Anbieter zu ermöglichen und zu vereinfachen (Kamargianni & Matyas, 2017, S. 8 f.). Die Marktordnung hinsichtlich solcher Dateninfrastrukturen im Zusammenhang mit MaaS kann dabei unterschiedlich ausgestaltet werden (siehe hierzu auch Grafenstein, 2022, S. 21 ff.):

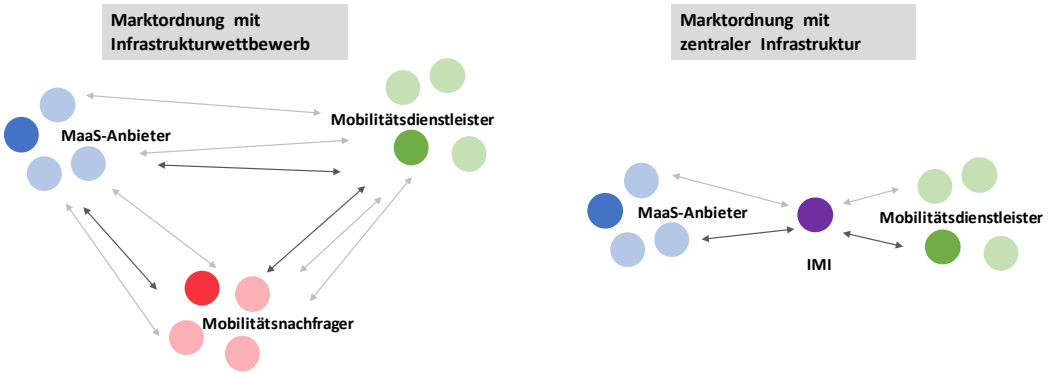


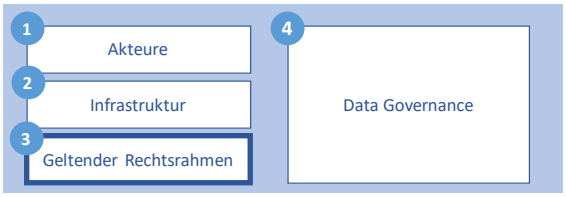
***Abb. 34** Die zwei unterschiedlichen Konzepte betr. MaaS-Dateninfrastruktur*

[13] Quellen der Symbole: https://commons.wikimedia.org/wiki/File:Bus_stop_symbol.svg, https://www.dekra-solutions.com/2020/06/carsharing-die-mobilitaet-der-zukunft/, https://www.data-infrastructure.eu/GAIAX/

Unterschieden werden einerseits **Marktordnungen mit Infrastrukturwettbewerb**, bei denen ein MaaS-Anbieter allein oder mehrere MaaS-Anbieter zusammen eine (dezentrale) Mobilitätsdateninfrastruktur betreiben. Bei einem solchen Marktdesign besteht der Wettbewerb also nicht nur im Bereich des Mobilitätsangebots der MaaS-Anbieter, sondern auch auf der Infrastrukturebene. Für solche Marktordnungen spricht grundsätzlich, dass der Wettbewerb auf der Infrastrukturebene Anreize bieten kann, möglichst gute (technische) Lösungen zu entwickeln. Allerdings bestehen zum heutigen Zeitpunkt Bedenken, ob dieser Wettbewerb zielführend ist – oder sich überhaupt erst etabliert. Denn gegenwärtig scheint es, also würden MaaS-Anbieter in der Schweiz nicht die kritische Masse erreichen können, die den Betrieb mehrerer konkurrierender Plattformen erlaubt. Besteht ein Wettbewerb auf der Infrastrukturebene, dürften sich zudem auf absehbare Zeit auch kaum Regeln herausbilden, welche die effiziente Datennutzung ermöglichen. Aller Voraussicht nach würde sich in Bezug auf jede Plattform unterscheiden, welche Daten die Mobilitätsdienstleister in welchen Formaten und zu welchem Preis bekanntgeben. Die damit verbundenen Kosten für die passende Aufbereitung der Daten und die Aushandlung passender Bedingungen in Bezug auf mehrere MaaS-Anbieter wären derart hoch, dass sich unter den MaaS-Anbietern entweder rasch ein Monopolist etablieren oder die Mobilitätsdienstleister ganz auf die Zusammenarbeit mit MaaS-Anbietern verzichten würden. Zudem besteht das Risiko, dass MaaS-Anbieter sich lediglich auf bestimmte einzelne Smart Mobility-Anwendungen (z.B. ausgewählte Arten von Verkehrsmittel) und Regionen (z.B. urbane Räume) fokussieren, was zu einer unerwünschten Fragmentierung der verschiedenen Anwendungen führen und das Mobilitätsökosystem schädigen könnte, weil kein flächendeckendes MaaS-Angebot existiert.

MaaS-Marktordnungen können andererseits auf einer **zentralen Infrastruktur** aufbauen. Mit der Schaffung eines sog. "Intermediary MaaS Integrator (IMI)" (auch Data Provider oder Platform Service Provider) bzw. einer zentralen Mobilitätsdateninfrastruktur können die Datentypen der Angebotsbeschreibung (wie z.B. die Verkehrsinfrastruktur als georeferenzierte Daten in einem Bezugsrahmen oder die Angebote von Mobilitätsdienstleistern als Betriebs- und Vertriebsdaten) zentral und einheitlich standardisiert gesammelt und bezogen werden (Smith et al., 2020). Über den IMI können die MaaS-Anbieter die Daten über die Angebote von Mobilitätsdienstleistern mit den Nutzeranfragen zusammenführen. Der Begriff der zentralen Infrastruktur impliziert dabei weder eine technische Lösung noch ein bestimmtes Vorverständnis der verwendeten technischen Architektur. Er macht allerdings klar, dass auf der Infrastrukturebene kein Wettbewerb gewünscht ist. Eine zentrale Infrastruktur schafft deswegen per se eine Art technischen Flaschenhals, dessen Benutzung aus Sicht der Wettbewerber unverzichtbar ist (im Kartellrecht ist in Bezug auf solche Infrastrukturen in Anlehnung an die sog. "essential facility doctrine" von einer "wesentlichen Einrichtung" die Rede). Die mit dieser Ausgangslage einhergehenden kartellrechtlichen Bedenken lassen sich jedoch zerstreuen, wenn allen Wettbewerbern unter diskriminierungsfreien Bedingungen Zugang zur Nutzung dieser Plattform gewährt wird. Unter dieser Voraussetzung ist nämlich dennoch Wettbewerb möglich. Bloss findet er nicht auf der Ebene der Infrastruktur, sondern – umso mehr – auf der Ebene der Dienstleistungen, d.h. der Preise und der Qualität der Leistungen statt; und zwar jeweils sowohl in Bezug auf die Angebote der MaaS-Anbieter als auch auf jene der Mobilitätsdienstleister. Weil für das Funktionieren von MaaS der Einbezug möglichst vieler Anbieter notwendig ist, fällt ins Gewicht, dass bei einer Marktordnung mit zentraler Infrastruktur, die für das Funktionieren des Systems notwendige kritische Masse an Anbietern und Nachfragern leichter erreicht werden dürfte. Zentral ist weiter, dass sich so einheitliche Regeln für die Datennutzung festlegen lassen, insbesondere was die Datenqualität und die Gegenleistung für das Bereitstellen von Daten betrifft. In diesem Element der zentralen Planung liegt gleichzeitig die grösste Schwierigkeit der Marktordnung mit zentraler Infrastruktur: Wie können allgemeingültige Regeln festgelegt werden, die von allen Akteuren akzeptiert werden und die das notwendige Vertrauen in das System gewährleisten? Diese wesentlichen Fragen werden im Rahmen der Ausführungen zu den Elementen des Data-Governance-Modells erneut aufgegriffen (siehe Kap.5.2.4).

5.2.3 Geltender Rechtsrahmen



Multimodales Reisen ist ein neueres Phänomen. Entsprechend muss davon ausgegangen werden, dass der geltende Rechtsrahmen in der Schweiz (noch) auf unimodales Reisen zugeschnitten ist – oder der Gesetzgeber beim Erlass der relevanten Bestimmungen zumindest implizit davon ausging, unimodales Reisen zu regulieren. Vor diesem Hintergrund ist denkbar, dass der bestehende Rechtsrahmen MaaS-Angebote nicht berücksichtigt, erschwert oder gar verhindert. Folglich ist in einem Governance-Modell für MaaS zu prüfen, ob eine Anpassung des bestehenden Rechtsrahmens notwendig ist. Nachfolgend sind in diesem Sinne einige rechtliche Einzelfragen aufzuzeigen, die es im Zusammenhang mit der Etablierung von MaaS zu klären gilt.

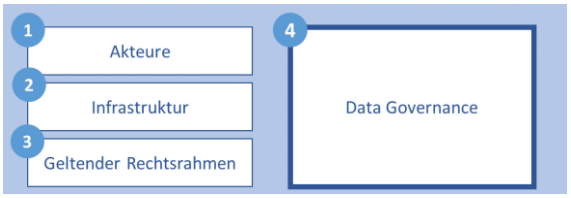
Drei Beispiele zeigen auf, dass das MaaS-Konzept in vielerlei Hinsicht nicht in den bestehenden Rechtsrahmen passt und dass künftig punktuell gesetzliche Anpassungen notwendig sind, um den MaaS-Angeboten zum Durchbruch zu verhelfen:

- Erstens bestehen die **Passagierrechte** des Personenbeförderungsgesetzes PBG (Anspruch auf Weiterfahrt, Fahrpreiserstattung, Fahrpreisentschädigung, Unterstützung, Haftung für Unterkunfts- oder Verpflegungskosten) nur, soweit ein Mobilitätsnachfrager mit einem konzessionierten Transportunternehmen reist (Art. 21 ff. PBG). Setzt sich eine multimodale Reise aus Leistungen von konzessionierten und nichtkonzessionierten Mobilitätsdienstleistern zusammen, entsteht aus rechtlicher Sicht eine uneinheitliche und bisweilen auch unübersichtliche Situation. Die reisende Person hat in Bezug auf die einzelnen Reiseabschnitte jeweils andere (vertragliche oder gesetzliche) Ansprüche bzw. Rechte.
- Wie bei den Passagierrechten orientiert sich zweitens auch die Geltung der **Behindertengleichstellungsrechte** (BehiG; VböV; VAböV) am rechtlichen Status des jeweiligen Transportunternehmens. Die Behindertengleichstellungsrechte stellen funktionale Anforderungen an die Einrichtungen, die Fahrzeuge und die Dienstleistungen des öffentlichen Verkehrs, so dass behinderte Personen, die in der Lage sind, den öffentlichen Raum autonom zu benützen, auch Dienstleistungen des öffentlichen Verkehrs selbstständig beanspruchen können. Sowohl in Bezug auf die Passagierrechte als auch in Bezug auf die Behindertengleichstellungsrechte zeigt sich: Setzt sich eine multimodale Reise aus Leistungen von konzessionierten und nichtkonzessionierten Mobilitätsdienstleistern zusammen, entsteht aus rechtlicher Sicht eine uneinheitliche und bisweilen auch unübersichtliche Situation. Die reisende Person hat in Bezug auf die einzelnen Reiseabschnitte jeweils andere (vertragliche oder gesetzliche) Ansprüche bzw. Rechte.
- Schliesslich kann auch das zwingende (**Konsumenten-)Recht** ein Hindernis für MaaS-Angebote darstellen. Die **Preisbekanntgabeverordnung** (PBV [SR 942.211] i.V.m. Art. 16 ff. UWG) sieht nämlich für bestimmte Dienstleistungen eine Pflicht zur vorgängigen Bekanntgabe von Preisen vor, namentlich für das Taxigewerbe (Art. 10 lit. f PBV), die Vermietung von Fahrzeugen (Art. 10 lit. h PBV), für Flug- und Pauschalreisen (Art. 10 lit. n PBV) oder für die mit der Buchung einer Reise zusammenhängenden und gesondert in Rechnung gestellten Leistungen wie Buchung, Reservation und Vermittlung (Art. 10 lit. o PBV). Werden solche Transportdienstleistungen in einem MaaS-Angebot integriert, schränkt dies das Geschäftsmodell des MaaS-Dienstes ein. Der Preis kann nämlich nicht mehr über sog. Integrated Fare Management Systems (IFMS) – wie z.B. FAIRTIQ – festgelegt werden, weil bei diesen der (Best-)Preis bewusst erst am Ende einer Reise berechnet wird (vgl. Thouvenin, 2016, S. 12 ff. zur Vereinbarkeit der dynamischen Preisgestaltung mit der Pflicht zur Preisbekanntgabe). Keine Einschränkungen dürften sich dagegen aus dem ebenfalls dem Konsumentenschutzrecht zugehörigen **Pauschalreisegesetz** (PauRG [SR 944.3]) ergeben.[14] Als Pauschalreise gelten nämlich nur touristische Reiseleistungen, die aus einer im Voraus festgelegten Verbindung von mindestens zwei Reiseleistungen bestehen. Die Pauschalreise muss zudem zu einem Gesamtpreis

[14] Zu anders lautenden Befürchtungen vorn Kap. 2.5.1 (SOB).

angeboten werden, länger als 24 Stunden dauern oder eine Übernachtung einschliessen (Art. 1 PauRG). Diese Erfordernisse dürften soweit ersichtlich die meisten MaaS-Angebote nicht erfüllen, sofern diese aus blossen Reiseleistungen bestehen. Werden hingegen – wie dies gewisse MaaS-Geschäftsmodelle anvisieren – zusätzlich zu einer Reise auch Unterkünfte über eine MaaS-Plattform angeboten, so kommt unter Umständen dennoch das Pauschalreisegesetz zur Anwendung (siehe Pollicino et al., 2022 zum zusätzlichen Verkauf von „endpoint activities“ durch MaaS-Anbieter).

5.2.4 Data Governance für Mobility-as-a-Service (MaaS)



Den Kern der Governance bildet die Data Governance, d.h. alle Regeln betreffend Umgang der Akteure mit den für die Mobilitätsanwendung relevanten Daten. Diese Regeln lassen sich in einem Analyseschema darstellen (siehe vorn Abb. 31). Im Folgenden bezieht sich die Strukturierung auf den jeweiligen Schritt des Analyseschema. Dieses geht von der Zielsetzung eines guten, d.h. funktionierenden MaaS-Angebotes aus (***4.1. Zielsetzung***), wobei zunächst zu ermitteln ist, welche Datenflüsse für dieses Mobilitätsangebot notwendig sind. In einem zweiten Schritt wird dann ermittelt, wer an welchen Daten berechtigt ist bzw. welche Akteure welche Daten kontrollieren (***4.2. Ausgangslage***). Ist die Datenzuordnung geklärt, wird im dritten Schritt ermittelt, welche Datenflüsse bestehen (***4.3. Anwendung***). Dies erlaubt sodann den Vergleich zur Zielsetzung und die Identifikation von Hindernissen für die Datenflüsse oder Datennutzung. Für die identifizierten Hindernisse können schliesslich gezielt Governance-Massnahmen vorgeschlagen werden (***4.4. Abgleich***). Besteht zwischen Anwendung und Zielsetzung keine Diskrepanz (mehr), sind keine weiteren Governance-Massnahmen notwendig.

4.1. Zielsetzung: Ein gutes MaaS-Angebot

Im ersten **Schritt** des Data-Governance-Modells geht es darum, zu beschreiben, welche Datenflüsse für den Betrieb eines funktionierenden MaaS-Angebots notwendig sind. Dabei kann auf der generalisierten Beschreibung der Datenflüsse aufgebaut werden (siehe Kap. 2.3.1):

Damit ein MaaS-Angebot bereitgestellt werden kann, müssen unterschiedliche Datentypen vom Mobilitätsnachfrager zum MaaS-Anbieter fliessen: *Vertragsdaten*, *Daten zur Benutzeridentifikation*, *sicherheitsrelevante Daten zur Benutzeridentifikation*, *aggregierte Nutzungsdaten* und *individuelle Nutzungsdaten*. Die *Daten zur Benutzeridentifikation* werden typischerweise vom MaaS-Anbieter an den Mobilitätsdienstleister übermittelt. Im Gegenzug erhält der MaaS-Anbieter vom Mobilitätsdienstleister die notwendigen Daten zur *Angebotsbeschreibung* und zum *Angebotsstatus*. Oft fliessen zudem Daten vom Mobilitätsnachfrager zum Mobilitätsdienstleister, namentlich *individuelle* und *aggregierte Nutzungsdaten* sowie *Daten zur Benutzeridentifikation*. Der Vollständigkeit halber kann angemerkt werden, dass nicht jeder Mobilitätsdienstleister auf diesen letzten Datenfluss angewiesen ist. In öffentlichen Verkehrsmitteln, in denen die Fahrausweise und damit die Nutzungsberechtigung nur stichprobenartig kontrolliert wird, fliessen typischerweise keine Daten zur Benutzeridentifikation. Dies ist erst der Fall, wenn Passagiere kontrolliert werden oder z.T. auch erst falls und sobald sie gebüsst werden.

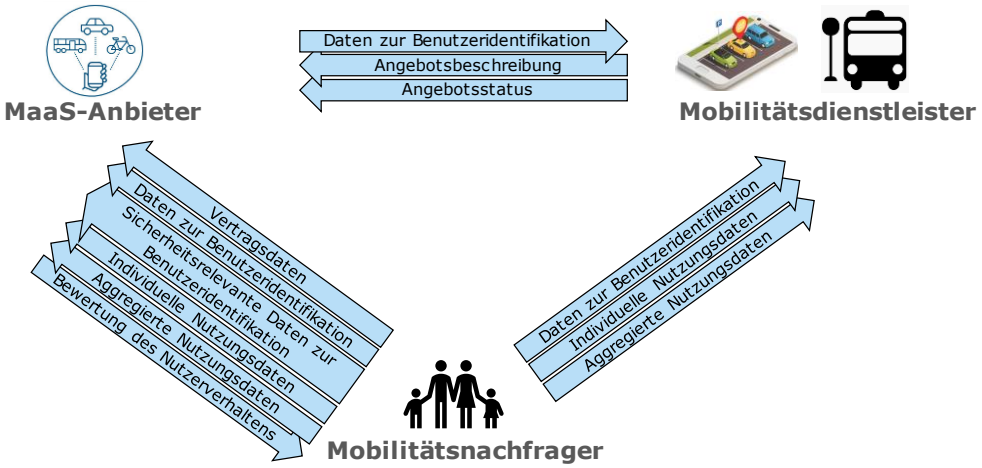


Abb. 35 Beschreibung der notwendigen Datenflüsse bei MaaS[15]

4.2. Ausganslage: Datenzuordnung

Im zweiten Schritt ist zu klären, welche Akteure aus welchen Gründen welche Daten tatsächlich oder rechtlich kontrollieren. Dazu ist die Anwendung der verschiedenen rechtlichen Instrumente auf die Daten zu prüfen (siehe Kap. 3.2 oben).

Typischerweise bestehen an den im Rahmen von MaaS verwendeten Datentypen **keine Immaterialgüterrechte**. Lediglich textförmig in Nutzerprofilen abgespeicherte Informationen über Mobilitätsnachfrager könnten als Sprachwerke (Art. 2 lit. a URG) geschützt sein. Meist dürften diese Einträge aber automatisiert erfolgen, womit es an der Schutzvoraussetzung der geistigen Schöpfung fehlt und kein Recht entsteht (Art. 2 Abs. 1 URG). Gleiches gilt für die grafische Darstellung von Nutzungsdaten und deren Einordnung als visuelles Werk (Art. 2 lit. g URG) (vgl. die Abbildung bei Wagner et al., 2020, S. 481).

Ein wesentliches Ziel von MaaS-Anbietern ist es, personalisierte Angebote für einzelne Mobilitätsnachfrager zu gestalten (Jittrapirom et al., 2017, S. 16; Lyons et al., 2019, S. 23). Hierfür werden verschiedene Daten in Nutzerprofilen gespeichert (vgl. MaaS4EU, 2018b, S. 10 ff.). Es ist davon auszugehen, dass solche *individuellen und aggregierten Nutzungs- bzw. Kundendaten* wertvolle Assets darstellen (vgl. Avenir Mobilité, 2018, S. 4) und grundsätzlich geheim gehalten werden – und zwar sowohl von MaaS-Anbieten als auch von den Mobilitätsdienstleistern. Damit greifen grundsätzlich die Instrumente des **strafrechtlichen und wettbewerbsrechtlichen Geheimnisschutzes** (vgl. Grafenstein, 2022, S. 20 f.). Zudem können insbesondere aufbereitete Daten unter den Schutz von **Art. 5. lit. c UWG** fallen, womit marktreife Arbeitsergebnisse vor einer Übernahme durch andere geschützt werden, sofern diese ohne angemessenen eigenen Aufwand durch technische Reproduktionsverfahren übernommen oder verwertet werden (zu Datenbanken als marktreife Arbeitsergebnisse siehe Weber & Chrobak, 2018, S. 984 f.). Trotz dieser Schutzmöglichkeiten können der hohe wirtschaftliche Wert dieser Daten und der fehlende absolutrechtliche Schutz Gründe dafür sein, dass die Unternehmen zögern, solche Daten in eine Mobilitätsdateninfrastruktur einzubringen. Immerhin können die Daten, sind sie einmal abhandengekommen, mit diesen Instrumenten nicht wiedererlangt werden.

Einige der im Rahmen von MaaS erhobenen generischen Datentypen weisen einen Personenbezug auf, namentlich *individuelle Nutzungsdaten*, *Vertragsdaten*, *Daten zur Benutzeridentifikation*, *Daten über die Bewertung des Nutzerverhaltens* und Daten über die *Produzentenbewertung*. Hinsichtlich der aggregierten Nutzungsdaten (anonymisierte oder

[15] Quellen der Symbole: https://commons.wikimedia.org/wiki/File:Bus_stop_symbol.svg, https://www.dekra-solutions.com/2020/06/carsharing-die-mobilitaet-der-zukunft/, https://www.data-infrastructure.eu/GAIAX/

pseudonymisierte individuelle Nutzungsdaten) muss je nach den Umständen geprüft werden, ob diese im Einzelfall beim Hinzufügen weiterer Informationen oder der Kombination mit anderen Daten ohne unverhältnismässigen Aufwand *re-individualisiert* werden und somit trotzdem als Personendaten gelten können. Gerade zwischen dem MaaS-Anbieter und den Mobilitätsdienstleistern findet ein intensiver Austausch von personenbezogenen Daten statt (MaaS4EU, 2018a, S. 21). Das bedeutet, dass – ohne besondere technische Vorkehrungen – auf einen grossen Teil der Daten die Bestimmungen zum **Datenschutzrecht** zur Anwendung kommen. Dieses schränkt einerseits grundsätzlich die Möglichkeiten der Datennutzung ein und räumt andererseits den Mobilitätsnachfragern gewisse Kontrollrechte ein. Für eine rechtskonforme Datenbearbeitung müssen sowohl Mobilitätsdienstleister als auch MaaS-Anbieter die betroffenen Personen über die Beschaffung und Bearbeitung ihrer Personendaten informieren (s. dazu Art. 19 nDSG) und ein rechtskonformes Einwilligungsmanagement implementieren.

4.3. Anwendung: Datennutzung

Generell darf davon ausgegangen werden, dass einige für MaaS-Angebote notwendige Daten frei verfügbar sind. Hierzu gehören **Geodaten** zur Angebotsbeschreibung**,** die durch die zuständigen Behörden im Rahmen von Open-Government-Initiativen bzw. aufgrund gesetzlicher Verpflichtungen (vgl. das Bundesgesetz über das Öffentlichkeitsprinzip in der Verwaltung für den Bund, BGÖ [SR 152.3]) in Mobilitätsdateninfrastrukturen eingebracht werden (z.B. Daten von Verkehrsnetz CH, welche in die zukünftige Mobilitätsdateninfrastruktur [MODI] einfliessen sollen).

Etwas komplexer ist die Situation bezüglich der **Betriebs- und Vertriebsdaten** der Mobilitätsdienstleister, wozu insbesondere *individuelle und aggregierte Nutzungsdaten*, *Angebotsbeschreibung* und *Angebotsstatus* zählen: Während konzessionierte Transportunternehmen aufgrund ihrer besonderen Nähe zum Gemeinwesen (durch Staatsbeteiligung und/oder Konzessionierung) sowie diverser gesetzlicher Datenoffenlegungspflichten ohnehin bestimmte Daten offenlegen müssen (s. vorn Kap. 3.3) und tendenziell eher bereit sein dürften, gewisse Datensätze gegenüber Dritten preiszugeben, muss in Bezug auf (private) Mobilitätsdienstleister differenziert werden. Diese sind typischerweise nicht bereit, *Vertriebsdaten* zu teilen. Demgegenüber scheint die Bereitschaft privater Stakeholder *Betriebsdaten* zu teilen etwas grösser zu sein, wie das Beispiel der Webseite zu Standorten und Verfügbarkeit von Shared Mobility Angeboten zeigt[16]. Auf dieser Plattform können auf freiwilliger Basis Daten zu Shared Mobility eingebracht werden. Die Interviews mit den Stakeholdern (siehe Kap. 2.5.2) bestätigen diesen Befund genauso wie die Tatsache, dass – mit Ausnahmen weniger Angebote und Pilotprojekte (z.B. Yumuv, Whim App, Sorglos mobil) – MaaS-Angebote in der Schweiz weitgehend fehlen. Insbesondere fehlen auf Vertriebsdaten basierende Angebote, bei denen die MaaS-Anbieter direkt Vertragsbeziehungen mit den Mobilitätsnachfragern eingehen (zu den verschiedenen Integrationsstufen von MaaS siehe Kamargianni et al., 2016, S. 3295 ff.; Lyons et al., 2019, S. 28 ff.; Sochor et al., 2018, S. 9 ff.).

[16] Siehe: https://www.sharedmobility.ch/

4.4. Beseitigung von Hindernissen

Der Vergleich dieses Zustands mit der angestrebten Zielsetzung (4.1.) zeigt, dass Mobilitätsdaten gegenwärtig nicht in ausreichendem Mass geteilt werden. Entsprechend gilt es, Massnahmen zu identifizieren, welche die Nutzung der Mobilitätsdaten verbessern und MaaS-Angebote ermöglichen. Sämtliche Governance-Massnahmen müssen darauf abzielen, das **Vertrauen aller Akteure** in das Funktionieren des Mobilitätsökosystems zu stärken, damit diese bereit sind, sich an einer Mobilitätsdateninfrastruktur zu beteiligen und insbesondere eigene Daten zur Verfügung zu stellen. Erst das gegenseitige Vertrauen erlaubt es, eine genügend grosse kritische Masse von Mobilitätsdienstleistern und Mobilitätsnachfragern zusammenzubringen.

Im Folgenden wird davon ausgegangen, die Data Governance setze an einer **zentralen Infrastruktur** an. (Zu den Gründen für diese Wahl vorstehend Kap. 5.2.2). Weil diese Wahl den Infrastrukturwettbewerb beseitigt, verlangt sie nach besonderen Regeln über den Zugang und die Nutzung der Infrastruktur. Bei einer Marktordnung mit Infrastrukturwettbewerb wären solche Regeln hingegen fehl am Platz und als Eingriff in die Wirtschaftsfreiheit auch rechtfertigungsbedürftig (vgl. Art. 36 BV).

Eine Hilfestellung bei der Formulierung von Data Governance-Massnahmen bietet die Zusammenstellung von möglichen Hindernissen für die Datennutzung, an der sich auch die folgenden Vorschläge orientieren.

4.4 Abgleich Welche Governance Massnahmen können die wesentlichen Hindernisse adressieren?

	Hindernisse	Governance-Massnahmen
a.	Fehlende Adaptation aus Sorge vor Verlust von Wettbewerbsvorteilen (Bekanntgabe von core business assets)	• Grundsatzregeln betreffend Aufnahme/Ausschluss von der Plattform, verknüpft mit Regeln zu den Bedingungen der Nutzung (vertraglich festgehalten) • Transparenzpflicht betr. Routing • Regeln zur Aufsicht und Kontrolle
b.	Datenschutzrechtliche Ansprüche könnten der Nutzung entgegenstehen	• Technische Massnahmen • Auftragsdatenverarbeitung • Rechtfertigung durch öffentliches Interesse
c.	Immaterialgüterrechtliche Ansprüche könnten der Nutzung entgegenstehen	• Anwendung oder Schaffung von Schrankenbestimmungen
d.	Fehlendes Vertrauen	• Klare (rechtlich oder technisch abgesichterte) Regeln und Pflichten • Verantwortlichkeiten, inkl. Haftung
e.	Fehlende kritische Masse, zu hohe Kosten, fehlende Skalierbarkeit	• Schaffung von guten Rahmenbedingungen durch vorgeschlagene Massnahmen

***Abb. 36** Hindernisse für die Datennutzung bei MaaS und mögliche Governance-Massnahmen*

4.4.a. Fehlende Beteiligung aus Sorge vor einem Verlust von Wettbewerbsvorteilen

Während Mobilitätsdienstleister weitgehend bereit sind, Daten zur Angebotsbeschreibung zur Verfügung zu stellen, dürften bezüglich der allgemeinen Zugänglichmachung von Daten über den Vertrieb (insb. *individuelle und aggregierte Nutzungsdaten*, *Daten über den Angebotsstatus* und *Vertragsdaten*) Vorbehalte bestehen. Selbst generierte oder veredelte Betriebs- und insbesondere Vertriebsdaten haben dabei einen grossen wirtschaftlichen Wert für die Mobilitätsdienstleister (core business asset, zum ökonomischen Wert von Daten siehe Grafenstein, 2022, S. 18 ff.) und dürften vom strafrechtlichen- und wettbewerbsrechtlichen Geheimnisschutz umfasst sein. Der rechtliche Schutz greift indes nur, wenn allen Vertragspartnern eine Geheimhaltungsverpflichtung auferlegt wird; im Falle einer Verletzung solcher Verpflichtungen kann aber die Kontrolle über die Daten nicht mehr

wiedererlangt werden. Die Ausarbeitung entsprechender Verträge mit MaaS-Anbietern ist für die Mobilitätsdienstleister teuer und aufwendig. Vor allem dürfte der Nutzen der Mobilitätsdienstleister – selbst bei Entgeltlichkeit der Datenlieferung – aus deren Sicht die Gefahr eines Verlustes der Wettbewerbsvorteile kaum überwiegen. Damit drängen sich folgende Governance-Massnahmen auf:

- Das **Aufstellen klarer Grundsätze und Regeln betreffend Datenbezug und Datenverwendung.** Diese Regeln müssen insbesondere festhalten:
    - Zu welchen ökonomischen Bedingungen welche Daten in die Mobilitätsdateninfrastruktur eingebracht und unter welchen Bedingungen welche Daten aus der Mobilitätsdateninfrastruktur bezogen werden können (z. B. nur bei finanzieller Vergütung oder unter der Voraussetzung der Rücklieferung von eigenen Daten) (zu gegenseitigem Datenaustausch bzw. Mutual Data Sharing siehe UVEK, 2022, S. 21) Dabei gibt es immer mehr praktische Beispiele, die zur Ausarbeitung dieser Bedingungen beigezogen werden könnten (s. z.B. die vom Institut für Geistiges Eigentum (IGE) veröffentlichen Musterverträge zur Datennutzung[17], die verschiedenen Lizenztypen für die Datennutzung in der Metropolitanregion Lyon[18] oder in der Region Île-de-France[19]);
    - welche technischen Anforderungen hinsichtlich der Datenqualität (Integrität, Authentizität, Aktualität, etc.) von den Datenlieferanten eingehalten werden müssen;
    - wie Datenzugriffe geregelt und Zugriffskontrollen durchgesetzt werden, und wie Zugriffe protokolliert werden, um möglichen Missbrauch detektieren zu können;
    - dass (unter dem Vorbehalt der Einhaltung der genannten Bedingungen) ein freier und gleichberechtigter Zugang zur Infrastruktur besteht, und
    - dass für alle Akteure erkennbar ist, nach welchen (frei konfigurierbaren) Kriterien und mit offengelegten Algorithmen das optionale Routing für die Mobilitätsnachfrager erstellt wird, sofern ein solches von der Dateninfrastruktur vorgenommen wird.

- Diese Grundsätze und Regeln sind von einer **neutralen Instanz** oder durch einen **moderierten Ansatz unter Einbezug der relevanten Stakeholder** zu entwickeln. Der Vorteil des Multistakeholder-Ansatzes würde darin liegen, dass sich die Regeln nah an den tatsächlichen Bedürfnissen orientieren würden. Demgegenüber würde sich der Regulator mit einer über die wesentlichen Grundsätze hinausgehenden Festlegung von Regeln (insbesondere hinsichtlich Nutzungsentgelt und Routing) Wissen anmassen, über das er nicht verfügt. So würden womöglich falsche Anreize gesetzt. Vor diesem Hintergrund sollten die verschiedenen potentiellen Datenlieferanten sowie Datenbezüger bei der Festsetzung der Regeln und Grundsätze einbezogen werden, wobei für deren Legitimierung auf eine ausreichende Vielfalt der Stakeholder zu achten ist (Belli, 2015). Dieser Ansatz soll dabei nicht nur beim Aufbau einer Mobilitätsdateninfrastruktur, sondern auch bei deren Weiterentwicklung (z.B. Anpassung an laufende Bedürfnisse) angewendet werden.
- Der **Betrieb** der Dateninfrastruktur hat ebenfalls durch eine **neutrale Instanz** (d.h. weder Mobilitätsdienstleister noch Mobilitätsnachfrager) oder ein **Multistakeholder-Forum** zu erfolgen. Die **Aufsicht** und **Kontrolle** über die Einhaltung der festgelegten Grundsätze wiederum hat durch ein weiteres Gremium zu erfolgen, das über die nötigen Vollzugs- bzw. Kontrollkompetenzen sowie -instrumente verfügt. Diese hat zudem auch die Finanzierung der Dateninfrastruktur sicherzustellen, etwa durch eine klare Regelung der Kosten, die beim Datenbezug und allgemein beim Betrieb der Mobilitätsdateninfrastruktur entstehen. Dabei ist zu berücksichtigen, dass der Vertrieb dadurch nicht teurer und Geld nicht aus dem System entzogen wird. Zur Aufsichts- und Vollzugskompetenz einer solchen Instanz gehört schliesslich auch die Regelung des Inkassos und die Einrichtung bzw. Bestimmung einer Streitschlichtungsstelle oder Beschwerdeinstanz, falls es im Rahmen des Betriebs der Mobilitätsdateninfrastruktur zu

[17] Siehe: https://www.ige.ch/de/uebersicht-geistiges-eigentum/gesellschaftliche-bedeutung/datenbearbeitung-und-datensicherheit
[18] Siehe Beispiel Lyon: https://data.grandlyon.com/jeux-de-donnees
[19] Siehe Beispiel: Île-de-France https://data.iledefrance-mobilites.fr/pages/licences/

Streitigkeiten kommen soll (z.B. bei der Auslegung von verschiedenen Bedingungen für den Datenbezug).

4.4.b. Datenschutzrechtliche Ansprüche könnten der Nutzung entgegenstehen

Wie bereits angedeutet, könnten zahlreiche im Rahmen von MaaS weitergegebene Datentypen Personendaten enthalten (siehe Kap. 2.3.1). Damit kann die Datennutzung durch zwei Aspekte erschwert werden: Einerseits könnten potentielle Datenlieferanten einwenden, sie dürften aufgrund datenschutzrechtlicher Vorgaben der Mobilitätsdateninfrastruktur keine Daten zur Verfügung stellen (vgl. Grafenstein, 2022, S. 20). Andererseits könnten die betroffenen Personen selbst durch die Ausübung ihrer Rechte (insbesondere dem Recht auf Widerruf oder Löschung) das Funktionieren der Infrastruktur erschweren oder gar gefährden. Damit drängen sich folgende Governance-Massnahmen auf:

- Aus **technologischer Sicht** bestehen verschiedene Möglichkeiten, eine Mobilitätsdateninfrastruktur so auszugestalten, dass Mobilitätsdaten unter Einhaltung der datenschutzrechtlichen Vorgaben geliefert und bezogen werden können. Allgemeingültige Aussagen zur Auswahl und dem Einsatz privatsphärenschützender Technologien sind aufgrund des breiten Spektrums an Daten, Datenflüssen, Berechnungen, und weiterer Anforderungen allerdings schwierig zu treffen, da die in der Praxis verfügbaren Technologien stark von den spezifischen Anwendungsfällen abhängen, wie beispielsweise Vertrauensannahmen, Komplexität der Berechnungen, Verfügbarkeit von (Rechen-) Ressourcen, oder Echtzeitanforderungen. Im Kontext von MaaS wäre beispielsweise der Einsatz von Trusted Execution Environments (vgl. Kap. 4.2.2) denkbar, wobei sensitive Daten in geschützten Umgebungen abgelegt werden, und Algorithmen zu den Daten gebracht werden anstatt umgekehrt, um jegliches nicht zwingend erforderliche Teilen von Daten zu reduzieren. Ergänzend sollten Techniken zur Pseudonymisierung bzw. Anonymisierung von Daten eingesetzt werden, wo immer dies funktional möglich ist. Mit dem Einsatz verteilter Systeme (wie Distributed Ledgers) wäre es zudem möglich, Zugriffsrechte, Zahlungen zwischen den Stakeholdern und ähnliches transparent und automatisiert zu verwalten. Dabei müssten allerdings die personenbezogenen Daten “off chain” bleiben oder verschlüsselt werden; zudem sind solche Lösungen nicht ohne weiteres skalierbar.
- Werden personenbezogene Daten durch Dritte (sowohl bei zentraler Infrastruktur als auch bei Infrastrukturwettbewerb) bearbeitet, kann eine Gewährleistung der Datenschutzkonformität durch eine Übertragung der Personendatenbearbeitung (sog. "**Auftragsdatenverarbeitung**"; Art. 10a DSG; Art. 9 ff. nDSG) geregelt werden (Rosenthal, 2020, S. 24 ff.). Eine Übertragung der Personendatenbearbeitung kann dabei durch Gesetz (vgl. als Beispiel Art. 18 E-MODIG) oder durch Vertrag erfolgen.
- Aus datenschutzrechtlicher Sicht könnte weiter die **Einführung gemeinsamer Verhaltensregeln und Datenschutzzertifizierungen im Zusammenhang mit zentralen Mobilitätsdateninfrastrukturen** Vertrauen seitens der potentiellen Datenlieferanten schaffen und damit den Austausch von Daten fördern (für die Schweiz siehe Art. 11 DSG i.V.m. Verordnung über die Datenschutzzertifizierungen [VDSZ] bzw. Art. 13 nDSG und für die EU siehe Costantini, 2017, S. 9 mit Verweis auf die Art. 40 und Art. 42 VO 2016/679).
- Zuletzt stellt sich die Frage, ob datenschutzrechtliche **Rechtfertigungsgründe** greifen, die gestützt auf öffentliche Interessen gewisse – an sich unzulässige – Datenbearbeitung erlauben würden. Als öffentliche Interessen kämen im Fall von MaaS etwa die ökologischere Ausgestaltung des Verkehrs oder die effizientere Nutzung der Verkehrsinfrastruktur in Frage.

4.4.c. Immaterialgüterrechtliche Ansprüche könnten der Nutzung entgegenstehen

Weil an den für MaaS-Anwendungen benötigten Daten keine Immaterialgüterrechte bestehen, stehen der Datennutzung typischerweise keine solchen Drittrechte entgegen.

Entsprechend braucht es für MaaS diesbezüglich keine besonderen Governance-Massnahmen.

4.4.d. Fehlendes Vertrauen

Das Vertrauen aller Akteure in das Funktionieren des Mobilitätsökosystems ist entscheidend dafür, ob sich MaaS-Angebote etablieren können. Dabei sind verschiedene Perspektiven zu berücksichtigen:

Das Vertrauen der Mobilitätsdienstleister und der MaaS-Anbieter hängt massgeblich davon ab, ob **klare Regeln und Pflichten**, insbes. betreffend Zugang zur Infrastruktur und betr. Routing bestehen, und in welchem Verfahren diese festgelegt werden. Der Einsatz dezentraler Systeme könnte das Vertrauen ebenfalls stärken.

Aus Sicht der Mobilitätsnachfrager hängt das Vertrauen davon ab, wie Mobilitätsdienstleister und MaaS-Anbieter mit personenbezogenen Daten umgehen. Zudem dürfte das Vertrauen in MaaS-Angebote steigen bzw. deren Entstehung erst möglich werden, wenn die MaaS-Anbieter für die gesamte multimodale Reisekette einstehen und die **Haftung** für verpasste Anschlüsse oder ausgefallene Verbindungen übernehmen, z.B. durch einen Anspruch auf Weiterfahrt, eine Fahrpreiserstattung oder ähnliches. Gut möglich, dass sich dies auch ein Geschäftsmodell für Versicherungsleistungen sein kann. Der Wettbewerb mehrerer MaaS-Anbieter auf einer zentralen Infrastruktur könnte hierfür die notwendigen Anreize setzen. Auch aus Sicht der Mobilitätsnachfrager kann der Einsatz transparenter Technologien wie Distributed Ledgers zur Dokumentation von Freigaben oder Datenzugriffen eingesetzt werden und so Vertrauen schaffen.

4.4.e. Fehlende kritische Masse; zu hohe Kosten; fehlende Skalierbarkeit

Damit sich MaaS-Angebote entwickeln können, braucht es eine gewisse kritische Masse von Anbietern und Nachfragern von MaaS-Angeboten. Der Entscheid zugunsten einer zentralen Infrastruktur vergrössert die Chance, dass diese kritische Masse erreicht wird. Auch das Verknüpfen der MaaS-Systeme über Ländergrenzen hinweg (sog. MaaS-Roaming), profitiert von einer zentralen Infrastruktur.

5.3 Governance der Strassengebührenerhebung (RUC)

Die Gebührenerhebung (für die Umsetzung von Mobility Pricing, IFMS, RUC) ist eine aktuelle und wichtige Anwendung, hinsichtlich derer noch ungelöste Fragen zur Governance bestehen. Dies gilt insbesondere für den Datenschutz, denn bei der Gebührenerhebung werden als Basis der Bepreisung von individuellen Nutzern äussert detaillierte Bewegungsprofile erfasst. Aus datenschutzrechtlicher Sicht kann daraus ein Persönlichkeitsprofil (Art. 3 lit. d DSG), ein Profiling (Art. 5 lit. f nDSG) oder gar ein Profiling mit hohem Risiko (Art. 5 lit. g nDSG) entstehen. Zudem können bei Kontrollen äusserst sensitive Daten anfallen, die unter Umständen besonders schützenswerte Personendaten darstellen (Art. 3 lit. c DSG, Art. 5 lit. c nDSG). Die Menge der involvierten Akteure und der häufig auch internationale Kontext erhöhen die Komplexität und schränken die Lösungsmöglichkeiten ein.

Bei der Strassengebührenerhebung, fortan mit RUC (Road User Charge) abgekürzt, wird die Benutzung der Strasseninfrastruktur bepreist. Während für den Schwerverkehr fast im gesamten EU-Raum RUC zu entrichten sind, die interoperabel mit EETS (siehe Kap. 2.2 & 2.3.2) umgesetzt werden, findet eine fahrleistungsabhängige Abgabe bei Personenkraftwagen mehrheitlich nur in Ländern mit privatisierten Strasseninfrastrukturen statt (bspw. Autobahnmauten in südeuropäischen Ländern).

Infolge der rasch fortschreitenden Elektrifizierung der Fahrzeuge nehmen die Einnahmen aus den Mineralölsteuern kontinuierlich ab. Das EU-Parlament hat beschlossen, den Verkauf von Fahrzeugen mit Verbrennungsmotoren ab 2035 zu verbieten (NZZ, 2022). Es ist zu erwarten, dass die Schweiz in diesem Entscheid der EU folgen wird. Dies gefährdet die Finanzierung der Schweizer Strasseninfrastruktur. Deswegen sollen auch nicht-fossil betriebene Fahrzeuge mittel- bis langfristig einen Finanzierungsbeitrag leisten und eine

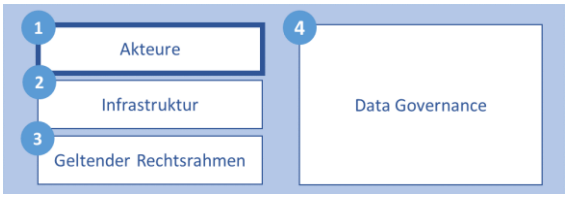
fahrleistungsabhängige Abgabe zahlen (INFRAS/Rapp/Ecoplan, 2021). In Anbetracht der benötigten Vorlaufzeit für die Umsetzung von RUC-Systemen nimmt der Handlungsbedarf zu. Dies hat der Bundesrat erkannt und im Juni 2022 die Eckwerte für den Ersatz der Mineralölsteuern festgelegt. Demnach soll sich die Ersatzabgabe aus einem festen Betrag pro gefahrene Kilometer und Fahrzeugkategorie zusammensetzen, womit der Charakter dieser Abgabe jenem des derzeitigen Systems für Benzin- und Dieselfahrzeuge entspräche. Während damit klar ist, *dass* künftig eine Abgabe erhoben werden soll, ist noch offen, *wie* dies geschehen soll. Das UVEK und das EFD sind beauftragt, bis Ende 2023 einen Gesetzesvorschlag auszuarbeiten; der Bundesrat geht davon aus, dass die Ersatzabgabe bis 2030 in Kraft treten wird (Bundesrat, 2022).

Bei der Umsetzung einer flächendeckenden fahrleistungsabhängigen Abgabe für sämtliche knapp 5 Mio. Motorfahrzeuge privater Nutzer in der Schweiz als Ersatz der Treibstoffabgaben steht der Schutz der persönlichen Daten, insbesondere der individuellen Fahrprofile, besonders im Fokus. Es ist wichtig zu ergänzen, dass die Abgabe auf allen Strassen gelten soll. Auch private Strassen sind in der Schweiz in der Regel öffentlich zugänglich.

Die Akzeptanz unter den Bürgern für ein umfassendes Tracking-System dürfte gering sein, falls die Nutzung verpflichtend ist und Personendaten an Behörden übermittelt werden. Man müsste Systeme erwägen, die die Privatsphäre besser schützen (NZZ, 2021). Im Governance-Modell für RUC ist somit die Frage zentral, wie eine fahrleistungsabhängige RUC datenschutzkonform umgesetzt werden kann.

5.3.1 Akteure

Bei RUC sind wie bei allen Mobilitätsanwendungen mehrere Akteure beteiligt. Die Anwendung des in Kap. 2.2 eingeführten Rollenmodells auf RUC zeigt erneut, dass der gleiche Akteur mehrere Rollen einnehmen kann.



Der **Nutzer** bei dieser Mobilitätsanwendung ist der Infrastrukturbenutzer. Ist eine Person mit einem (motorisierten) Fahrzeug auf der bereitgestellten Infrastruktur unterwegs, ist dafür eine entsprechende Gebühr zu entrichten.

Leistungserbringer sind der Gebührenerheber sowie der Infrastrukturbereitsteller. Ersterer ist diejenige Instanz, die gesetzlich verpflichtet wird, die Gebühr der Infrastrukturbenutzung zu erheben. Dabei kann es sein, dass sich mehrere Gebührenerheber je nach Art der Gebühr (fahrleistungsabhängige Abgabe, städtisches Mobility Pricing, Mautgebühren für z.B. einen Tunnel) entwickeln und durch separate Instanzen repräsentiert werden. Der Infrastrukturbereitsteller ist dafür verantwortlich, die Infrastrukturbenutzung zu gewährleisten und das abgabepflichtige Netz zu definieren. Trotzdem ist davon auszugehen, dass pro RUC jeweils nur ein Gebührenerheber existiert. Im Folgenden wird nur noch der Gebührenerheber als Leistungserbringer betrachtet, da der Infrastrukturbereitsteller im Erhebungskonzept einer Strassengebühr eine untergeordnete Rolle einnimmt.

Der **Vermittler** ist bei dieser Smart Mobility-Anwendung der Maut-Dienstanbieter, also die Instanz, die dem Nutzer einen Dienst anbietet, mit dem die Maut erhoben werden kann. Bis anhin war z.B. in der Schweiz bei der Erhebung der LSVA der Maut-Dienstanbieter und der Gebührenerheber dieselbe Instanz. In Zukunft und mit der neuesten LSVA-Systemgeneration werden diese Aufgaben getrennt. Es wird zudem ermöglicht, dass dem Nutzer mehrere Maut-Dienstanbieter zur Verfügung stehen und er aus diesem Angebot frei wählen kann. Es zeichnet sich ab, dass für eine flächendeckende RUC in der Schweiz, in der für sämtliche Nutzer eine Gebühr fällig wird, ebenfalls dieser Ansatz zu verfolgen sein wird. Die Beteiligung dieser Instanz im System der Gebührenerhebung ist letztlich unabdingbar, weil kaum vorstellbar ist, dass alle Infrastrukturnutzer die zur Gebührenerhebung notwendigen Daten selbst erheben könnten. Dies würde nicht nur an den unterschiedlichen Fähigkeiten der Nutzer, sondern auch an daran scheitern, dass immer das von einer behördlichen Stelle einheitlich vorgehaltene aktuellste Kartenmaterial für die Erhebung verwendet werden muss (s. hierzu hinten in Kap. 5.3.4 Absatz 4.1).

Der **Regulator** ist bei RUC die gesetzgeberische Stelle, welche die Rahmenbedingungen durch Gesetze und Verordnungen festlegt. Diese Rahmenbedingungen binden den Maut-Dienstanbieter und schreiben ihm vor, mit welcher Qualität er seinen Dienst anzubieten hat. Der Regulator kann mehrere Maut-Dienstanbieter zulassen, sofern diese die Qualitätsanforderungen erfüllen. Zusätzlich ist der Regulator auch dafür verantwortlich, dem Gebührenerheber die Verantwortung zu übertragen, die Gebühr entsprechend den geltenden Vorschriften zu erheben.

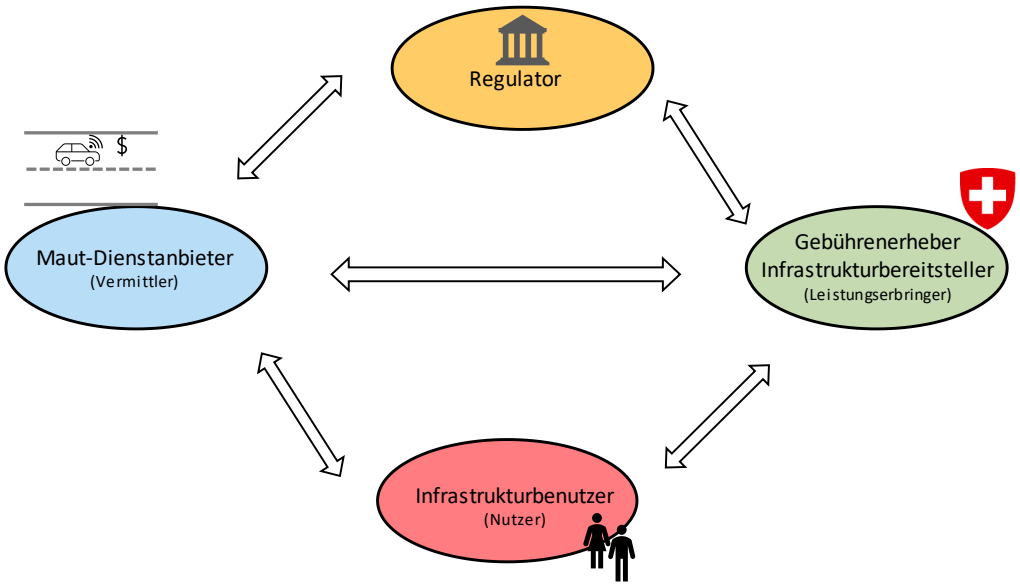
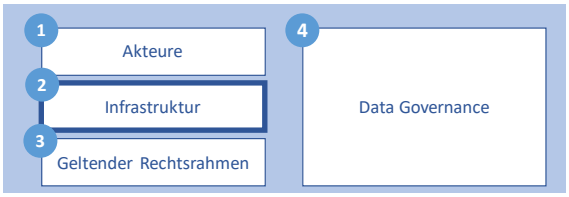


Abb. 37 *Rollenmodell der Strassengebührenerhebung.*

5.3.2 Dateninfrastrukturen (bzw. Datenzugang)



Bei einer RUC werden über fahrzeugseitige Erfassungssysteme Daten bereitgestellt, um die Gebühr zu berechnen. Die Daten (z.B. Geodaten) werden durch die Bewegung der Nutzer generiert, vom Maut-Dienstanbieter gesammelt und für die Berechnung der Gebühr bereitgestellt. Ähnlich wie bei MaaS sind auch hier grundsätzlich zwei Arten denkbar, wie die notwendigen Dateninfrastrukturen ausgestaltet werden: Entweder mit einer zentralen Infrastruktur oder mit dezentralen Infrastrukturen der jeweiligen Maut-Dienstanbieter. Anders als bei MaaS wäre eine zentrale Dateninfrastruktur hier aber nicht sinnvoll. Denn zwischen Maut-Dienstanbieter und Gebührenerheber fliessen Daten nur in eine Richtung und nur zum Zweck, dass der Gebührenerheber eine Gebühr erheben und dem Infrastrukturbenutzer eine Rechnung zustellen kann. Solange die Maut-Dienstanbieter dem Gebührenerheber die Daten im richtigen Format übermitteln, braucht es damit keine zentrale Infrastruktur. Eine dezentrale Infrastruktur ist effizienter und schützt v.a. die Privatsphäre der Personen potentiell besser. Überdies können den Infrastrukturbetreibern auch mit der Wahl einer dezentralen Infrastruktur gewisse Vorgaben gemacht werden.

Die Wahl einer dezentralen Infrastruktur bedeutet gleichzeitig, dass zwischen mehreren Maut-Dienstanbietern nicht nur auf der Infrastrukturebene, sondern auch auf der Dienstleistungsebene Wettbewerb entsteht. Der durch dieses Marktdesign entstehende Wettbewerb garantiert den RUC-pflichtigen Infrastrukturnutzern kompetitive und attraktive Lösungen. Sie haben die freie Wahl, sich denjenigen Maut-Dienstanbieter auszusuchen, der die für sie attraktivste Lösung bereitstellt. Dieser Wettbewerb auf der Dienstleistungsebene bietet grundsätzlich Anreize, möglichst gute betriebliche und technische Lösungen zu entwickeln und Angebote für die Nutzer zu schaffen, mit demselben Dienstanbieter auch international unterwegs zu sein. Aufgrund der hohen Anzahl immatrikulierter Fahrzeuge in

der Schweiz kann davon ausgegangen werden, dass eine kritische Masse erreicht wird, die den Betrieb mehrerer konkurrierender Angebote erlaubt.

In diesem Marktdesign mit dezentraler Infrastruktur müsste geprüft werden, ob es notwendig ist, einen einzelnen (oder alle) Maut-Dienstanbieter rechtlich zur Aufnahme von Nutzern zu verpflichten, falls sie keinen anderen Maut-Dienstanbieter wählen. Das wäre wohl v.a. dann in Erwägung zu ziehen, wenn die Maut-Dienstanbieter über die Gebührenerhebung hinausgehende weitere Dienste anbieten dürfen (s. dazu hinten in Kap. 5.3.4 Absatz 4.4.b)

Die Gebührenerheber geniessen – in ihrem jeweiligen Bereich - ein natürliches oder rechtliches Monopol, da für eine bestimmte Strasseninfrastruktur selbstverständlich nur jeweils eine Institution befugt ist, Gebühren zu erheben.

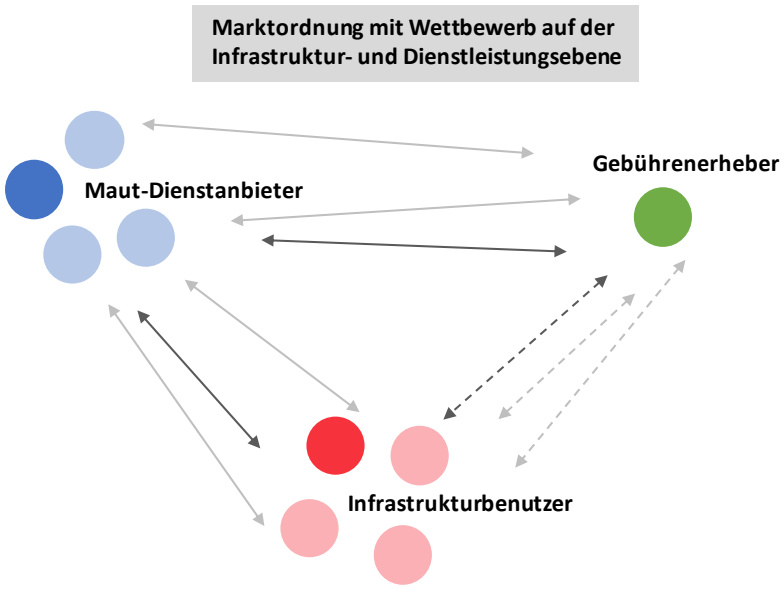
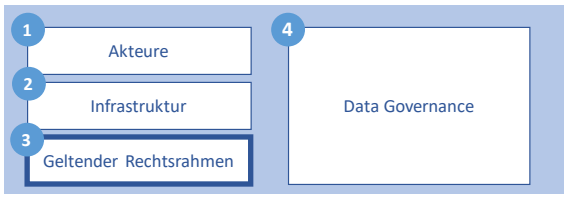


Abb. 38 *Marktordnung mit Wettbewerb auf der Infrastruktur- und der Dienstleistungsebene.*

5.3.3 Geltender Rechtsrahmen



Die geltende Schweizer Rechtsordnung kennt auf dem Gebiet des Road Pricing bisher zwei Formen von Strassenverkehrsabgaben:[20]

So haben einerseits Transportmotorwagen und Transportanhänger eine **leistungsabhängige Schwerverkehrsabgabe (LSVA)** zu entrichten, sofern ihr Gesamtgewicht über 3,5 t beträgt (Art. 3 Schwerverkehrsabgabegesetz [SVAG] [SR 641.81] i.V.m. Art. 2 Schwerverkehrsabgabeverordnung [SVAV] [SR 641.811]) (Art. 85 Abs. 1 BV). Für Fahrten mit bestimmten schweren Transportmotorwagen und Transportanhängern wird eine **pauschale Schwerverkehrsabgabe (PSVA)** erhoben (Art. 4 SVAV).

Andererseits wird für die **Benutzung von Nationalstrassen** eine Abgabe erhoben, die durch den Kauf einer **Vignette** zu entrichten ist (Art. 7 Nationalstrassenabgabegesetz [NSAG]; SR 741.71, Art. 86 Abs. 1 BV).

Abgaberechtlich handelt es sich sowohl bei der LSVA, PSVA wie auch den Nationalstrassenabgaben um **Kausalabgaben**, da diese als Entgelt für staatliche Leistungen entrichtet werden. Innerhalb der Kausalabgaben sind Strassenabgaben als **Gebühren** zu

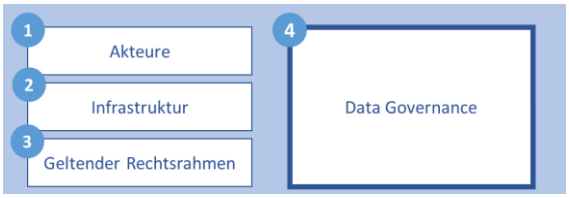
[20] Zu den bestehenden Road-Pricing-Instrumenten können noch Benutzungsgebühren für den Strassentunnel am Grossen St. Bernhard sowie die die Erhebung von Parkgebühren im öffentlichen Raum gezählt werden. Siehe BÜHLER CHRISTINE, Energieeinsparungen mit «Mobility Pricing»?, in: Jusletter vom 12. November 2018, Rz. 5.

qualifizieren. Bei den Gebühren werden wiederum Verwaltungs-, Benutzungs- und Konzessionsgebühren sowie Aufsichtsabgaben unterschieden. Da Strassengebühren zur Dekkung der Kosten für die Benutzung einer öffentlichen Einrichtung erhoben werden, handelt es sich bei Strassenabgaben um **Benutzungsgebühren**.

Für Fahrten auf öffentlichen Strassen, die nicht von der LSVA, PSVA oder Nationalstrassenabgabe erfasst sind, dürfen keine Abgaben erhoben werden (vgl. Art. 83 Abs. 2 Bundesverfassung [SR 101]); die Bundesversammlung kann lediglich begrenzt Ausnahmen bewilligen (Art. 82 Abs 3 zweiter Satz BV). Entsprechend bedürfte die Einführung einer flächendeckenden Strassengebührenerhebung für alle Fahrten auf öffentlichen Strassen in der Schweiz einer Teilrevision der Bundesverfassung.[21]

Die Umsetzung von RUC in der Schweiz muss zudem insoweit den Europäischen Rechtsrahmen berücksichtigen, als sich die Schweiz auch am EETS orientiert. Daraus ergeben sich die Anforderungen and die Interoperabilität sowie der damit verbundenen Auswahl möglicher Auswahl von Maut-Dienstanbietern.

5.3.4 Data Governance der RUC



Auch für die RUC bildet die Data Governance den Kern des Governance-Modells. Es handelt sich dabei um die Regeln bezüglich des Umgangs der Akteure mit den für die Gebührenerhebung relevanten Daten. Es zeigt sich, dass diese Regeln im selben Analyseschema darstellbar sind (siehe Abb. 31).

Die Analyse der Data Governance folgt dem Analyseschema und geht im Folgenden von der Zielsetzung einer vertrauenswürdigen, korrekten und die Privatsphäre schützenden Gebührenerhebung aus (**4.1.**). Es ist zunächst zu ermitteln, welche Datenflüsse für dieses Mobilitätsangebot notwendig sind. In einem zweiten Schritt wird dann ermittelt, wer an welchen Daten berechtigt ist bzw. welche Akteure welche Daten kontrollieren (**4.2.**). Ist die Datenzuordnung geklärt, wird im dritten Schritt ermittelt, welche Datenflüsse bereits heute bestehen (**4.3**.). Dies erlaubt sodann den Vergleich mit der Zielsetzung sowie die Identifikation von Hindernissen für die Datenflüsse oder Datennutzung. Für die identifizierten Hindernisse können schliesslich spezifische Governance-Massnahmen vorgeschlagen werden (**4.4.**). Besteht zwischen Anwendung und Zielsetzung keine Diskrepanz (mehr), sind keine weiteren Governance-Massnahmen notwendig.

4.1. Zielsetzung: Eine funktionierende Strassengebührenerhebung

Das Ziel von Road Pricing ist die Erhebung benutzungsbezogener Abgaben für den motorisierten Individualverkehr. Es gibt unterschiedliche Ausführungsvarianten mit entsprechend unterschiedlichen Zielsetzungen:

Bei **Mobility Pricing** sollen insbesondere Verkehrsspitzen gebrochen und eine gleichmässigere Auslastung der Verkehrsinfrastrukturen erreicht werden (UVEK, 2007).

Mit einer **fahrleistungsabhängigen Abgabe** kann ein **Ersatz für die wegfallende Mineralölsteuer** durch die zunehmende Elektrifizierung der Fahrzeugflotte geschaffen werden

[21] SCHAFFHAUSER, SGK BV, Art. 82 N 11; KERN, BSK BV, Art. 82 N 12 und N 17; auf die Streichung von Art. 82 Abs. 3 BV, die ein Road pricing ermöglicht hätte, wurde verzichtet, da sich im Vernehmlassungsverfahren für die neue BV kein Konsens abgezeichnet hatte. Siehe Botschaft über eine neue Bundesverfassung vom 20. November 1996, S. 261. Zudem erwähnt in Bundesrat (2022)

(INFRAS/Rapp/Ecoplan, 2021). Die Erhebung benützungsbezogener Abgaben hat zudem das Ziel, eine verursachergerechte Anlastung der Kosten für den fahrenden motorisierten Individualverkehr zu erreichen (Kostenwahrheit, Verursachergerechtigkeit), womit Klimaschutzziele anvisiert werden ("pay as you pollute") (AGORA, 2022).

Grundsätzlich werden bei sämtlichen Anwendungen die gleichen technologischen Erhebungsansätze verfolgt. Die Anwendungsfälle unterscheiden sich aber bezüglich Systemkonzept in der örtlichen, zeitlichen und fahrzeugabhängigen Variabilität der Bepreisung der Infrastruktur. Im Folgenden wird nur der Anwendungsfall der fahrleistungsabhängigen Abgabe als RUC betrachtet, bei der die Höhe der Abgabe weder vom Ort noch von der Zeit abhängig ist.

Um eine solche RUC unabhängig von Zeit, Ort oder Fahrzeug zu erheben, wäre grundsätzlich lediglich die Kenntnis der gefahrenen Kilometer pro Zeiteinheit notwendig. Allerdings wird auf den Ortsbezug nur schwer verzichtet werden können. Die Kilometerzahl pro Zeiteinheit sagt nämlich nichts darüber aus, wo die Kilometer zurückgelegt wurden. Es könnte sich um eine Fahrt im In- oder Ausland handeln, eine Fahrt mit (mehreren) Grenzüberschreitungen, eine Fahrt auf einer Nationalstrasse und/oder einer kantonalen, kommunalen oder privaten Strasse. Insbesondere die Kenntnis, zu welchem Anteil eine Kilometerzahl im Inland zurückgelegt wurde, ist für die Berechnung der Gebühr aber unabdingbar. Sinnvoll dürfte auch die Möglichkeit der Ermittlung der Strassenart (z. B. National- oder kantonale Strasse) sein, auf welcher die Kilometer zurückgelegt wurden.

Im Grundsatz wäre es zwar einleuchtend, nur die explizit gefahrenen Kilometer auf dem Schweizer Strassennetz zu erfassen. Dies bringt jedoch viele andere Schwierigkeiten mit sich. In den bereits zugelassenen Fahrzeugen sind keine geeichten Distanzmessgeräte vorhanden. Dies wird sich auch für zukünftige Zulassungen nicht ändern. Folglich müssten für über 5 Mio. Schweizer Fahrzeuge entsprechende Geräte von zertifizierten Werkstätten eingebaut werden, was einen erheblichen organisatorischen Aufwand mit sich bringt. Zudem ist dies, bei der Vielzahl an zugelassenen Fahrzeugtypen, wohl kaum technisch machbar und mögliche Manipulationen wären kaum oder nur mit nicht verantwortbarem Aufwand zu detektieren. Ein weiterer Nachteil wäre die Interoperabilität für grenzquerende Fahrzeuge. Ein analoges System für Elektrofahrzeuge, wie bei der heutigen Erhebung der Mineralölsteuer, bei dem die den Fahrzeugen zugeführten Elektrizität besteuert würde, kann ebenfalls kaum umgesetzt werden. Einerseits wäre unklar, ob die Elektrizität für die Infrastrukturbenutzung in der Schweiz verwendet wird. Andererseits ist ein zertifiziertes Erfassungsgerät, welches die zugeführte Elektrizität an der Ladestation oder im Fahrzeug messen kann, keine Option. Es würde neben den Manipulationsmöglichkeiten auch äussert schwer zu kommunizieren sein, warum Personen, welche die Elektrizität mit eigenen Solaranlagen produzieren, dafür eine Abgabe bezahlen müssten. Zudem würden solche Messvorrichtungen die Bestrebungen hinsichtlich des bidirektionalen Ladens behindern.

Somit führt bei der Umsetzung einer RUC aus heutiger Sicht kein Weg an der satellitengestützten Erhebung aller Bewegungen und dem folgenden Kartenabgleich vorbei.[22] Dieser Ansatz erlaubt zudem die Möglichkeit, zu einem späteren Zeitpunkt Preisdifferenzierungen anhand der benutzten Strassen oder dem Zeitpunkt der Fahrt einzuführen, sofern der Schutz der Privatsphäre gewahrt bleibt.

Aus diesem Grund bedingt eine funktionierende Strassengebührenerhebung einzig, dass basierend auf den Geodaten der Bepreisungsobjekte (Strassen, Brücken, Tunnels etc.) und anhand satellitengestützter Geolokalisationen die Standorte und gefahrenen Strecken von Fahrzeugen (Nutzungsdaten von Bepreisungssubjekten) eindeutig identifiziert und erfasst werden. Besonders wichtig ist dabei, dass die Privatsphäre durch geeignete rechtliche und technische Massnahmen geschützt wird. Die konkrete Gebührenerhebung ergibt sich dann aus der jeweiligen Tarifgestaltung und Tariffestlegung (Bundesrat, 2016).

[22] S. mit dem gleichen Ergebnis (AGORA, 2022), wonach das Konzept der satellitengestützten Erfassung als "einzige valable, zukunftstaugliche Lösung" bezeichnet wird.

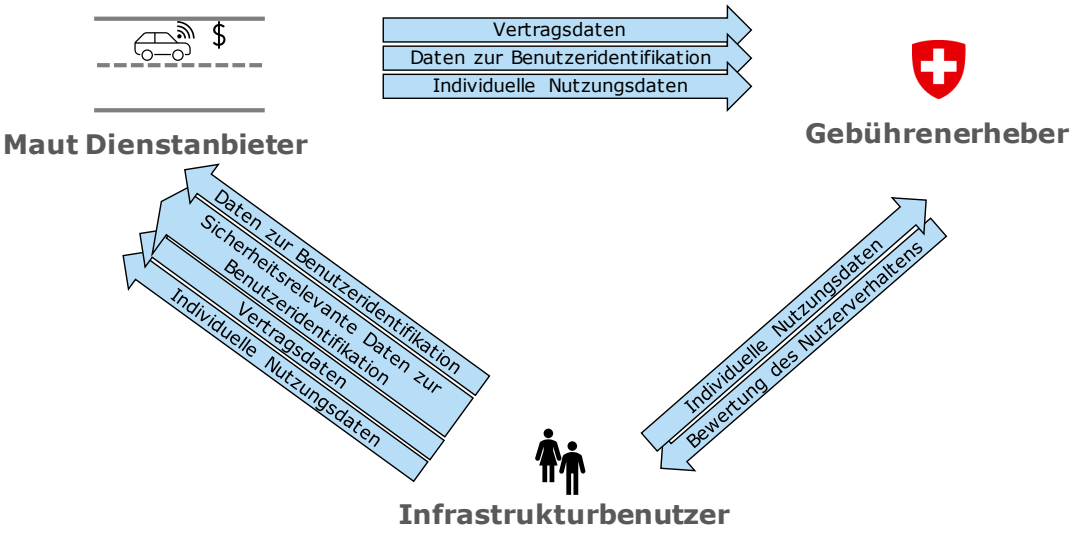


Abb. 39 *Beschreibung der notwendigen Datenflüsse bei RUC*

Damit die RUC erhoben werden kann, müssen unterschiedliche Datentypen zwischen dem Infrastrukturbenutzer, dem Gebührenerheber und dem Maut-Dienstanbieter fliessen: *Vertragsdaten*, *Daten zur Benutzeridentifikation*, *sicherheitsrelevante Daten zur Benutzeridentifikation*, *individuelle Nutzungsdaten* und *Bewertung des Nutzerverhaltens*. Diese Datenflüsse wurden anhand der Prozessanalyse in Kap. 2.3.2 hergeleitet.

Die *Daten zur Benutzeridentifikation* werden vom Infrastrukturbenutzer via den Maut-Dienstanbieter an den Gebührenerheber übermittelt. Zudem übermittelt der Infrastrukturbenutzer *individuelle Nutzungsdaten* in Form der gefahrenen Strecken je Fahrzeugtyp dem Maut-Dienstanbieter. Dieser leitet die Daten an den Gebührenerheber weiter – heute typischerweise in unbearbeiteter Form – der daraus die Höhe der Gebühr berechnet und dem Infrastrukturbenutzer die Rechnung via Maut-Dienstanbieter zustellt. Aus Sicht des Datenschutzes wäre es natürlich wünschenswert, wenn die Nutzungsdaten nur in aggregierter Form vom Maut-Dienstanbieter an den Gebührenerheber übermittelt würden (bspw. in Form einer täglichen Gesamtfahrleistung, ohne Ortsangaben). Der nachstehend in 4.4. vorgestellte technisch/organisatorische Ansatz wird sich dieses Aspekts besonders annehmen.

Eine Data Governance ohne Maut-Dienstanbieter, bei der der Infrastrukturbenutzer die relevanten Daten selbst an den Gebührenerheber übermittelt, wirkt zwar auf den ersten Blick hinsichtlich des Privatsphärenschutzes weniger problematisch, ist aber kaum praktikabel. Realistischerweise sind nicht alle Infrastrukturbenutzer in der Lage oder gewillt, die relevanten Daten selbst zu erheben, auszuwerten und an den Gebührenerheber weiterzuleiten. Im Weiteren müsste ein Infrastrukturbenutzer, der international unterwegs ist, je nach Land dem jeweils zuständigen Gebührenerheber die Daten zukommen lassen. Gleiches gilt zudem für weitere Smart Mobility-Anwendungen wie z.B. Mobility Pricing. Auch für den Gebührenerheber ist es ein zusätzlicher Aufwand, die Daten jedes Infrastrukturbenutzers entgegenzunehmen bzw. einzufordern. Damit das System effizient funktionieren kann, hat der Gebührenerheber auch dafür Sorge zu tragen, einen Markt zu kreieren, in dem ein Infrastrukturbenutzer den für ihn besten Maut-Dienstleister wählen kann.

Um die Korrektheit und Vollständigkeit der Fahrtdeklarationen der Infrastrukturbenutzer zu überprüfen, finden auf der Infrastruktur stichprobenhaft automatisierte Kontrollen statt. Bei diesen Kontrollen werden dem Gebührenerheber *individuelle Nutzungsdaten* in Form von Bildaufnahmen von Passagen der Fahrzeuge übermittelt. Der Gebührenerheber gleicht die Fahrtdeklarationen mit den aufgenommenen Passagen ab. Im Fall einer Falschdeklaration wird das Verhalten des Infrastrukturbenutzers gemäss den gesetzlichen Vorgaben bewertet. Bei einer festgestellten Zuwiderhandlung wird die Ahndung eingeleitet.

4.2. Datenzuordnung

Im nächsten Schritt ist zu klären, welche Akteure aus welchen Gründen welche Daten tatsächlich oder rechtlich kontrollieren. Dazu ist die Anwendung der verschiedenen rechtlichen Instrumente auf die Daten zu prüfen (siehe Kap. 3.2 oben).

Bei praktisch allen von den Infrastrukturbenutzern an die Maut-Dienstanbieter übermittelten Daten (*Daten zur Benutzeridentifikation*; *sicherheitsrelevante Daten zur Benutzeridentifikation*, *Vertragsdaten* und *individuelle Nutzungsdaten*) handelt es sich um Personendaten im Sinne des DSG bzw. nDSG. Den betroffenen Personen stehen damit in Bezug auf diese Daten zahlreiche Ansprüche und Rechtsbehelfe des **Datenschutzrechts** zu. Auf diese Rechte können sie grundsätzlich nicht verzichten. Dass bisweilen nicht der Halter oder die Halterin selbst das Fahrzeug fährt, spielt hierbei keine Rolle; identifizierbar ist die betroffene Person praktisch immer. Weil ein Bewegungsprofil in Bezug auf ein einzelnes Fahrzeug erstellt wird, liegt ein Profiling vor (Art. 5 lit. f nDSG), möglicherweise sogar ein Profiling mit hohem Risiko (Art. 5 lit. g nDSG). Ist Letzteres der Fall, werden besondere Anforderungen an eine allfällige Einwilligung zur Datenbearbeitung gestellt, sie muss ausdrücklich erfolgen (Art. 6 Abs. 7 lit. bB nDSG). Das gleiche gilt, wenn ein Bundesorgan das Profiling vornimmt (Art. 6 Abs. 7 lit. c nDSG).

Aus Sicht der Maut-Dienstanbieter sind die bei den Infrastrukturbenutzern erhobenen Daten der zentrale Baustein ihres Geschäftsmodells. Trotzdem hat hier – im Gegensatz zu den MaaS-Angeboten - der **strafrechtliche und wettbewerbsrechtliche Geheimnisschutz** einen geringeren Stellenwert, weil der primäre Zweck der Erhebung der Mobilitätsdaten darin liegt, die Benutzungsgebühr zu berechnen und (via Gebührenerheber) in Rechnung zu stellen. Dennoch ist grundsätzlich auch denkbar, dass die Maut-Dienstanbieter oder der Gebührenerheber die erhobenen Daten anders nutzen (sog. Sekundärnutzungen), z.B. um den Infrastrukturbenutzern weitere Angebote zu machen oder für verschiedene verkehrsplanerische Zwecke. Selbstverständlich müsste die Sekundärnutzung die entsprechenden datenschutzrechtlichen Vorgaben wahren. Ob solche Sekundärnutzungen erwünscht sind, ist eine andere Frage und separat zu diskutieren (s. hinten *4.4.b*). Demgegenüber besteht an den zwischen den Akteuren ausgetauschten Daten **kein immaterialgüterrechtlicher Schutz**.

4.3. Datennutzung

Die Tatsache, dass es sich bei den wichtigsten Daten, die für das Funktionieren von RUC benötigt werden, um Personendaten handelt, steht der Datennutzung nicht grundsätzlich entgegen. Zwar müssen die Maut-Dienstanbieter eine Reihe von Pflichten einhalten (so z.B. die Pflicht, die betroffenen Personen bei der Beschaffung von Personendaten angemessen zu informieren, Art. 19 nDSG) und unter Einhaltung der Datenbearbeitungsgrundsätze zu bearbeiten (Art. 12 Abs. 2 DSG, Art. 30 Abs. 2 nDSG). Es sind allerdings keine Anhaltspunkte ersichtlich, weshalb die Maut-Dienstanbieter diese Grundsätze nicht einhalten können. Selbst wenn – wie oben ausgeführt – aufgrund des Vorliegens eines Profilings, strengere Anforderungen gestellt werden (Ausdrücklichkeit einer gegebenenfalls notwendigen Einwilligung), können diese durch geeignete Vorkehrungen ohne weiteres erfüllt werden.

Damit besteht aber noch keine Gewähr für eine reibungslose Datennutzung. Eine solche hängt im Rahmen der RUC nämlich weniger vom rechtlichen, sondern eher vom faktischen

Datenschutz ab: Massgebend ist, ob die Infrastrukturnutzer den anderen Akteuren das notwendige Vertrauen schenken, dass der Datenschutz effektiv eingehalten wird. Dieses Vertrauen ist angesichts der Tatsache, dass zwecks Erhebung von Gebühren detaillierte Bewegungsprofile erstellt werden müssen, zentral. Das Argument, weniger invasive Erhebungsmethoden könnten nicht den vorgegebenen Zweck erfüllen, mag zwar sachlich richtig sein, vermag aber für sich alleine wohl nicht, dem Vorhaben zu politischer und gesellschaftlicher Akzeptanz zu verhelfen. Fehlt diese Akzeptanz, kann Widerstand bei der politischen Umsetzung von RUC dazu führen, dass die notwendige Verfassungsänderung abgelehnt wird oder gegen entsprechende gesetzliche Grundlagen das Referendum ergriffen wird.

Zudem kommt die erfolgreiche Umsetzung von RUC nicht ohne Vorgaben in Bezug auf die technische Implementierung aus: Nur wenn die Daten aller Verkehrsteilnehmer erfasst werden, kann die Benutzungsgebühr rechtsgleich erhoben werden. Und schliesslich muss die RUC gegenüber allen Verkehrsteilnehmern durchgesetzt werden können.

4.4. Beseitigung von Hindernissen

Vergleicht man dies mit der angestrebten Zielsetzung (siehe vorn in *4.1.*), drängen sich in Bezug auf RUC eine Reihe von Governance-Massnahmen auf. Wie bei den MaaS-Angeboten müssen diese auch bei RUC das **Vertrauen aller Akteure** in das Funktionieren der Gebührenerhebung stärken. Die Systeme müssen sich die gesellschaftliche Akzeptanz mit zielgerichteten Massnahmen erarbeiten.

Im Folgenden wird davon ausgegangen, die Data Governance setze an einer **dezentralen Infrastruktur** an, weil jeder Maut-Dienstanbieter grundsätzlich für seine eigene Infrastruktur verantwortlich ist. (Zu den Gründen für diese Wahl vorstehend Kap. 5.3.2).

Die Formulierung von Data Governance-Massnahmen kann anhand der folgenden Zusammenstellung möglicher Hindernisse strukturiert werden.

4.4 Abgleich Welche Governance Massnahmen können die wesentlichen Hindernisse adressieren?

	Hindernisse	Governance-Massnahmen
a.	Erfassung aller Infrastrukturbenutzer	• nutzungsspezifische Angebote
b.	Datenschutz	• privacy by design • TEE
c.	Durchsetzbarkeit	• Kontrollorgane • TEE • Spot-Checking mittels Road-Side Units
d.	Fehlendes Vertrauen (gefühlter Datenschutz)	• Offenlegung der Algorithmen • Protokollierung (Logging) der Datenzugriffe • Korrektheit der Berechnung • Dateneinsicht des Nutzers • Nachvollziehbarkeit

***Abb. 40**: Hindernisse für eine flächendeckende Strassengebührenerhebung und mögliche Governance-Massnahmen, um diese zu beheben.*

4.4.a. Erfassung aller Infrastrukturbenutzer

Da es sich bei einer RUC um eine verpflichtende Abgabe handelt, müssen die Daten aller Infrastrukturbenutzer erfasst werden können – und zwar ungeachtet von deren Wohnsitz, Fahrzeugzulassung und Fahrzeugtyp. Nur wenn alle Infrastrukturbenutzer erfasst sind, kommt es zwischen diesen nicht zu Ungleichbehandlungen. Zu rechtfertigen wäre

allerdings eine Ausnahme für kurzzeitig in der Schweiz fahrende Personen, z.B. Touristen, die anstelle einer benutzerspezifischen Erfassung eine vorgängig festgelegte Pauschale entrichten. Eine solche Pauschale müsste in der Höhe so angesetzt werden, dass sie im Regelfall nicht zu einer geringeren Abgabe führt als eine benutzerspezifische Abgabe. Eine allgemeine Wahlmöglichkeit für Infrastrukturbenutzer zwischen der Entrichtung einer individualisierten Gebühr und einer gegenüber der voraussichtlichen Gebühr leicht höheren Pauschale ist dagegen abzulehnen. Eine solche Lösung würde dazu führen, dass finanziell besser situierte Infrastrukturbenutzer sich die teurere, aber aus ihrer Sicht vielleicht datenschutzfreundlichere Option erkaufen könnten, während finanziell schlechter gestellte Personen diese Möglichkeit faktisch nicht nutzen können.

In Bezug auf die Frage, *wie* die Infrastrukturbenutzer an der RUC teilnehmen, haben sie aber Wahlfreiheit. Jeder Infrastrukturbenutzer und jede Infrastrukturbenutzerin kann aufgrund der eigenen Bedürfnisse den Zugang wählen, der für ihn oder sie am besten passt. Damit muss die RUC in technischer Hinsicht mindestens die folgenden Modi anbieten:

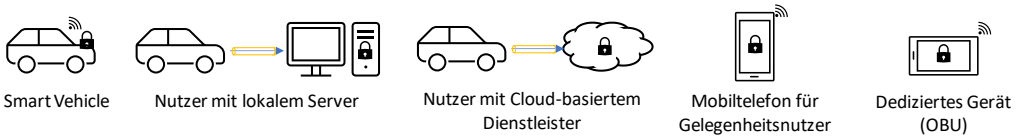


***Abb. 41** Erfassung aller Infrastrukturbenutzer*

- **Smart Vehicle** / Connected car:
  Um die Zugangsbarrieren möglichst gering zu halten, ist eine möglichst hohe Kompatibilität mit in aktuellen Fahrzeugen verbauten Geräten (GNSS/CN Technologien sind schon an Bord) eine grundlegende Voraussetzung. Die Daten werden in diesem Fall automatisiert vom Fahrzeug erhoben (siehe Kap. 1.6) und in das nötige technische Format gebracht, bevor sie an den Maut-Dienstanbieter übertragen werden.
- **Nutzer mit** lokalem oder Cloud-basiertem **Server**:
  Im Fall, dass die notwendige Vorverarbeitung der Daten aus Technologiegründen nicht im Fahrzeug passieren kann, oder dies vom Infrastrukturbenutzer nicht gewünscht ist, können die Rohdaten an einen externen Server übertragen werden, wo die Datenaufbereitung stattfindet. Dies kann – im Fall technologie-affiner Nutzer – entweder ein vom Infrastrukturbenutzer selbst kontrollierter Server sein, oder ein von einem Cloud-Dienstleister, wie beispielsweise einem internationalen Maut-Dienstanbieter, angebotener Service. Die Übertragung an den Maut-Dienstanbieter erfolgt dann durch diesen Server.
  Wiewohl seit der Einführung des seit 2018 in neuen PKW-Modellen verpflichtenden eCall-Notrufsystems die technischen Voraussetzungen in jedem Fahrzeug gegeben sind, müssten die Zugriffsrechte auf diese Funktionalität gegebenenfalls erst geschaffen werden. Es darf daher insbesondere keine inhärente Möglichkeit zur fahrzeugseitigen Datenerfassung, -verarbeitung, und -übertragung vorausgesetzt werden.

Aus Gründen der Rückwärtskompatibilität ist daher zudem zumindest eine Auswahl der folgenden Modi notwendig:

- **Mobiltelefone für Gelegenheitsnutzer:**
  Die Bereitstellung einer dedizierten Applikation für Mobiltelefone, welche unter Nutzung der Funktionalitäten des Mobiltelefons die Daten erfasst, verarbeitet, und überträgt, stellt eine Möglichkeit dar, um allen Nutzern das korrekte Rapportieren der Daten zu ermöglichen. Gerade für ausländische Nutzer kann dies eine niederschwellige Möglichkeit darstellen.
- **Dediziertes Gerät (OBU):**
  Alternativ zum Mobiltelefon können die notwendigen Funktionen auch mittels einer On-Board Unit (OBU) umgesetzt werden. Zu beachten ist hier, dass die Verwendung einer OBU nicht zwingend notwendig sein darf, und alternative Möglichkeiten zur Verfügung stehen müssen.

4.4.b. Datenschutz

Geht man – wie in diesem Forschungsprojekt – bei der Planung und Umsetzung eines RUC-Systems davon aus, dass dieses auf der Erhebung von GNSS-Daten und einem Kartenabgleich basiert, stellt sich die zentrale Frage, wie es datenschutzkonform ausgestaltet werden kann. Die rechtlichen Hürden sind dabei nicht unüberwindbar: Handelt es sich bei den Maut-Dienstanbietern um private Unternehmen, können diese über alle möglichen Bearbeitungen und Bearbeitungszwecke informieren und ggf. in Bezug auf diese die Einwilligung der Infrastrukturbenutzer einholen. Soweit Bundesorgane Daten bearbeiten, kann dafür eine gesetzliche Grundlage geschaffen werden.

Diese Vorkehrungen allein sind angesichts der massenhaften Erhebung von Mobilitätsdaten allerdings nicht ausreichend. Insbesondere wenn der mit Art. 7 nDSG neu ins Gesetz aufgenommen Grundsatz des Datenschutzes durch Technik ("privacy by design") bzw. der datenschutzfreundlichen Voreinstellungen ("privacy by default") ernst genommen wird, bedarf es des Einsatzes geeigneter technischer Mittel, um die Privatsphäre der Einzelnen zu wahren.

Technisch sorgfältig konstruierte Systeme vermeiden einzelne Punkte des Versagens (*single point of failure*), erhöhen dadurch die Datensicherheit, verringern die Gefahr von *data breaches* und setzen in technischer und organisatorischer Hinsicht auf die Einhaltung eines Mehraugenprinzips (z.B. durch externe Audits, Offenlegung der Algorithmen, etc.).

Ein derartiges System lässt sich wie folgt beschreiben (vgl. Abb. 42):

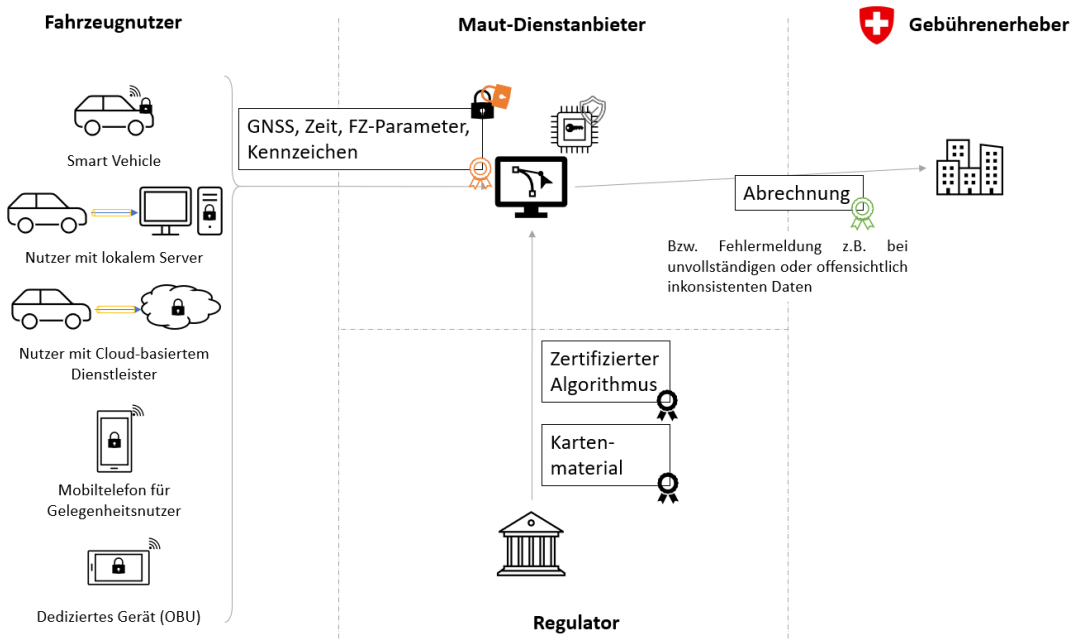


***Abb. 42** Mögliche Architektur einer datenschutzfreundlichen Lösung zur Strassengebührenerhebung*

Mittels GNSS erfasste Positionierungsdaten werden an einen vom Nutzer gewählten Maut-Dienstanbieter übertragen, welcher mittels einer Karte des mautpflichtigen Wegenetzes die anfallende Strassengebühr feststellt und an den Gebührenerheber übermittelt.

Um hohe technische Standards bezüglich Data Governance im Allgemeinen und zum Schutz der Bewegungsprofile einzelner Infrastrukturbenutzer im Speziellen zu erreichen, muss gewährleistet werden, dass sensitive Daten nur für die Gebührenberechnung verwendet werden können, nicht jedoch im Klartext von jeglicher Entität abseits des Infrastrukturbenutzers selbst gelesen, verarbeitet, oder manipuliert werden können. Von den in Kapitel 4 vorgestellten technologischen Instrumenten scheiden Multi-Party Computation (Kapitel 4.2.1) sowie vollhomomorphe Verschlüsselung (Kapitel 4.2.3) trotz signifikanter Fortschritte aus Effizienzgründen für die komplexen durchzuführenden Operationen für ein

praktikables, skalierendes und kosteneffizientes System in ihren aktuellen Ausprägungen aus.

Die präsentierte Lösung basiert daher auf Trusted Execution Environments (TEEs, Kapitel 4.2.2). Im Wesentlichen wird durch die Verwendung von TEEs garantiert, dass die Nutzerdaten ausschliesslich von zertifizierten Algorithmen genutzt werden können, während jeglicher andere Zugriff verhindert wird, da die Daten sowie sämtliche Zwischenresultate der Berechnung im Speicher („at rest“) ausschliesslich in verschlüsselter Form vorliegen, und lediglich während der Verarbeitung („in use“) entschlüsselt werden. Die Kosten der Verschlüsselung sind dabei dank der bereits etablierten Technologie und einer weit fortgeschrittenen Standardisierung gering.

Als zentrale Designentscheidung sei hier noch erwähnt, dass auf Fahrzeugseite lediglich eine Möglichkeit zur Erfassung von Positionsdaten sowie zur Datenübertragung vorausgesetzt wird, um höchstmögliche Kompatibilität mit bestehenden Fahrzeugflotten zu erreichen.

Die zentralen Phasen der Gebührenerhebung werden im Folgenden näher skizziert:

Datenerfassung und -übertragung

Die GNSS Daten werden periodisch fahrzeugseitig gemeinsam mit einem aktuellen Zeitstempel erfasst. Die Frequenz der Datenerfassung hängt unter anderem von der Präzision der Datenerfassung, der Genauigkeit des gewählten Algorithmus zur Karteneinpassung, welcher die GNSS-Daten mit der validen Strassenkarte abgleicht, und der verlangten Genauigkeit der Distanzberechnung ab. Zu erwartende Übertragungsintervalle liegen im Bereich von 10s bis 30s.

Anschliessend werden diese Daten, um für die Gebührenerhebung relevante, variable Fahrzeugparameter (z.B. Anhänger, Gewicht, etc.) sowie das Kennzeichen erweitert.

Abhängig vom konkreten Szenario kann diese Verarbeitung an unterschiedlichen Stellen erfolgen, wobei keine zentrale Wahl für das Gesamtsystem getroffen werden muss, sondern die Wahl jeder einzelnen abgabepflichtigen (natürlichen oder juristischen) Person freigestellt werden kann.

Die bereits erwähnte Vorverarbeitung der Daten beinhaltet in diesem Konzept insbesondere die Verschlüsselung aller relevanten Daten unter einem vom Maut-Dienstanbieter innerhalb einer TEE erstellten kryptographischen Schlüssel. Dadurch wird sichergestellt, dass die Daten lediglich innerhalb dieser TEE zur weiteren Verarbeitung im Klartext vorliegen, jedoch für keine Partei – einschliesslich des Maut-Dienstanbieters – im Klartext lesbar sind. Durch entsprechende Zertifizierungsprozesse und Transparenz darüber, welche Algorithmen innerhalb der TEE ausgeführt werden können, kann der Datenschutz so technisch garantiert werden.

Zudem werden die Daten nutzerseitig signiert, um eine eindeutige spätere Zuordnung von Daten an einen Nutzer zu ermöglichen. Optional kann durch eine zusätzliche Verschlüsselung mittels eines vom Nutzer kontrollierten Schlüssels der spätere Zugriff des Nutzers auf seine Daten ermöglicht werden.

Während im Fall des Smart Vehicles, bei der Verwendung eines Mobiltelefons, einer OBU sowie der Verwendung eines vom Benutzer kontrollierten Servers die Klartextdaten ausschliesslich dem Nutzer vorliegen, ist zu beachten, dass bei der Verwendung eines Cloudbasierten Anbieters zur Datenverarbeitung die Verschlüsselung erst dort erfolgt, und dieser potentiell Zugriff auf die Bewegungsdaten eines Nutzers erhält. Die Wahl eines solchen Serviceanbieters steht dem Nutzer jedoch frei und wird auf Systemebene keineswegs vorgeschrieben, wodurch etwaige Vertrauensbedenken ausgeräumt werden können.

Algorithmus und Kartenmaterial

Der Algorithmus, welcher der Gebührenerhebung zugrunde liegt sowie das zu verwendende Kartenmaterial werden vom Regulator in authentischer Form öffentlich und für jedermann einsehbar zur Verfügung gestellt, wobei die spezifischen Prozesse hier je nach TEE-Anbieter variieren können.

Eine vom Mautdienstanbieter und vom Regulator unabhängige und neutrale Stelle, die über die entsprechenden fachlichen Kompetenzen verfügt, hat die für die Berechnung der

Gebühr eingesetzten Algorithmen zu zertifizieren. Über diese Stelle müssten auch weitere Algorithmen zertifiziert werden, die für eine allfällige Sekundärnutzung der Daten eingesetzt werden. Denkbar wäre z.B., dass diese Zertifizierungsstelle im Eidgenössischen Institut für Metrologie (METAS) oder in der Digitalen Verwaltung Schweiz (DVS) angesiedelt wird. Allgemein ist bei der Wahl der Behörde zu berücksichtigen, wie viele Aufgaben sie hat (z.B. in Bezug auf andere Mobilitätsdienstleistungen wie MaaS, vgl. in Kap. 5.2.4 Absatz 4.4.a) oder in Bezug auf die Anzahl der voraussichtlich durchzuführenden Zertifizierungen.

Abrechnung

In einem ersten Schritt verifiziert der Maut-Dienstanbieter die Authentizität des Algorithmus und des Kartenmaterials.

Anschliessend erfolgt die Rechnungslegung innerhalb der TEE. Während innerhalb dieser Enklave data in use im Klartext vorliegen, werden data at rest (insbesondere also auf Festplatten abgelegte Daten) lediglich in verschlüsselter Form abgelegt. Aufgrund der Isolierung der Prozesse innerhalb der TEE sind Nutzerdaten daher von unautorisiertem Zugriff geschützt.

Am Ende der Berechnung erfolgt die Ausgabe eines digital signierten Belegs, welcher an den Gebührenerheber übermittelt wird.

Da innerhalb einer TEE beliebige Berechnungen durchgeführt werden können, sofern diese vorab authentisiert wurden, und dadurch keine Einschränkung der Funktionalität oder Nutzbarkeit der Daten erzwungen wird, ist es möglich, im Zuge der Rechnungslegung z.B. bereits bestehende Prozesse zur Überprüfung der Plausibilität der Daten anzuwenden und ggf. eine entsprechende Fehlermeldung auszugegeben.

Sekundärnutzung der Daten

Das hier präsentierte System beeinflusst auch die weiteren Verwendungsmöglichkeiten der erhobenen Daten, die sog. Sekundärnutzung. Denn solche Sekundärnutzungen sind von vornherein nur möglich, wenn dafür ein zertifizierter Algorithmus vorliegt, der auf die erhobenen Mobilitätsdaten angewendet werden kann. Weil die Maut-Dienstanbieter trotz Infrastruktur- und Dienstleistungswettbewerb einen öffentlichen Auftrag erfüllen, sind erhebliche Bedenken angebracht, soweit es darum geht, ob einzelne dieser Akteure eigene Algorithmen zertifizieren lassen können, mit denen Sie Funktionen umsetzen, die über die blosse RUC und deren Durchsetzbarkeit (sogl. 4.4.c) hinausgehen. Zudem dürfte der Nutzen bei vielen Anwendungen ohnehin beschränkt sein, solange sie nicht *alle* Maut-Dienstanbieter – und damit alle Fahrzeuge – erfassen. Umgekehrt stellt sich die Frage, ob und wie mehrere Maut-Dienstanbieter überhaupt miteinander in einen Wettbewerb treten können, wenn sie alle die gleiche Basisdienstleistung erbringen. Jedenfalls könnten sie nicht mit besonderen Leistungen um neue Nutzer werben. Immerhin könnten sie aber mit einer möglichst effizienten Abwicklung intern ihre Profitabilität steigern. Ob und in welchem Umfang Sekundärnutzungen der Maut-Dienstanbieter möglich sein können, ohne das Vertrauen der Nutzer zu gefährden (s.a. sogl. 4.4.d), muss noch vertieft diskutiert werden.

Fraglich ist indes, ob nicht zusätzliche Algorithmen zertifiziert und eingesetzt werden können, mit denen sich auf aggregierter Ebene wichtige Informationen zur Verkehrsplanung gewinnen liessen. Diese Sekundärnutzung sollte auf Gesetzesstufe geregelt werden – unabhängig von der Tatsache, dass auch diese innerhalb eines auf TEE beruhenden Systems erfolgt.

4.4.c. Durchsetzbarkeit

In einem flächendeckenden Strassengebührensystem ist ein effizienter Kontrollmechanismus notwendig, um möglichst alle Nutzer zu veranlassen, korrekte Daten zu liefern und Gebühren zu bezahlen. Ein rein physischer Kontrollansatz, beispielsweise mittels Spot-Checking und Ausleiten von verdächtigen Fahrzeugen aus dem fliessenden Verkehr durch befugte Kontrollorgane ist zu personalintensiv und zu wenig skalierbar, um den notwendigen Kontrolldruck zu erreichen. Nur mit einem automatisierten Ansatz kann die erforderliche Kontrolldichte generiert werden. Die dabei generierten Datensätze von Durchfahrten, insbesondere Bild- bzw. Videoaufnahmen, stellen hohe Anforderungen an den

Datenschutz. Die Übermittlung und Bearbeitung dieser Datensätze muss auf nachvollziehbare Weise datenschutzkonform erfolgen, insbesondere um die Akzeptanz des Systems nicht zu untergraben.

Die in Abb. 43 vorgeschlagene Lösung erlaubt eine Automatisierung der Erhebung der Kontrolldaten unter Wahrung des Datenschutzes, abermals unter der Verwendung von TEE.

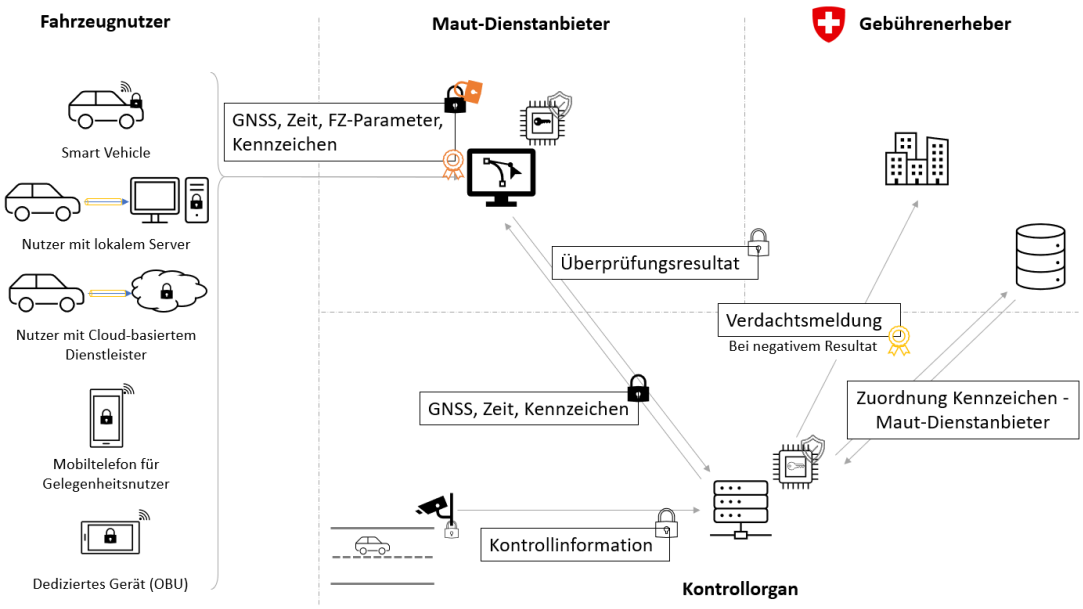


Abb. 43 Übersichtsbild zur datenschutzfreundlichen Durchsetzbarkeit

In diesem Konzept wird durch – möglicherweise mobile – strassenseitige Kontrolleinheiten (Roadside units, RSU) die für die Überprüfung notwendigen Kontrollinformation erhoben (z.B. Bilddaten oder bereits extrahierte Fahrzeuginformationen). Diese Daten werden im Sinne eines *Edge Computing*-Ansatzes bereits dezentral auf Seite der Kontrollgeräte verschlüsselt, wofür ein vom TEE des Kontrollorgans zur Verfügung gestellter Schlüssel verwendet wird. Die erhobenen verschlüsselten Informationen werden beim Kontrollorgan gespeichert.

Die Kontrollorgan-seitige TEE gleicht im Anschluss die erhaltenen Daten mit der TEE des Maut-Dienstanbieters ab. Dabei wird sichergestellt, dass keine sensitiven Klartextdaten übertragen werden, sondern nach einem initialen Schlüsselaustausch die beiden TEEs lediglich verschlüsselte Daten austauschen. Im Zuge des Abgleichs kommuniziert die TEE des Kontrollorgans relevante Fahrzeuginformationen sowie Position und Zeitstempel der Überprüfung an den Maut-Dienstanbieter, welcher seinerseits überprüft, ob für den angegebenen Zeitpunkt eine Verrechnung des angegebenen Fahrzeugs stattgefunden hat. Resultiert aus dieser Überprüfung kein Vergehen, können die Daten seitens des Kontrollorgans verworfen werden. Kontrollinformationen ehrlicher Nutzer, welche korrekte Daten rapportiert haben, werden keiner Partei im Klartext zur Verfügung gestellt, wodurch die Privatsphäre dieser Nutzer bestmöglich geschützt wird.

Im Falle einer negativen Überprüfung kann eine Verdachtsmeldung beispielsweise an den Gebührenerheber erfolgen. Diese Verdachtsmeldung kann alle für die weitere Verfolgung notwendigen Daten wie beispielsweise die Klartextdaten der Kontrollinformationen enthalten.

Im Falle mehrerer parallel operierender Maut-Dienstanbieter muss vor dem Abgleich der Kontrollinformationen eine Abfrage der Zuordnung eines bestimmten Fahrzeugs, beispielsweise über das Kennzeichen, zu einem bestimmten Maut-Dienstanbieter erfolgen.

4.4.d. Fehlendes Vertrauen (gefühlter Datenschutz)

Das Vertrauen aller Akteure in eine RUC-Lösung ist entscheidend für die breite gesellschaftliche Akzeptanz. Die Einhaltung der datenschutzrechtlichen Bestimmungen – d.h. der Datenbearbeitungsgrundsätze und das Vorliegen etwaiger Rechtfertigungsgründe – allein sind kein Garant für diese Akzeptanz.

Stattdessen ist oft massgebend, ob die Spielregeln für die Akteure von Anfang an klar sind und wie vertrauenswürdig der Verantwortliche eingeschätzt wird. Man spricht dabei vom "gefühlten Datenschutz" (Rosenthal, 2012, S.88 ff.).

Um diesem gefühlten Datenschutz Rechnung zu tragen und die notwendige Akzeptanz zu erreichen, sind neben der Einhaltung der datenschutzrechtlichen Vorschriften auch technische und organisatorische Vorkehrungen notwendig, welche die missbräuchliche Verwendung der erhobenen Daten verhindern.

- Es sollten **technische Massnahmen** eingesetzt werden, welche den Zugriff auf Bewegungsprofile ausschliesslich zur Mauterhebung und verwandte Aufgaben ermöglichen. Neben starken Mechanismen für sichere Zugriffskontrollen und Protokollierung von Zugriffen bieten sich hier insbesondere die in Abschnitt 4 besprochenen Technologien an, um kryptographische Garantien geben zu können.
- Um durch die spätere Einführung zusätzlicher Funktionalitäten des Gesamtsystems die Privatsphäre der Benutzer nicht rückwirkend zu beeinträchtigen, ist weiters das regelmässige Rotieren des verwendeten Schlüsselmaterials zu beachten, wodurch auch die faktische **Löschung sensitiver Daten** durch das Zerstören des korrespondierenden geheimen Schlüssels innerhalb einer sicheren Umgebung nach Ablauf gesetzlicher oder vertraglicher Datenaufbewahrungsfristen erreicht werden kann.
- Um Missbrauch der erhobenen Daten zu vermeiden, ist es notwendig, höchstmögliche **Transparenz** des Systems zu garantieren. Auf politischer und Prozess-Seite werden transparente Regeln und Entscheidungsmechanismen benötigt, welche Algorithmen innerhalb der TEE ausgeführt werden dürfen. Auf technischer Seite sollten die Algorithmen selbst so weit wie möglich offengelegt werden, um eine Zertifizierung und Validierung nicht nur durch entsprechende Institutionen, sondern auch durch die Zivilgesellschaft, zu ermöglichen.
- Detailliertes **Logging** aller Zugriffe auf Daten und die Möglichkeit zur Einsichtnahme für Nutzer auf die entsprechenden Logs kann überdies vertrauensstiftend wirken. Um die Manipulationssicherheit der Log-Daten zu garantieren, könnten in einem verteilten System Distributed Ledgers als eine mögliche Technologie zur Dokumentation gewählt werden.
- Um Nutzern die **Überprüfung der Korrektheit** der Berechnungen zu ermöglichen, wäre ein möglicher Ansatz die bereits in Abschnitt 4.4.b erwähnte zusätzliche Verschlüsselung der übertragenen Daten unter einem kryptographischen Schlüssel des Nutzers. In Kombination mit der Offenlegung der implementierten Algorithmen und der öffentlichen Zugänglichkeit des Kartenmaterials könnte eine Referenzimplementierung zur Verfügung gestellt werden, welche die zu bezahlende Strassengebühr lokal nachzurechnen ermöglicht. Im Fall einer Inkonsistenz zwischen der vom Benutzer berechneten und der vorgeschriebenen Gebühr wäre eine Ombudsstelle zur Klärung etwaiger Abweichungen denkbar. Weiters muss dem Benutzer die Möglichkeit eingeräumt werden, fehlende Daten, beispielsweise aufgrund eines Defekts des Endgeräts, nachzumelden und zu korrigieren.
- Durch oben erwähnte Verschlüsselung unter einem kryptografischen Schlüssel des Nutzers erhält jener auch die Möglichkeit, die ihn betreffenden **Bewegungsdaten** nach eigenem Ermessen mit anderen Parteien zu **teilen**. Der durch diesen freiwilligen Datenzugriff gewonnene Mehrwert könnte möglicherweise einen zusätzlichen Anreiz für eine Marktbildung von Mautdienstanbietern darstellen.
- Letztlich ist insbesondere bei **kommerziellen Fahrzeugvermietern** oder Car-Sharing Anbietern zu unterscheiden, dass Fahrzeughalter und Infrastrukturbenutzer voneinander abweichen können und üblicherweise der Fahrzeughalter die entsprechenden Verträge mit Maut-Dienstanbietern abschliessen wird und dadurch die oben erwähnten Einsichtsmöglichkeiten wahrnehmen kann. Um ein Tracking von Nutzern der Car-Sharing Angeboten zu vermeiden, können hier entsprechende Vertragsklauseln dienen oder auch das (freiwillige) externe Auditieren der Datenzugriffe durch die jeweiligen Anbieter.

Schliesslich müssen alle Vorkehrungen für die Infrastrukturnutzer – und damit aus Sicht der Bevölkerung – nachvollziehbar sein. Dafür müssen sie in verständlicher Form dargelegt werden können. Diese Aufgabe liegt zwar ausserhalb des hier zu entwickelnden Governance-Modells für Mobilitätsdaten, ist jedoch für eine breite gesellschaftliche Akzeptanz von grosser Bedeutung. Volle Transparenz durch Offenlegung der Algorithmen und Source-Codes kann erheblich dazu beitragen, das Vertrauen in eine datenbasiere Dienstleistung zu stärken. Dies hat sich bei der Entwicklung der SwissCovid Tracing App bestätigt. Obwohl deren Verwendung auf Freiwilligkeit beruht und die verwendeten Technologien schwer zu verstehen sind, wurde sie von einem grossen Teil der Bevölkerung akzeptiert und verwendet. Die völlige Transparenz des verwendeten Source-Codes[23] hat stark dazu beigetragen, das Vertrauen zu erhöhen[24].

[23] Siehe: https://github.com/DP-3T

[24] Mit der von Google und Apple adaptierten Lösung fand eine technologisch annähernd übereinstimmende Lösung Anwendung in unterschiedlichsten west-europäischen Ländern. https://www.google.com/covid19/exposurenotifications/

6 Evaluation des Governance-Modells

6.1 Vorgehensweise

Die Entwicklung und Evaluation des vorstehend präsentierten Data Governance-Modells basiert auf einem iterativen Prozess. In diesem Prozess wurden zunächst Mobilitätsangebote, Akteure und Datenflüsse systematisiert (Kap. 2). Danach wurden die juristischen (Kap. 0) und technischen (Kap. 4) Instrumente beschrieben, welche für die Governance von Mobilitätsdaten relevant sind. Auf dieser Grundlage wurden für MaaS und RUC spezifische Governance-Modelle entwickelt (Kap. 5.2 und 5.3) und gleichzeitig die Elemente eines generellen – für alle Mobilitätsangebote geltenden – Governance-Modells skizziert (Kap. 5.1). Dies so gewonnenen Erkenntnisse wurden in qualitativen Workshops sowie von AlgorithmWatch kritisch hinterfragt. Die Diskussionen haben insbesondere gezeigt, welche Aspekte im Hinblick auf den Erfolg einer Anwendung als kritisch eingeschätzt werden. Auf der Basis dieser Auseinandersetzung und der in den Workshops gewonnenen Erkenntnisse wurden sowohl das generelle Governance-Modell als auch die spezifischen Governance-Modelle angepasst und verfeinert. Im Projekt wurde keine Evaluation im sozialwissenschaftlichen Sinne vorgenommen – und zwar weder im Sinne einer klassischen ex post-Evaluation noch im Sinne einer ex ante-Evaluation (Regulierungsfolgenabschätzung). Entsprechend wurden auch keine sozialwissenschaftlichen Methoden verwendet. Stattdessen lautete der Forschungsauftrag, mit den Methoden der beteiligten Disziplinen der Rechtswissenschaften, Kryptographie und Mobilitätsforschung sowie unter Einbezug der Begleitkommission und weiteren Beteiligten eine «Data Governance», mithin ein theoretisches Konzept für die Nutzung von Mobilitätsdaten zu entwickeln.

Wie in Kap. 5.1.1 hergeleitet, ist zur Sicherstellung einer Data Governance das Zusammenspiel der organisatorischen, rechtlichen und technischen Governance notwendig. Vor diesem Hintergrund werden im Folgenden die einzelnen Schritte und die gewonnenen Erkenntnisse zusammengefasst.

6.2 Systematisierung von Mobilitätsangeboten

Die in Kapitel 2 entwickelte Kategorisierung von generischen Anwendungen, Prozessen und Datentypen sowie das generische Rollenmodell haben es erlaubt, die Vielfalt an Mobilitätsangeboten zu systematisieren. Die Ausarbeitung generischer Elemente hat eine systematische Analyse erst ermöglicht und sich bei der Analyse der einzelnen Mobilitätsangebote und bei der Entwicklung eines Data Governance-Modells bewährt:

Erstens legte die Strukturierung der Datenflüsse anhand der generischen Datentypen die Grundlage für die Erstellung der Governance-Modelle. Denn rasch zeigte sich, dass die Datenflüsse in der jeweiligen Mobilitätsanwendung in einem relativ hohen Detailgrad beschrieben werden müssen, damit eine rechtliche Einschätzung überhaupt möglich ist. Gleichzeitig ist eine gewisse Abstrahierung bei den Datentypen notwendig, weil ansonsten gar keine generellen Aussagen getroffen werden können.

Zweitens erwies sich auch das verwendete Rollenmodell als ein äusserst nützliches Instrument. Die Verantwortlichkeiten, welche den verschiedenen Akteuren im Rollenmodell zugeteilt werden, können klar abgegrenzt werden, selbst wenn einem Akteur in einem bestimmten Mobilitätsangebot einmal zwei Rollen zufallen sollten. Die Rolle des Regulators ist dabei nicht zwingend an eine Behörde oder einen Akteur im herkömmlichen Sinne gebunden, in einigen Mobilitätsangeboten kann der Regulator auch bloss abstrakt für das herrschende regulatorische Umfeld stehen.

Drittens konnten ausnahmslos alle betrachteten Smart Mobility-Anwendungen einem generischen Mobilitätsangebot zugeordnet werden. Insoweit hat sich auch diese systematische Vorgehensweise als sinnvoll erwiesen. Viele Geschäftsmodelle der Smart Mobility-Anwendungen beruhen, zumindest aus der Sichtweise der Datenflüsse, auf ähnlichen Ansätzen. Anhand einer Smart Mobility-Anwendung können so die Grundzüge eines Governance-Modells herausgearbeitet werden, welches repräsentativ für das generische Mobilitätsangebot steht und die Interessen aller beteiligten Akteure einbezieht.

Folglich eignet sich die angewendete Systematisierung, um die organisatorischen Aspekte hinsichtlich der Verantwortlichkeiten der unterschiedlichen Akteure einzuordnen. Dies bietet zudem eine erforderliche Grundlage, um die juristischen sowie technischen Aspekte zu entwickeln.

6.3 Anwendbarkeit der juristischen und technologischen Instrumente

6.3.1 Rechtliche Instrumente

Das Recht stellt zahlreiche Instrumente zur Verfügung mit denen Daten den Akteuren zugeordnet werden können. Jedes dieser Instrumente hat allerdings andere Anwendungsvoraussetzungen, Zielsetzungen und Rechtsfolgen: So schützt beispielsweise das Immaterialgüterrecht die Resultate kreativer und innovativer Prozesse, um Kreation und Innovation zu fördern und erlaubt es, allen anderen Akteuren die Nutzung so geschützter Daten zu verbieten. Der Schutz von Geschäftsgeheimnissen sichert demgegenüber die Kontrolle eines Akteurs über dessen Daten rechtlich ab, geht aber im Schutz nicht so weit wie die immaterialgüterrechtlichen Ansprüche. Das Datenschutzrecht wiederum bezieht sich nur auf personenbezogene Daten und vermittelt den Akteuren gewisse Kontrollrechte zum Schutz von deren Persönlichkeit.

Insgesamt kann sich so in Bezug auf Smart Mobility ein komplexes Geflecht von Zuordnungen ergeben. Welche Instrumente konkret wirken, hängt davon ab, welche Datentypen und welche Akteure beteiligt sind. Konkrete Aussagen lassen sich deswegen nicht generell, sondern nur in Bezug auf ein konkretes Mobilitätsangebot machen. Zu diesem Zweck wurden im Forschungsprojekt Prüfschemata entwickelt, mit denen sich schematisiert prüfen lässt, welche Akteure in einem konkreten Mobilitätsangebot an welchen Daten berechtigt sind. Diese Zuordnung ist wesentlich für die Data Governance: Die initiale Zuordnung von Daten kann die Nutzung bestimmter Mobilitätsangebote begünstigen aber auch erschweren oder auch verunmöglichen (und muss sodann im Rahmen der Data Governance korrigiert werden).

Im Gegensatz zu den Zuordnungsinstrumenten ist die Zahl der rechtlichen Instrumente, welche Akteuren einen Zugang zu den Daten anderer Akteure verschaffen, viel kleiner. Dennoch konnten im Projekt auch hier einige rechtliche Bestimmungen identifiziert werden, welche sich auf die Data Governance auswirken können. Es handelt sich einerseits um Daten, die mittels Öffentlichkeitsgesetz erlangt werden können und andererseits um spezifische Offenlegungspflichten in öffentlich-rechtlichen Spezialgesetzen, typischerweise betreffend konzessionierte Leistungserbringer. Unter besonderen Umständen kann schliesslich auch das Kartellgesetz Zugangsansprüche vermitteln.

6.3.2 Technologische Instrumente

Anhand der beiden gewählten Anwendungsfälle MaaS und RUC wird ersichtlich, dass die Wahl der technologischen Instrumente stark vom Mobilitätsangebot abhängt. Teilweiselässt sich ein Mobilitätsangebot nur so abstrakt beschreiben, dass es schwierig ist, valide technische Empfehlungen abzugeben; nicht nur die Skalierbarkeit, sondern gegebenenfalls die gesamte technische Machbarkeit hängt von Details der Datenflüsse und Schutzanforderungen ab, die u.U. nicht vollständig bekannt sind (vgl. Kap. 5.2). Umgekehrt erlaubt eine klare Spezifikation des Anwendungsfalls die konkrete Auswahl technologischer und kryptographischer Methoden für Datenschutz, Authentizität, oder Auditierbarkeit (vgl. Kap. 5.3).

Insbesondere veranschaulichen die beiden gewählten Anwendungsfälle, dass keine generischen technischen Empfehlungen für sämtliche Smart Mobility-Anwendungen abgegeben werden können, sondern diese anwendungsspezifisch erarbeitet werden müssen, um technologisch bestmöglich Datenschutz und Datensicherheit bei gleichzeitig hohem Anspruch an Effizienz und Skalierbarkeit umsetzen zu können. Hingegen erlaubt unsere vorgeschlagene Klassierung von Anwendungen, Daten und Prozessen in wenige generische Elemente, dass eine entwickelte Lösung grundsätzlich für eine ganze Klasse von Anwendungen eingesetzt werden kann.

Aufgrund der Schnelllebigkeit der kryptographischen und sicherheitsrelevanten Forschung sind zwingend aktuelle Entwicklungen in diese Abwägungen und Designs einzubeziehen, wodurch die genaue technologische Ausgestaltung jeweils die interdisziplinäre Zusammenarbeit von Experten mit domänenspezifischem Wissen aus dem Anwendungsfall einerseits, sowie dem Sicherheitsbereich andererseits erfordert. Aufgrund des ständig fortschreitenden Stands der Forschung ergibt sich auch aus Blick der Technologie die Forderung nach einer technologieneutralen Regulierung.

Bei jeder technischen Umsetzung sind zudem schliesslich mindestens zwei zentrale Fragen zu stellen: Einerseits muss das entwickelte System die gestellten funktionalen Anforderungen und Datenschutzanforderungen erfüllen, was auf mehreren Ebenen sichergestellt werden kann: zentrale kryptographische Bausteine werden dem Stand der Technik entsprechend von der wissenschaftlichen Community modelliert und als sicher bewiesen, Best Practices bei der Auswahl und Kombination von Komponenten müssen befolgt (z.B im Einklang mit den Empfehlungen der Agentur der Europäischen Union für Cybersicherheit[25] zu Cybersicherheits-Standards und Zertifizierung), und entsprechende Datenschutz-Folgeabschätzungen ausgeführt werden. Andererseits stellt sich jedoch auch nach Fertigstellung eines soliden Designs die Frage nach dessen korrekter Umsetzung und Implementierung. Neben der Auswahl hochqualitativer Bausteine für sicherheitssensitive Komponenten stellt insbesondere die erforderliche Art der Zertifizierung (Erst-, Zweit- oder Drittzertifizierung und deren Vertrauenswürdigkeit (ISO 15408) und Transparenz der Implementierung einen zentralen Aspekt dar, um über "gefühltes Vertrauen" auch Akzeptanz bei allen relevanten Stakeholdern einer Smart Mobility-Anwendung erreichen zu können.

6.4 Das Governance-Modell im Allgemeinen

Das generische Data Governance-Modell (Kapitel 5.1.2) wurde sowohl für den Anwendungsfall MaaS als auch für die Strassengebührenerhebung (RUC) entwickelt, angewendet und erfolgreich getestet. Es war für beide Anwendungen möglich, einem modellhaften Vorgehen in vier Schritten zu folgen:

1. Identifikation und Beschreibung der involvierten Akteure
2. Beschreibung der zu verwendenden Infrastruktur für den Datenaustausch
3. Darstellung des geltenden Rechtsrahmens (und dessen Einschränkungen)
4. Umsetzung der Data Governance.

Auch innerhalb des Schrittes der Umsetzung der Data Governance war es für beide Anwendungen möglich, dem zirkulären Vorgehen zu folgen:

4.1. Zielsetzung – gute Mobilitätsanwendung
4.2. Ausgangslage – Datenzuordnung
4.3. Anwendung – Datennutzung
4.4. Abgleich – Hindernisse

Nach den Punkten 4.1. bis 4.3. wird beim Abgleich und der Beseitigung der Hindernisse ersichtlich, ob und welche Massnahmen im jeweiligen Mobilitätsangebot zu treffen sind.

Dabei zeigt sich auch, dass sich dies je nach Anwendungsfall (bzw. Mobilitätsangebot) unterscheidet. Je nach der verwendeten Infrastruktur, den sich ergebenden Datenflüssen und der rechtlichen Kontrolle über die Daten kann der Schwerpunkt der Massnahmen eher auf dem rechtlichen oder auf dem technischen Aspekt liegen. Wesentlich ist auch, ob der Zugang zur Smart Mobility-Anwendung freiwillig oder verpflichtend ist. Im Fall von RUC ist es aufgrund der sensiblen personenbezogenen Datenflüsse, aber besonders auch aufgrund der verpflichtenden Teilnahme aller Verkehrsteilnehmenden notwendig, dass die Governance besonders hohe Ansprüche in Bezug auf den Datenschutz erfüllt. Entsprechend kann hier die Technik eine besondere Rolle spielen.

Dennoch hat sich das generische Data Governance-Modell insofern bewährt, als es – soweit ersichtlich – auf alle Mobilitätsanwendungen anwendbar ist und damit jeweils anwendungsspezifische Data Governance-Massnahmen entwickelt werden können.

25 ENISA, https://www.enisa.europa.eu/

6.5 Spezifische Anwendung des Governance-Modells

Im Folgenden werden die Governance-Modelle evaluiert, welche spezifisch für MaaS und RUC entwickelt wurden. Die Auswahl dieser zwei Mobilitätsangebote deckt einerseits eine weite Palette an Smart Mobility-Anwendungen beispielhaft ab. Gleichzeitig werfen beide Mobilitätsangebote sehr anspruchsvolle Governance-Fragen auf.

6.5.1 Das Governance-Modell für MaaS

Funktionierende Mobility-as-a-Service (MaaS)-Angebote setzen voraus, dass die Akteure in grossem Umfang Daten teilen. Anders als bei der RUC handelt es sich aber nicht um eine hoheitliche Aufgabe; ob MaaS-Dienste angeboten oder beansprucht werden, beruht auf Freiwilligkeit und hängt letztlich von den Motiven und Anreizen der beteiligten Akteure ab. Aber auch diese können durch die Governance beeinflusst werden.

Rahmenbedingungen

Im Zusammenhang mit MaaS zeigt ein Blick auf den geltenden Rechtsrahmen, dass der Gesetzgeber beim Erlass relevanter Bestimmungen implizit von monomodalem Reisen ausgegangen ist. Entsprechend bestehen in verschiedenen Regelungsbereichen Bestimmungen, die sich nicht oder nur schwer auf multimodales Reisen anwenden lassen. Für die unterschiedlichen Verkehrsträger gelten unterschiedlich strenge Regeln und beim Ausfall oder einer Verspätung in einem Teil der Reisekette gelten keine einheitlichen Regeln betreffend Anspruch auf Weiterreise, Erstattung oder Entschädigung. Eine Anpassung des Rechtsrahmens könnte massgeblich zur Steigerung der Attraktivität von MaaS-Angeboten beitragen.

Infrastruktur

Bei der systematischen Anwendung des Governance-Modells ergibt sich, dass die Wahl der technischen Infrastruktur bei MaaS entscheidend ist. Dies wird deutlich, sobald gedanklich zwischen der Infrastrukturebene (wo der Datenaustausch stattfindet) und der Dienstleistungsebene (wo die MaaS-Anbieter mit ihren – auf den Daten aufbauenden – Angeboten miteinander im Wettbewerb stehen) unterschieden wird. Müsste jeder MaaS-Anbieter eine eigene Infrastruktur anbieten, bliebe der Markt fragmentiert und könnte sich, besonders in der räumlich kleinen Schweiz, von vornherein nicht etablieren. Aus diesem Grund spricht alles für eine zentrale Infrastruktur mit einem so genannten Intermediary MaaS Integrator (IMI). Aus dieser Designentscheidung ergibt sich indes die Governance-Vorgabe, dass alle Akteure zu nicht-diskriminierenden Bedingungen an dieser Infrastruktur teilnehmen können müssen.

Data Governance

Die Anwendung des Data Governance-Modells auf MaaS zeigt, dass nicht alle Akteure die gleichen Anreize haben, ihre Daten über die zentrale Infrastruktur mit anderen zu teilen. Namentlich bestehen Unterschiede zwischen konzessionierten Unternehmen des öffentlichen Verkehrs, die ihre Daten ohnehin veröffentlichen müssen und privaten Unternehmen, welche ihre Daten oft in geschlossenen Silos halten und als Geschäftsgeheimnisse betrachten. Zu guten MaaS-Angeboten kann es nur kommen, wenn die Nutzung der zentralen Infrastruktur mit klaren Grundsätzen und Vorschriften betreffend Datenbezug und Datenverwendung geregelt wird. Damit die betriebswirtschaftlichen und technischen Parameter festgelegt werden können, braucht es eine neutrale Instanz sowie einen Multistakeholder-Ansatz, der alle betroffenen Interessen miteinbezieht. So können technische und rechtliche Herausforderungen bewältigt werden. In technischer Hinsicht steht im Vordergrund, wie Daten interoperabel standardisiert werden können und wie grosse Datenmengen mit schnellen Reaktionszeiten komplex berechnet werden können. In rechtlicher Hinsicht steht im Vordergrund, welche allgemeingültigen Bedingungen für die Nutzung der Infrastruktur aufgestellt werden können, ob MaaS-Anbieter auch auf der Dienstleistungsebene (wo Wettbewerb herrscht) die Pflicht haben sollen, alle Angebote zu listen und ob den MaaS-Anbietern Vorgaben zum Routing (der Erstellung eines Routenvorschlags) gemacht werden sollen.

Die neutrale Instanz ist sodann für Aufsicht und Kontrolle über die zentrale Infrastruktur zuständig.

6.5.2 Das Governance-Modell für RUC

Obwohl die Bewegungen der Verkehrsteilnehmenden über ihre Smartphones, durch die Navigationsgeräte und nicht zuletzt auch durch ihre Fahrzeuge selbst in hoher Auflösung und kontinuierlich erfasst werden, wird dies mehrheitlich akzeptiert oder der Datenfluss ist ihnen schlicht nicht bewusst. Sollte der Staat diese Daten jedoch verpflichtend erheben wollen, ist mit Widerstand zu rechnen. Diesem Widerstand kann nur einem vertrauenswürdigen Systemdesign sowie mit ebenso vertrauenswürdigen Prozessen und Akteuren begegnet werden.

Es geht hierbei nicht nur darum, sich vor einer möglichen Überwachung durch den Staat zu schützen, sondern auch darum, dass das System Sicherheiten bieten muss, dass Daten (insbesondere durch "Hacking" oder Verkauf) nicht an Dritte gelangen können. Zudem hängt die Glaubwürdigkeit des Systems davon ab, ob alle Nutzer gleich behandelt werden. So wäre beispielsweise ein opt out aus dem technischen System (bspw. in Form einer teureren Tagesvignette) keine Option, da so der Datenschutz zum Privileg der sozial Stärkeren würde.

Für die Akzeptanz des Systems ist es ist ein bedeutsamer Unterschied, ob Personen Daten einem Dienstanbieter liefern, den sie frei wählen können oder ob sie diese direkt dem Staat übergeben müssen. Die Wahl des Maut-Dienstanbieters hat aber auch das Potenzial, einen Markt für weitere Dienstleistungen zu eröffnen (sofern dies – auch politisch – gewollt ist) und kann die Dienstanbieter anspornen, den bestmöglichen Service zu bieten, um ihre Marktanteile zu erhöhen. Unabdingbar in einem Marktmodell ist, dass alle Nutzer unabhängig von ihrer technischen Ausrüstung und dem gewählten Dienstanbieter für gleiche Strecken die gleichen Abgaben bezahlen. Dies wird durch die vorgestellte Lösung, mit der zur Verfügungstellung einer TEE mit einem zertifizierten Algorithmus zur Berechnung der Abgabe und zu deren Kontrolle, gewährleistet.

Die Tracking-Daten dürfen beim Maut-Dienstleister nur in verschlüsselter Form vorliegen. Nur innerhalb der sicheren Rechenumgebung können sie entschlüsselt und verarbeitet werden, ohne dass irgendeine Partei darauf Zugriff hätte. Die sichere Umgebung verlassen nur aggregierte Daten. Mit diesen Ansätzen kann sichergestellt werden, dass die organisatorische und juristische Governance durch den Einsatz technologischer Instrumente gewährleistet wird.

Dezentralisierte Berechnung des Map-Matching

Bei automatisierten Fahrzeugen entwickelt sich der Systemansatz in Richtung Edge-Computing. Die Daten sollen also dezentral, möglichst gleich im Fahrzeug bearbeitet werden. Es stellt sich daher die Frage, warum das für die Distanzmessung in der Gebührenerhebung notwendige Map Matching (d.h. der Abgleich der Positionsdaten mit dem Kartenmaterial) nicht ebenfalls im Sinne des Edge-Computing im Fahrzeug vorgenommen wird. Dies würde auch die Datenschutzproblematik deutlich entschärfen, weil dabei die sensiblen detaillierten Rohdaten im Fahrzeug verbleiben könnten.

Die Prämisse für die Erstellung des Governance-Modells lautete, die Gebühren mit heute verfügbaren und verbreiteten Technologien zu erheben. Das Problem wurde deshalb im Hinblick auf die bereits jetzt in den Fahrzeugen realistischerweise verfügbaren Ressourcen betrachtet, was insbesondere für den Technologieansatz GNSS/CN der Fall ist. Zudem stellt weniger die notwendige Rechenleistung als die Komplexität der Haltung und Verteilung aktueller Karten die grösste Herausforderung für eine Edge-Computing Lösung dar. Bei einer staatlich erhobenen Steuer ist es unabdingbar, dass sich alle Benutzer auf dieselbe einheitliche amtliche Karte beziehen, welche zudem mit hoher Frequenz aktualisiert und angepasst werden muss, z.B. bei Strassensperren, Umleitungen, etc. Nur eine aktuelle Karte erlaubt es, bei allen abgabepflichtigen Personen die Gebühr mit der gleichen Genauigkeit zu berechnen.

In Zukunft wären dezentrale (Edge-lastige) Ansätze denkbar, setzen aber eine entsprechende Penetration des Automobilmarktes durch hochautomatisierte Fahrzeuge und gut strukturierte Prozesse zur Kartenaktualisierung voraus.

Grundlegend andere Ansätze der Gebührenerhebung, beispielsweise über geeichte Stromzähler in elektrischen Fahrzeugen, wären prinzipiell denkbar, leiden jedoch unter einer Vielzahl an Nachteilen (s. bereits in Kap.5.3.4 Absatz 4.1).

Vertrauen

Vertrauen der Gebührenzahlenden in das Erhebungssystem ist für die Akzeptanz einer RUC unabdingbar. Ein wesentliches Element dabei ist das Vertrauen in den Schutz der persönlichen Daten. Die Gebühren werden schliesslich aus sehr detaillierten, umfassenden und somit äusserst sensiblen Bewegungsprofilen errechnet. Das Vertrauen wird im vorgestellten Konzept anhand mehrerer ineinandergreifenden Elemente gefestigt.

In Anwendung des "privacy-by-design" Prinzips beruht das Systemkonzept darauf, dass nur zertifizierte Algorithmen Zugang zu den Daten erhalten und diese bearbeiten dürfen, was Missbräuche schon dank der grundlegenden Systemarchitektur vereitelt. Als wesentliches Element ist die Zertifizierung durch eine dritte Stelle, insbesondere der Umfang und der Studie der Vetrauenswürdigkeit der Prüfung stellen einen zentralem Vertrauensanker dar. Dies betrifft vor allem die Zertifizierung der verwendeten Algorithmen für die Berechnung der Strassengebühren und deren Kontrolle. Aus Sicht der Schweizer Bevölkerung sind vertrauenswürdige Institutionen für die Durchführung der Zertifizierung wohl bevorzugt öffentlich-rechtlichen Anstalten, wie z.B. das METAS, oder spezialisierte Zertifizierungsstellen für Cybersecurity[26]. Es ist wichtig, dass diese Stelle unabhängig bleibt. Ob eine bestehende oder eine neu zu errichtende Anstalt mit der Aufgabe betraut wird, ist wohl auch abhängig von der Anzahl zu zertifizierenden Algorithmen und der Periodizität der notwendigen Aktualisierung der Algorithmen inkl. Zertifizierungen.

Bei der Entwicklung der Algorithmen, durch welchen die Gebühren berechnet werden, bietet es sich bereits während der Entwicklungsphase an, Vertreter der Zivilgesellschaft zu integrieren. Dies erlaubt es, frühzeitig Feedback einzuholen und die Lösung entsprechend auszurichten. Damit kann im Rahmen der organisatorischen Governance sichergestellt werden, dass bei allen Beteiligten Vertrauen vorhanden ist und die verwendeten technologischen Instrumente akzeptiert werden.

Kommunikation

Interessensvertreter der beteiligten Akteure können einen starken Einfluss auf die allgemeine Akzeptanz haben. Ihre Einschätzung kann die Akzeptanz des Systems sowohl negativ als auch positiv beeinflussen. Werden solche Vertreter bei der Entwicklung transparent informiert oder haben sie frühzeitig eine Mitsprache oder sind eingebunden, kann dies das Vertrauen in die Lösung stärken. Dies ist notwendig, weil gerade bei komplexen Systemen nicht davon ausgegangen werden kann, dass die breite Bevölkerung ein tieferes Verständnis der Technologie und der technischen Lösung erlangt.

[26] sektorspezifisch siehe bspw. CertX, https://certx.com/de/

7 Schlussfolgerung & Empfehlungen

7.1 Schlussfolgerungen

Das Hauptziel dieser Forschungsarbeit war, ein möglichst breit nutzbares Governance-Modell für datenverarbeitungsgestützte Mobilitätsanwendungen ("Smart Mobility") zu entwickeln. Dieses soll als Instrument genutzt werden können, um die organisatorischen und vertraglichen bzw. rechtlichen Beziehungen zwischen den Akteuren zu definieren und durch technologische Mittel zu unterstützen.

Um dieses Ziel zu erreichen, wurde der Versuch unternommen, die Akteure, Anwendungen und Datenflüsse der gesamten Mobilitätslandschaft in generalisierender und umfassender Weise zu beschreiben (Kap. 2). Im Rahmen des Projektes erwiesen sich diese Generalisierungen sowohl in Bezug auf die Akteure aber auch in Bezug auf die Anwendungen und Datenflüsse als robust, weswegen sie so verwendet werden können. Künftige Anpassungen aufgrund neuer Erkenntnisse sind damit aber nicht ausgeschlossen. Darüber hinaus hat das Forschungsprojekt wesentliche für ein Governance-Modell relevante juristische und technische Instrumente zusammengetragen und analysiert (Kap. 0 und 4).

Auf dieser Grundlage wurde im Forschungsprojekt ein generisches Data Governance-Modell für Smart Mobility-Anwendungen entwickelt, bei dem (in dieser Reihenfolge) die Akteure, die Infrastruktur, der geltende Rechtsrahmen und die eigentliche Data Governance identifiziert und definiert werden. Dieses Modell wurde anhand zweier spezifischer Anwendungen getestet. Ausgewählt wurden dafür die Mobilitätsanwendungen Mobility-as-a-Service (MaaS) und Road User Charge (RUC), welche ihr (Zukunfts-)Potenzial derzeit noch nicht voll entfaltet haben. In beiden Fällen ist Entwicklung des Governance-Modells dabei generisch zu verstehen. Insbesondere bezieht sich jenes für MaaS nicht auf laufende Arbeiten zu NADIM bzw. MODI.

Im Rahmen dieser Arbeiten hat sich gezeigt, dass mit dem vorgeschlagenen Governance-Modell das Zusammenspiel organisatorischer, rechtlicher und technischer Aspekte einheitlich analysiert werden kann. So lässt sich bei der Entwicklung von Dienstleistungen in der "Neuen Mobilität" jeweils auch eine passende Data Governance entwickeln und implementieren. Je nach Mobilitätsanwendung können dabei eher rechtliche (wie bei MaaS) oder eher technische Aspekte (wie bei RUC) im Vordergrund stehen. Das generische Data Governance-Modell kann nun anhand einer breiten Palette von Mobilitätsanwendungen angewendet, überprüft und ggf. weiterentwickelt werden.

Eine zentrale Erkenntnis des Forschungsprojekts lautet, dass Governance-Strukturen – ganz unabhängig von der konkreten Mobilitätsanwendung – zuvorderst Vertrauen zwischen den Akteuren schaffen müssen und dass der Aufbau des Vertrauens im Idealfall die frühzeitige Integration sämtlicher Interessensgruppen erfordert. Im Zusammenhang mit MaaS ist gegenseitiges Vertrauen eine entscheidende Voraussetzung, damit multilaterale Geschäftsbeziehungen überhaupt entstehen können. Beim Anwendungsfall der Road User Charge (RUC) hat sich diese generelle Erkenntnis bestätigt, obwohl diese Smart-Mobility-Anwendung völlig andere Akteure, Datentypen und Prozesse aufweist. Für beide untersuchten Mobilitätsanwendungen wird eine vertrauenswürdige Stelle vorgeschlagen. Bei MaaS hat sie im Wesentlichen eine Aufsichtsfunktion über die Nutzung der zentralen Infrastruktur, bei RUC hat sie die Aufgabe, die verwendeten Algorithmen zu zertifizieren. Wie diese Stelle(n) organisatorisch ausgestaltet werden soll(en), ist weiter zu erforschen. Auch womöglich notwendige – einschliesslich zuständiger Stelle, Umfang und Tiefe – ist noch im Einzelfall zu klären.

7.2 Empfehlungen

Die in diesem Forschungsprojekt entwickelten Modelle können einen Beitrag leisten, um die Data Governance für die Schweizer Mobilität zu fördern. Konkret ergeben sich aus Sicht der am Forschungsprojekt beteiligten Disziplinen drei Empfehlungen:

Empfehlung 1 – Anwendung und ggf. Weiterentwicklung des allgemeinen Governance-Modells

Smarte, vernetzte Mobilitätsangebote sind aktuell im Entstehen begriffen und entwickeln sich angesichts des Innovationstempos und des technologischen Fortschritts schnell. Wie in Kap. 1.1 erwähnt, besteht nun ein Zeitfenster, um diese Entwicklungen mit regulatorischen Massnahmen in Bezug auf die Data Governance zu beeinflussen. Im Nachhinein – wenn eine Smart Mobility-Anwendung bereits flächendeckend etabliert ist – lässt sich eine Governance kaum mehr einführen.

Aus diesem Grund bietet sich die Anwendung des hier entwickelten Governance-Modells an und zwar indem konkret:

- Erstens die Akteure und deren Rollen (Leistungserbringer, Vermittler, Nutzer, Regulator) identifiziert werden, wobei ein Akteur bisweilen mehrere Rollen innehaben kann;
- zweitens die Ansprüche an die Infrastruktur bzw. deren Architektur (zentrale oder dezentrale Datenhaltung) festgelegt werden, unter Trennung von Infrastruktur und darauf aufbauenden Dienstleistungen;
- drittens der geltende Rechtsrahmen daraufhin untersucht wird, wie er ein bestimmtes Mobilitätsangebot beeinflusst (insbesondere hemmt);
- viertens eine Data Governance entwickelt wird, die danach fragt, welche Datenflüsse für das Funktionieren des Mobilitätsangebots notwendig sind, unter welchen Bedingungen sich diese tatsächlich etablieren und welche Massnahmen dafür zu ergreifen sind, und
- fünftens und letztens vertieft wird, wie die entwickelte Governance für eine kontinuierliche und laufende (Re-)zertifizierung und Auditierung ausgestaltet werden kann, um die Einhaltung des Regelwerks und der vereinbarten Prozesse fortlaufend sicherzustellen.

Empfehlung 2 – Anpassung des Rechtsrahmens für MaaS

Das Forschungsprojekt hat gezeigt, dass der Gesetzgeber beim Erlass der relevanten Rechtsnormen implizit davon ausging, monomodalen Verkehr zu regeln. Dies führt dazu, dass sich für Angebote des multimodalen Reisens zahlreiche Reibungen mit dem geltenden Rechtsrahmen ergeben: Das Gesetz regelt beispielsweise nicht, wer die Gesamtverantwortung für die gesamte Reisekette trägt. Entsprechend hängt der Umfang der Passagierrechte vom einzelnen Verkehrsträger ab. Die Schaffung von MaaS-Angeboten wird zudem dadurch erschwert, dass konzessionierte und private Transportanbieter unterschiedliche Rechte (hinsichtlich des Schutzes vor Konkurrenz oder der finanziellen Förderung durch den Staat) und Pflichten (hinsichtlich Beförderungs- und Fahrplanpflicht sowie in Bezug auf die Rechte von Personen mit Behinderungen) haben. Und schliesslich können – unabhängig von diesen Unterschieden – auch gewisse Bestimmungen des Konsumentenrechts MaaS-Anwendungen hemmen.

Aus diesen Gründen drängt es sich auf, den geltenden Rechtsrahmen weiter dahingehend zu untersuchen, wie – unter Berücksichtigung der Rechte und Pflichten aller Akteure – regulatorische Hindernisse für multimodales Reisen beseitigt werden können.

Empfehlung 3 – Machbarkeitsstudie zu RUC

Im Forschungsprojekt wurde deutlich, dass eine vor allem in Bezug auf einen transparent implementierten Datenschutz erfolgreiche Umsetzung von RUC den Einsatz neuer technischer Mittel voraussetzt. Die formalen Datenschutzanforderungen können zwar grundsätzlich schon durch etablierte Massnahmen erfüllt werden. Um bei dieser Anwendung, die in Bezug auf die Privatsphäre sehr invasiv ist, auch dem “gefühlten Datenschutz” Rechnung zu tragen, wurde ein System vorgeschlagen, bei dem die Daten durchgängig verschlüsselt sind und nur innerhalb vertrauenswürdiger isolierter Bereiche im Klartext vorliegen. Welche Herausforderungen mit der Einführung eines solchen Systems verbunden sind, ist aber noch nicht vollständig geklärt. Es ist beispielsweise unklar, ob die Skalier- und Anwendbarkeit für die Umsetzung des vorgeschlagenen Systemkonzepts für eine wie auch immer geartete RUC in der Schweiz – einschliesslich notwendiger Redundanzen und Rückfalllösungen – mit über 5 Mio. Fahrzeugen gegeben ist.

Aus diesem Grund sehen wir vor einer breiten Einführung eine *Machbarkeitsstudie zur Umsetzung von RUC mit einem (dezentral organisierten) TEE* erforderlich. Diese Studie sollte die Machbarkeit, Wirtschaftlichkeit und Skalierbarkeit sowie die notwendigen Zertifizierungsprozesse darlegen. Da die Studie sich notgedrungen mit komplexen und schwer allgemein verständlich zu machenden Inhalten beschäftigt, wäre eine Begleitung durch eine breit abgestützte, vertrauenswürdige zivilgesellschaftiche Institution (AlgorithmWatch, Chaos Computer Club, o.dgl.) wünschenswert.

Anhänge

I Prozesse und Datenflüsse Smart Mobility-Anwendungen

I.1 Sharing (on demand)

Sharing (on demand)

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Registrierung	Daten zur Benutzeridentifikation	Bei der Registrierung geben User Daten wie Name, Rechnungsadresse, E-Mail-Adresse, Nationalität, Geschlecht, Alter, Zahlungsdetails, Führerschein, bestehende Abonnemente (Halbtax) an den Transportanbieter (Produzent) weiter.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Der User erhält Identifizierungsmerkmale mit denen er sich beim Transportanbieter (Produzent) sicher identifizieren kann.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
pre trip	Vertrag	Vertragsdaten	Um den Dienst nutzen zu können, akzeptiert der User die AGBs des Transportanbieter (Produzent)s.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
pre trip	Informationen bereitstellen	Angebotsstatus	Die Fahrzeuge liefern in Echtzeit Fahrzeugbetriebsinformationen wie Verfügbarkeit, aktueller Standort, Grösse des Fahrzeugs, Batterie-/Tankfüllstand an das Backoffice des Transportanbieter (Produzent)s.	Transportanbieter (Produzent)	juristische Person			sehr hoch (s)
pre trip	Informationen bereitstellen	Angebotsstatus	Der Service Provider bietet dem User Service-Betriebsinformationen wie der zu erwartende Preis, die Fahrerbewertung, die zu erwarntede Wartezeit, etc. an. Anhand der Informationen kann der User ein Angebot auswählen.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Durch die Nutzung der Dienste stellt der User dem Transportanbieter (Produzent) Daten wie Fahrrouten (Geo-Positionsdaten, Zeit, Start und Ziel) zur Verfügung. Anhand der Benutzer-ID können die Daten direkt mit den Benutzeridentifikationsdaten verbunden werden. Aus diesen können persönliche Präferenzen abgeleitet werden.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	hoch (s)
post trip	Abrechnung	individuelle Nutzungsdaten	Der User erhält gemäss der zurückgelegten Distanz eine Rechnung.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte der User die Rechnung nicht begleichen, so wird er gebüsst und für mindestens zwei Jahre in einer nationalen Datenbank erfasst. Der Zugang zur Serviceplattform kann entzogen werden.	Transportanbieter (Produzent)	natürliche / juristische Person	User	natürliche / juristische Person	sehr tief (> Jahr)

I.2 Vernetztes privates Fahrzeug

vernetzte private Fahrzeugnutzung

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Registrierung	Daten zur Benutzeridentifikation	Der Benutzer erstellte ein Konto um ein Fahrzeug zu bestellen (z.B. Tesla Account). Dem Fahrzeughersteller zur verfügung gestellte Daten umfassen Angaben zur Name, Adresse, Telefonnummern, Führerausweis, Kreditkarteninformatione etc. umfassen.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
pre trip	Vertrag	Vertragsdaten	Mit dem unterzeichenen des Kaufvertrags akzeptiert der Benutzer die AGBs des Fahrzeugherstellers. Die AGBs informieren u.a. über die Datenerhebungen durch das Fahrzeug und den Datentransfer vom Fahrzeug an den Fahrzeughersteller. In der Regel wird dem Benutzer hierbei garantiert, dass die personenbezogenen Daten nur anonymisiert weiterverwendet werden dürfen z.B. für Marketing. Daten werden nicht an Dritte verkauft, aber an Geschäftspartner und Dienstleister weitergegeben.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Vertrag	Vertragsdaten	Seit 2018 sind in Europa alle neuen Fahrzeuge mit eCall ausgestattet. Beim Kauf oder Leasing eines Fahrzeugs die mit dieser Technologie ausgestattet ist, akzeptiert der Benutzer die AGBs von eCall.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Das Fahrzeug muss vor der Benutzung bei den Behörden registiert und eingelöst werden (Name, VIN, Adresse, Versicherungen etc.). Der Benutzer erhält von den Behörden ein Nummernschild für das Fahrzeug.	User	natürliche / juristische Person	Regulator	staatlich	sehr tief (> Jahr)
on trip	Informationen bereitstellen	Angebotsstatus	Der Transportanbieter stellt dem User sämtliche Informationen für die Navigation wie z.B. Karte, Geschwindigkeitsbegrenzungen, Auslastung zur Verfügung, allfällige zeitabhängige Gebühren für die Strassenbenutzung.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	hoch (min - h)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Der Transportanbieter (z.B. Tesla) sammelt vom Fahrzeug und dem User etliche individuelle Nutzungsdaten wie Fernanalysedaten (Kontakte, Browser-Verlauf, Navigations-Verlauf, aktueller Standort, etc.) sowie auch Ton und Bildaufnahmen aus dem Fahrzeuginneren sammeln. Dieese gesammelten Daten beinhalten zudem sämtliche Informationen in Bezug auf die Navaigation wie Starts, Ziele, benutzte Routen, vorgeschlagenen Routen, Pausen etc.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	hoch (min - h)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Der Transportanbieter (Produzent, z.B. Tesla) sammelt automatisiert Informationen über die Umgebung des Fahrzeug, inkl. Bilder und Videos. Diese können Personen und andere Fahrzeuge in nicht anonymisierter Form enthalten.	Transportanbieter (Produzent)	juristische Person			hoch (min - h)
on trip	Informationen bereitstellen	Angebotsstatus	Das Fahrzeug liefert dem Transportanbieter (Produzent, z.B. Tesla) in Echtzeit Betriebsdaten wie Telematikprotokolldaten (Daten über Leistung, Nutzung, Betrieb, den Zustand des Fahrzeugs; sicherheitsrelevante Kamerabilder und Videoaufnahmen; etc.) und Fahrsicherheits-Analysedaten (Daten über Unfälle, etc.).	Service Anbieter	juristische Person			sehr hoch (s)
on trip	Informationen bereitstellen	Angebotsstatus	Der Transportanbieter (Produzent, z.B. Tesla) oder dessen Geschäftspartner können Daten dem Nutzer zur Verfügung stellen: - Informationen über das Fahrzeug (z.B. Tips zur Energienutzung)	Transportanbieter (Produzent)	juristische Person	User	natürliche Person	sehr hoch (s)
on trip	Überwachung	aggregierte Nutzungsdaten	car2x communication (vgl. traffic management)	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr hoch (s)
Sonderfälle	Informationen bereitstellen	individuelle Nutzungsdaten	vgl. eCall	User	natürliche / juristische Person	Service Anbieter	juristische Person	hoch (min - h)

I.3 Riding (on demand)

Riding (on demand)

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	Ein Transportanbieter schliesst einen Vertrag mit einem Service Anbieter ab. Der Vertrag regelt die finanziellen Bedingungen zwischen den Parteien.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	natürliche / juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Identifizierungsmerkmale, die es dem Service Anbieter erlauben, sich beim Transportanbieter eindeutig und in einer gesicherte Art und Weise zu identifizieren.	Transportanbieter (Produzent)	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Bei der Registrierung geben User Daten wie Name, Rechnungsadresse, E-Mail-Adresse, Nationalität, Geschlecht, Alter, Zahlungsdetails, Führerschein, bestehende Abonnemente (Halbtax) an den Service Anbieter weiter.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Der User erhält Identifizierungsmerkmale mit denen er sich beim Service Anbieter sicher identifizieren kann.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
pre trip	Vertrag	Vertragsdaten	Um den Dienst nutzen zu können, akzeptiert der User die AGBs des Service Anbieters.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
pre trip	Informationen bereitstellen	Angebotsstatus	Der Transportanbieter liefert Angebotsbeschreibung wie Preise, Verfügbarkeit (temporär, räumlich) etc. an den Service Anbieter.	Transportanbieter (Produzent)	natürliche / juristische Person	Service Anbieter	juristische Person	sehr hoch (s)
pre trip	Informationen bereitstellen	Daten zur Benutzeridentifikation	Der Service Anbieter muss dem Transportanbieter Informationen über den User zur Verfügung stellen. Die Daten umfassen benutzeridentifikationsbezogene Daten wie Name, Nationalität, Geschlecht, Alter, Benutzer-ID.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	natürliche / juristische Person	hoch (s)
pre trip	Informationen bereitstellen	Wertung von Nutzerverhalten	Wenn Nutzer oder Nutzerinnen einen Dienst buchen will, wird seine Wertung (z. B. die Pünktlichkeit des Nutzenden) zwischen dem Service Anbieter und dem Transportanbierter ausgetauscht.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	natürliche / juristische Person	mittel (Tag - Monat)
pre trip	Informationen bereitstellen	Angebotsstatus	Der Service Provider bietet dem User Daten zum Angebotsstatus wie der zu erwartende Preis, die Fahrerbewertung, die zu erwarntede Wartezeit, etc. an. Anhand der Informationen kann der User ein Angebot auswählen.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Durch die Nutzung der Dienste stellt der User dem Service Anbieter Daten wie Fahrrouten (Geo-Positionsdaten, Zeit, Start und Ziel) zur Verfügung. Anhand der Benutzer-ID können die Daten direkt mit den Benutzeridentifikationsdaten verbunden werden und persönliche Präferenzen abgeleitet werden.	User	natürliche / juristische Person	Service Anbieter	juristische Person	hoch (s)
post trip	Abrechnung	individuelle Nutzungsdaten	Der User erhält gemäss der zurückgelegten Distanz eine Rechnung.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Service Anbieter	juristische Person	tief (Monat - Jahr)
post trip	Inkasso	aggregierte Nutzungsdaten	Der Service Anbieter überweist den durch den Vertrag geregelten Betrag an den Transportanbieter.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Informationen sammeln	Wertung von Nutzerverhalten	Basierend auf der Fahrt, dem gewählten Service und dem Feedback des Fahrers aktualisiert der Service Anbieter die Wertung des Nutzerverhaltens entsprechend.	Service Anbieter	natürliche / juristische Person			mittel (Tag - Monat)
post trip	Informationen sammeln	Produzentenbewertung	Basierend auf der Fahrt kann der User den Transportanbieter (Fahrer) bewerten.	User	natürliche / juristische Person	Transportanbieter (Produzent)	natürliche / juristische Person	mittel (Tag - Monat)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte der User die Rechnung nicht begleichen, so wird er gebüsst und für mindestens zwei Jahre in einer nationalen Datenbank erfasst. Der Zugang zur Serviceplattform kann entzogen werden.	Service Anbieter	natürliche / juristische Person	User	natürliche / juristische Person	sehr tief (> Jahr)

I.4 ÖV (on demand)

ÖV (on demand)

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	Ein Transportanbieter (Tranpsortunternehmung) schliesst einen Vertrag mit einem Service Anbieter (Verkehrsverbund) ab. Der Vertrag regelt die finanziellen Bedingungen sowie die erwarteten Leistungen zwischen den Parteien.	Transportanbieter (Produzent)	juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Bei der Registrierung geben User Daten wie Name, Rechnungsadresse, E-Mail-Adresse, Nationalität, Geschlecht, Alter, Zahlungsdetails, Führerschein, bestehende Abonnemente (Halbtax) an den Service Anbieter weiter.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Der User erhält Identifizierungsmerkmale mit denen er sich beim Service Anbieter sicher identifizieren kann.	Service Anbieter	juristische Person	User	natürliche / juristische Person	sehr tief (> Jahr)
pre trip	Vertrag	Vertragsdaten	Um den Dienst nutzen zu können, akzeptiert der User die AGBs des Service Anbieters.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
pre trip	Informationen bereitstellen	Angebotsbeschreibung	Der Transportanbieter liefert Angebotsbeschreibung wie Preise, Verfügbarkeit (temporär, räumlich) etc. an den Service Anbieter.	Transportanbieter (Produzent)	juristische Person	Service Anbieter	juristische Person	tief (Monat - Jahr)
pre trip	Informationen bereitstellen	Angebotsstatus	Der Transportanbieter liefert Angebotsstatus wie Verfügbarkeit, aktuelle Pünktlichkeit eines Fahrzeugs, etc. an den Service Anbieter.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	hoch (s)
pre trip	Informationen bereitstellen	Daten zur Benutzeridentifikation	Der Service Anbieter muss dem Transportanbieter Informationen über den User zur Verfügung stellen. Die Daten umfassen benutzeridentifikationsbezogene Daten wie Name, Nationalität, Geschlecht, Alter, Benutzer-ID.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	hoch (s)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Durch die Nutzung der Dienste stellt der User dem Service Anbieter Daten wie Fahrrouten (Geo-Positionsdaten, Zeit, Start und Ziel) zur Verfügung. Anhand der Benutzer-ID können die Daten direkt mit den Benutzeridentifikationsdaten verbunden werden. Aus diesen können persönliche Präferenzen abgeleitet werden.	User	natürliche / juristische Person	Service Anbieter	juristische Person	hoch (s)
on trip	Kontrolle	individuelle Nutzungsdaten	Der Transportanbieter kontrolliert die User vor oder während der Fahrt. Der User muss seine Abonnemente (Halbtax, GA) oder das von der MaaS-Plattform bereitgestellte Ticket vorweisen. Die digitalen Tickets sind i.d.R. direkt mit der Identität des Users verknüpft.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	hoch (min - h)
post trip	Abrechnung	individuelle Nutzungsdaten	Der User erhält gemäss der zurückgelegten Distanz eine Rechnung.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der Service Anbieter überweist den durch den Vertrag geregelten Betrag an den Transportanbieter.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
Sonderfälle	Deliktumgang	individuelle Nutzungsdaten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User anhand des Userratings gebüsst.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User für mindestens zwei Jahre in einer nationalen Datenbank erfasst.	Transportanbieter (Produzent)	juristische Person	Regulator	staatlich	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte der User die Rechnung nicht begleichen, so wird er gebüsst und für mindestens zwei Jahre in einer nationalen Datenbank erfasst. Der Zugang zur Serviceplattform kann entzogen werden.	Service Anbieter	juristische Person	Regulator	staatlich	tief (Monat - Jahr)

I.5 ÖV (klassisch)

ÖV (klassisch)

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Registrierung	Daten zur Benutzeridentifikation	Für digitale Tickets ist eine Registrierung notwendig. Der User gibt Daten wie Name, Rechnungsadresse, E-Mail-Adresse, Nationalität, Geschlecht, Alter, Zahlungsdetails, Führerschein, bestehende Abonnemente (Halbtax) an den Service Anbieter weiter.	User	natürliche Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Vertrag	Vertragsdaten	Um den Dienst nutzen zu können, akzeptiert der User die AGBs des Service Anbieters.	User	natürliche Person	Service Anbieter	juristische Person	tief (Monat - Jahr)
pre trip	Informationen bereitstellen	Angebotsbeschreibung	Der Transportanbieter liefert Angebotsbeschreibung wie Fahrplaninformationen, Verfügbarkeit, Preise, etc. an den Service Anbieter.	Transportanbieter (Produzent)	juristische Person	Service Anbieter	juristische Person	tief (Monat - Jahr)
pre trip	Informationen bereitstellen	Angebotsstatus	Der Transportanbieter liefert Angebotsstatus wie Verfügbarkeit, aktuelle Pünktlichkeit eines Fahrzeugs, etc. an den Service Anbieter.	Transportanbieter (Produzent)	juristische Person	Service Anbieter	juristische Person	hoch (s)
pre trip	Informationen bereitstellen	individuelle Nutzungsdaten	Wenn eine Leistung im Voraus gebucht werden muss (z. B. Einzelfahrt), werden individuelle Nutzungsdaten (z.B. Quell & Zielort) an den Leistungserbringer übermittelt.	User	natürliche Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
on trip	Kontrolle	individuelle Nutzungsdaten	Der Transportanbieter kontrolliert die User vor oder während der Fahrt. Der User muss seine Abonnemente (Halbtax, GA) oder das Ticket vorweisen. Die digitalen Tickets sind i.d.R. direkt mit der Identität des Users verknüpft.	User	natürliche Person	Transportanbieter (Produzent)	juristische Person	hoch (min - h)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Der ÖV Betreiber sammelt Informationen zu den Fahrrouten seiner Kundschaft. Über den digitalen Ticketvertrieb sind die Informationen direkt mit den hinterlegten Abonnements (z.B. Halbtax) verknüpft.	User	natürliche Person	Service Anbieter	juristische Person	sehr hoch (s)
post trip	Abrechnung	individuelle Nutzungsdaten	Falls nicht im Voraus bezahlt erhält der User erhält gemäss der gebuchten Tickets / der zurückgelegten Distanz eine Rechnung.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der Service Anbieter überweist den durch den Vertrag geregelten Betrag an den Transportanbieter.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
Sonderfälle	Deliktumgang	individuelle Nutzungsdaten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User anhand des Userratings gebüsst.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User für mindestens zwei Jahre in einer nationalen Datenbank erfasst.	Transportanbieter (Produzent)	juristische Person	Regulator		tief (Monat - Jahr)

I.6 MaaS

MaaS

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	MaaS-Betreiber (Service Provider) schliessen Verträge mit verschiedenen Transportanbietern (Producer)	Service Anbieter		Transportanbieter (Produzent)		sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Identifizierungsmerkmale, die es dem Service Anbieter erlauben, sich beim Transportanbieter eindeutig und in einer gesicherte Art und Weise zu identifizieren.	Transportanbieter (Produzent)		Service Anbieter		sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Bei der Registrierung geben User Daten wie Name, Rechnungsadresse, E-Mail-Adresse, Nationalität, Geschlecht, Alter, Zahlungsdetails, Führerschein, bestehende Abonnemente (Halbtax) an den Service Anbieter weiter.	User		Service Anbieter		sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Der User erhält Identifizierungsmerkmale mit denen er sich beim Service Anbieter sicher identifizieren kann.	Service Anbieter		User		mittel (Tag - Monat)
pre trip	Vertrag	Vertragsdaten	Um den Dienst nutzen zu können, akzeptiert der User die AGBs des Service Anbieters. Darüber hinaus wählt der User zwischen verschiedenen Angeboten/Modellen (in der Regel Pay-as-you-go oder Abonnemente).	User		Service Anbieter		mittel (Tag - Monat)
pre trip	Informationen bereitstellen	Angebotsbeschreibung	Der Transportanbieter liefert Angebotsbeschreibung wie Fahrplaninformationen, Verfügbarkeit, Preise, etc. an den Service Anbieter.	Transportanbieter (Produzent)		Service Anbieter		mittel (Tag - Monat)
pre trip	Informationen bereitstellen	Angebotsstatus	Der Transportanbieter liefert Angebotsstatus wie Verfügbarkeit, aktuelle Pünktlichkeit eines Fahrzeugs, etc. an den Service Anbieter.	Transportanbieter (Produzent)		Service Anbieter		sehr hoch (s)
pre trip	Informationen bereitstellen	Daten zur Benutzeridentifikation	Der Service Anbieter muss dem Transportanbieter Informationen über den User zur Verfügung stellen. Die Daten umfassen benutzeridentifikationsbezogene Daten wie Name, Nationalität, Geschlecht, Alter, Benutzer-ID.	Service Anbieter		Transportanbieter (Produzent)		hoch (s)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Durch die Nutzung der Dienste stellt der User dem Service Anbieter Daten wie Fahrrouten (Geo-Positionsdaten, Zeit, Start und Ziel) zur Verfügung. Anhand der Benutzer-ID können die Daten direkt mit den Benutzeridentifikationsdaten verbunden werden. Aus diesen können persönliche Präferenzen abgeleitet werden.	User		Service Anbieter		hoch (s)
on trip	Informationen sammeln	aggregierte Nutzungsdaten	Durch die Nutzung der Dienste stellt der User dem Service Anbieter nicht-personenbezogene Nutzungsdaten wie genutzter Verkehrsanbieter, gefahrene Strecke, Fahrzeit, etc. zur Verfügung	User		Service Anbieter		mittel (Tag - Monat)
on trip	Kontrolle	Daten zur Benutzeridentifikation	Der Transportanbieter kontrolliert die User vor oder während der Fahrt. Der User muss seine Abonnemente (Halbtax, GA) oder das von der MaaS-Plattform bereitgestellte Ticket vorweisen. Die digitalen Tickets sind i.d.R. direkt mit der Identität des Users verknüpft.	User		Transportanbieter (Produzent)		hoch (min - h)
post trip	Abrechnung	individuelle Nutzungsdaten	Der User erhält gemäss der zurückgelegten Distanz eine Rechnung.	Service Anbieter		User		mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Je nach Modell bzw. Inanspruchnahme der Transportdienstleistungen erfolgt die Begleichung der Rechnung durch den User.	User		Service Anbieter		tief (Monat - Jahr)
post trip	Inkasso	aggregierte Nutzungsdaten	Der Service Anbieter überweist den durch den Vertrag geregelten Betrag an den Transportanbieter.	Service Anbieter		Transportanbieter (Produzent)		mittel (Tag - Monat)
Sonderfälle	Deliktumgang	individuelle Nutzungsdaten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User anhand des Userratings gebüsst.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User für mindestens zwei Jahre in einer nationalen Datenbank erfasst.	Transportanbieter (Produzent)	juristische Person	Regulator		tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte der User die Rechnung nicht begleichen, so wird er gebüsst und für mindestens zwei Jahre in einer nationalen Datenbank erfasst. Der Zugang zur Serviceplattform kann entzogen werden.	Service Anbieter	juristische Person			sehr tief (> Jahr)

I.7 eCall

eCall

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	Seit 2018 sind alle Neufahrzeuge in Europa mit eCall ausgestattet. Beim Kauf / Leasing / Nutzung eines mit der Technologie ausgestatteten Fahrzeuge akzeptiert der Nutzer die allgemeinen Geschäftsbedingungen von eCall.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
on trip	Überwachung	Angebotsstatus	Während der Fahrt überwacht die eCall-Technologie die Betriebsdaten des Fahrzeugs (z.B. Geschwindigkeit, Beschleunigung, Verlangsamung, Status der Airbags, Ausrichtung des Fahrzeugs) um einen Unfall zu erkennen. Da das eCall-System mit einer "ruhenden SIM" arbeitet, die nur im Falle eines Unfalls aktiviert wird, werden während der Überwachung des Fahrzeugs keine Daten ausgetauscht. Im Fahrzeug werden zudem nur die letzten drei Standorte gespeichert, ältere Standorte werden fortlaufend überschrieben. Dies bietet Datenschutz auf einem sehr hohen Niveau.					
Sonderfälle	Informationen bereitstellen	individuelle Nutzungsdaten	Im Falle eines schweren Unfalls stellt das eCall-System automatisch eine Mobiltelefonverbindung mit dem Mobilfunkbetreiber her und sendet einen Mindestdatensatz (nkl. Geolokalisierung, Fahrtrichtung, Fahrzeugtyp und Fahrzeugidentifikationsnummer).	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
Sonderfälle	Informationen bereitstellen	individuelle Nutzungsdaten	Der Mindestdatensatz wird vom Mobilfunkbetreiber (Mobile network operator) an die Notrufabfragestelle weitergeleitet und eine Telefonverbindung zwischen User und Notrufzentrale hergestellt. Da die Notrufzentralen in der Schweiz von den kantonalen Polizeibehörden betrieben werden, kann der Besitzer oder die Besitzerin des Fahrzeugs anhand der Fahrgestellnummer identifiziert werden.	Service Anbieter	natürliche / juristische Person	Transportanbieter (Produzent)	öffentlich	sehr tief (> Jahr)
Sonderfälle	Informationen sammeln	individuelle Nutzungsdaten	Die Notrufabfragestelle kommuniziert direkt mit den betroffenen Personen im Fahrzeug per Telefon.	Transportanbieter (Produzent)		User	natürliche / juristische Person	sehr hoch (s)

I.8 Letzte Meile Logistik

letzte Meile Logistik

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Daten zur Benutzeridentifikation	Sobald der User sich bei einem Händler registiert stimmt er den Allgemeinen Geschäftsbedingungen zu und übermittelt personelle Informationen wie finanzielle Details, Rechnungs- und Lieferadresse.	User	natürliche / juristische Person	Service Anbieter	juristische Person	tief (Monat - Jahr)
pre trip	Vertrag	sicherheitsrelevante Daten zur Benutzeridentifikation						
pre trip	Vertrag	Vertragsdaten	Der Händler beauftragt einen Paketdienstleister mit der Auslieferung. Dabei wird ein Vertrag geschlossen, der die Konditionen regelt.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
pre trip	Nutzung	individuelle Nutzungsdaten	Der User bestellt etwas beim Händler.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
pre trip	Abrechnung	individuelle Nutzungsdaten	Der User erhält gemäss der Bestellung eine Rechnung.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
pre trip	Inkasso	Daten zur Benutzeridentifikation	Der Kunde bezahlt die Bestellung im Voraus oder gibt die notwendigen Kreditkarteninformationen an, um die Lastschrift automatisch auszulösen.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
pre trip	Informationen bereitstellen	individuelle Nutzungsdaten	Der Paketdienstleister erhält vom Händler den Auftrag, ein Paket an einen bestimmten User zu liefern. Dabei wird dem Paketdiensleister die Lieferadresse übermittelt.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
on trip	Informationen bereitstellen	individuelle Nutzungsdaten	Bei erfolgreicher Auslieferung bestätigt der Kunde ggf. die Lieferung durch eine (digitale) Unterschrift.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
on trip	Informationen bereitstellen	individuelle Nutzungsdaten	Der Paketdienstleister bestätigt dem Händler die erfolgreiche Zustellung der Bestellung an den Nutzer.	Transportanbieter (Produzent)	juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
on trip	Informationen bereitstellen	Angebotsstatus	Die Flottenmanagement- und Betriebszentrale des Paketdienstleisters informiert den Fahrer des Zustellfahrzeugs über die beste Route, die aktuelle Situation (Parkmöglichkeiten beim Kunden), usw.	Transportanbieter (Produzent)	juristische Person			
on trip	Informationen bereitstellen	Angebotsstatus	Das Fahrzeug und der Fahrer liefern der Flottenmanagement- und Betriebszentrale des Paketdienstleisters Informationen über den Status des Fahrzeugs (z. B. Kraftstoffstand), die Aufträge (z. B. Lieferstatus).	Transportanbieter (Produzent)	juristische Person			
post trip	Inkasso	Daten zur Benutzeridentifikation	Nach erfolgreicher Auslieferung des Pakets wird der Paketdienstleister vom Händler bezahlt.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
Sonderfälle	Informationen sammeln	Wertung von Nutzerverhalten	Der Händler sammelt Informationen über den Benutzer bezüglich seiner Bestellungen und der betrachteten Produkte, um ihm in Zukunft personalisierte Werbung anbieten zu können.	User	natürliche / juristische Person	Service Anbieter	juristische Person	hoch (s)

I.9 Pay-as-you-drive Autoversicherung

Pay-as-you-drive Autoversicherung

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten		User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation		User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation		User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Während der Fahrt sammelt das installierte Gerät (Black Box, Smartphone App, bordeigene Systeme oder Plug-in-Gerät) automatisch Daten zum Fahrverhalten (z.B. Geschwindigkeit, Beschleunigung, Vollbremsung/Kurvenfahrt, gefahrenen Kilometern, Tageszeit, Telefonnutzung während der Fahrt und Geolokalisierung) und verknüpft die gesammelten Daten direkt mit der versicherten Person.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	sehr hoch (s)
post trip	Informationen bereitstellen	individuelle Nutzungsdaten	Die Versicherung ermöglicht dem Nutzer über eine Nutzeroberfläche (Web, App) Einsicht auf die aufgezeichnete Fahrleistung.	Transportanbieter (Produzent)	natürliche / juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Abrechnung	individuelle Nutzungsdaten	Die Versicherung stellt dem Nutzer in Abhängigkeit der gesammelten Daten die Rechnung. Die Höhe korreliert dabei direkt mit dem Fahrstil des Benutzers.	Transportanbieter (Produzent)	natürliche / juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
Sonderfälle	Informationen bereitstellen	Wertung von Nutzerverhalten	Anhand der gesammelten Daten kann die Versicherung ein persönliches Risikoprofil des Nutzers erstellen. Dieses kann weiterverwendet werden, insbesondere für die Risikokalkulation von Lebens-, Invaliditäts- / Unfall- oder Krankenversicherungen.	Transportanbieter (Produzent)	natürliche / juristische Person			sehr tief (> Jahr)

I.10 Elektronische Strassengebührenhebung

Strassengebührerhebung

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	Mautanbieter (toll service provider) gehen mit dem Mauterheber (toll charger) einen Zulassungsvertrag eingehen. Der Vertrag regelt die Erhebung und Bereitstellung von Pflichtdaten (GNNS Lokalisationen & Zeitpunkte, gefahrene Distanzen, etc.) und deren Genauigkeit. Darüber hinaus wird im Vertrag geklärt, wie der Mauterheber den Mautbetreiber bezahlt. In der Schweiz bildet das Bestehen eines mehrstufigen Zulassungsverfahren die Grundlagen für den Abschluss eines Zulassungsvertrags und den Erhalt einer Zulassungsverfügung	Service Anbieter	juristische Person	Transportanbieter (Produzent)	staatlich	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Identifizierungsmerkmale, die es dem Mautanbieter erlauben, sich beim Mauterheber eindeutig und in einer gesicherte Art und Weise zu identifizieren.	Transportanbieter (Produzent)	staatlich	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Der User registriet sich bei einem Mautanbieter mit Name, VIN, Zahlungsadresse und Zahlungsdetails.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Der User erhält Identifizierungsmerkmale mit denen er sich beim Service Anbieter sicher identifizieren kann.	Service Anbieter	juristische Person	User	natürliche / juristische Person	sehr tief (> Jahr)
pre trip	Vertrag	Vertragsdaten	Der Nutzer akzeptiert die AGBs des Mautanbieters. Im Gegenzug erhält er ein Erfassungsgerät / App, mit der die Gebühr basierend auf der zurückgelegten Strecke berechnet werden kann.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr hoch (s)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Während der Fahrt sammelt der Dienstanbieter die GNSS Lokalisationen des Nutzers mit einer On-Board-Unit / Applikation. (Thin-Client)	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr hoch (s)
on trip	Informationen sammeln	aggregierte Nutzungsdaten	Die On-Board-Unit berechnet anhand der gefahrene Strecke in einer Tarifzone die Mautkosten (Thick-Client).	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
post trip	Informationen bereitstellen	aggregierte Nutzungsdaten	Die berechnete Distanz pro Tarifzone wird vom Mautanbieter an den Mauterheber übermittelt (Thick-Client).	Service Anbieter	juristische Person	Transportanbieter (Produzent)	staatlich	mittel (Tag - Monat)
post trip	Informationen bereitstellen	individuelle Nutzungsdaten	Alternativ werden vom OBU die GPS-Punkte mit hoher Auflösung (zur Berechnung der Fahrrouten mit Kartenabgleich) an den Mautanbieter übermittelt (Thin-Client)	Service Anbieter	juristische Person	Transportanbieter (Produzent)	staatlich	mittel (Tag - Monat)
post trip	Informationen bereitstellen	individuelle Nutzungsdaten	Je nach System werden die GPS-Punkte, oder die zurückgelegten Distanzen pro Tarifzone dem Mauterheber übermittelt	Service Anbieter	juristische Person	Transportanbieter (Produzent)	staatlich	mittel (Tag - Monat)
post trip	Kontrolle	individuelle Nutzungsdaten	Der Mauterheber kontrolliert ob die erhaltenen Fahrrouten komplett sind.	Transportanbieter (Produzent)	staatlich			mittel (Tag - Monat)
on trip	Kontrolle	individuelle Nutzungsdaten	Der Mautanbieter bzw. der Mauterheber erhebt Bilder, die mit einem Zeitstempel und dem Standort signiert sind. Anhand der Bilder wird die Einhaltung der Nutzungsbedingungen überprüft.	Service Anbieter		Transportanbieter (Produzent)	staatlich	mittel (Tag - Monat)
post trip	Abrechnung	individuelle Nutzungsdaten	Der User bekommt vom Mauterheber gemäss der zurückgelegten Distanz eine Rechnung.	Transportanbieter (Produzent)	staatlich	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Transportanbieter (Produzent)	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der Mauterheber begleicht die laut Vertrag anfallenden Gebühren dem Mautanbieter	Transportanbieter (Produzent)	staatlich	Service Anbieter	juristische Person	mittel (Tag - Monat)
Sonderfälle	Deliktumgang	individuelle Nutzungsdaten	Falls bei den Kontrollen ein Vergehen festgestellt wird, eröffnet der Mauterheber ein Verfahren gegenüber dem Nutzer.	Transportanbieter (Produzent)	staatlich	User	natürliche / juristische Person	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Bei Vergehen wird der Nutzer von dem Mautanbieter und dem Mauterheber bewertet. Die Informationen werden zwischen den beiden Parteien ausgetauscht.	Transportanbieter (Produzent)	staatlich	Service Anbieter	juristische Person	tief (Monat - Jahr)

I.11 IFMS

IFMS

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	Ein FMP schliesst einen Vertrag mit den Verkehrsunternehmen oder deren Tarifverbund. Der Vertrag regelt die finanziellen Bedingungen zwischen den Parteien.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Identifizierungsmerkmale, die es dem Service Anbieter erlauben, sich beim Transportanbieter eindeutig und in einer gesicherte Art und Weise zu identifizieren.	Transportanbieter (Produzent)	juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	Daten zur Benutzeridentifikation	Der User registriert sich bei Service Anbieter mit seinem Namen, seiner Rechnungsadresse und Zahlungsdetails. Zusätzliche Daten werden aus betrieblichen Gründen gespeichert, siehe Link in der Beschreibung.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr tief (> Jahr)
pre trip	Registrierung	sicherheitsrelevante Daten zur Benutzeridentifikation	Der User erhält Identifizierungsmerkmale mit denen er sich beim Service Anbieter sicher identifizieren kann.	Service Anbieter	juristische Person	User	natürliche / juristische Person	sehr tief (> Jahr)
pre trip	Vertrag	Vertragsdaten	Um den Dienst zu nutzen, akzeptiert der Benutzer die ABGs des Service Anbieters. Im Gegenzug erhält er eine Applikation, mit der der Fahrpreis, basierend auf der gefahrenen Strecke und den genutzten Transportanbietern berechnet wird.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr hoch (s)
on trip	Informationen sammeln	individuelle Nutzungsdaten	Während der Fahrt sammelt der Service Anbieter mit einer Applikation (Thin-Client) die Fahrrouten (GNSS-Standorte mit hoher Auflösung) des Benutzers. Die Daten werden dann vollständig an das Backoffice übertragen. Weitere Daten über die Aktivität des Benutzers / des verwendeten Gerätes werden gespeichert. Siehe Link in der Beschreibung.	User	natürliche / juristische Person	Service Anbieter	juristische Person	sehr hoch (s)
post trip	Kontrolle	individuelle Nutzungsdaten	Anhand der gesammelten Daten werden die Kosten für den Nutzer berechnet.	Service Anbieter	juristische Person			
post trip	Informationen bereitstellen	aggregierte Nutzungsdaten	Der Transportanbieter erhält vom Service Anbieter eine Übersicht über die Dienstleistungen die der User benutzte. Dies beinhaltet bei Tarifverbünden die benutzten Zonen, damit sie die Einnahmen unter den verschiedenen Transportanbieter im Verbund verteilen können.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
on trip	Kontrolle	Daten zur Benutzeridentifikation	Der Transportanbieter kontrolliert die User vor oder während der Fahrt.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Abrechnung	individuelle Nutzungsdaten	Der User erhält gemäss der zurückgelegten Distanz eine Rechnung.	Service Anbieter	juristische Person	User	natürliche / juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der User begleicht die Rechnung.	User	natürliche / juristische Person	Service Anbieter	juristische Person	mittel (Tag - Monat)
post trip	Inkasso	Daten zur Benutzeridentifikation	Der Service Anbieter überweist den durch den Vertrag geregelten Betrag an den Transportanbieter.	Service Anbieter	juristische Person	Transportanbieter (Produzent)	juristische Person	mittel (Tag - Monat)
Sonderfälle	Deliktumgang	individuelle Nutzungsdaten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User anhand des Userratings gebüsst.	Transportanbieter (Produzent)	juristische Person	User	natürliche / juristische Person	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte die Kontrolle das Fahren ohne gültigen Fahrschein ergeben, so wird der User für mindestens zwei Jahre in einer nationalen Datenbank erfasst.	Transportanbieter (Produzent)	juristische Person	Regulator	staatlich	tief (Monat - Jahr)
Sonderfälle	Deliktumgang	Wertung von Nutzerverhalten	Sollte der User die Rechnung nicht begleichen, so wird er gebüsst und für mindestens zwei Jahre in einer nationalen Datenbank erfasst. Der Zugang zur Serviceplattform kann entzogen werden.	Service Anbieter	juristische Person			

I.12 Strassenverkehrsmanagement

Strassenverkehrsmanagement

				Datenflüsse				
Event:	**Prozess:**	**Datentyp:**	Beschreibung Prozesse und Daten	**von Akteur**	**rechtliche Qualifizierung**	**zu Akteur**	**rechtliche Qualifizierung**	**Frequenz**
pre trip	Vertrag	Vertragsdaten	Der Regulator, in diesem Fall eine Behörde, beauftragt eine Verkehrsmanagement- und Verkehrssteuerungszentrale mit der Erfüllung der geforderten Tätigkeiten.	Regulator	staatlich	Transportanbieter (Produzent)	öffentlich	sehr tief (> Jahr)
on trip	Überwachung	aggregierte Nutzungsdaten	Die Verkehrsmanagement- und Verkehrssteuerungszentrale überwacht automatisiert die aktuellen Bedingungen auf der Strasse (Geschwindigkeit, Fluss, Rückstau, Signale...). Sie macht dazu (i.d.R. anonymisierte)Bilder / Videos von Verkehrsteilnehmenden. Bei Kameras auf Autobahnen zur Verkehrsüberwachung ist zur Garantie der Anonymsierung die Auflösung entsprechend gering bzw. die Winkel der Kameras so gewählt, dass Nummernschilder nicht ausgewertet werden können.	Transportanbieter (Produzent)	öffentlich			sehr hoch (s)
on trip	Steuerung	Angebotsstatus	Die Verkehrsleistelle reagiert, um die Verkehrssteuerung an das aktuelle Verkehrsgeschehen anzupassen. Mögliche Reaktionen sind bspw. Geschwindigkeitsreduktionen, die Verkürzung der Freigabezeit an Lichtsignalanlagen, die Öffnung von Sicherheitsspuren für den Verkehr.	Transportanbieter (Produzent)	öffentlich	User	natürliche / juristische Person	hoch (s)

Literaturverzeichnis

AGORA. (2022). Pkw-Maut für die Mobilitätswende, Eine verursachergerechte Straßennutzungsgebühr als Baustein für ein digitalisiertes und klimaneutrales Verkehrssystem.

Amstutz, M. (2018). Dateneigentum. Funktion und Form. Archiv fuer die civilistische Praxis, 218(2), 438–551.

ASTRA. (2019). Auswirkungen des automatisierten Fahrens; Teilprojekt 4; Neue Angebotsformen.

ASTRA. (2020). Verkehr der Zukunft 2060: Neue Angebotsformen – Organisation und Diffusion.

Avenir Mobilité. (2018). Mobilität wird als Dienstleistung neu definiert – Fazitbericht der Dialogveranstaltung vom 23. Februar 2018. https://www.zukunft-mobilitaet.ch/images/Dialoganlass_23.Februar_2018/Fazitbericht_Dialoganlass_MaaS_2018-02-23_vf.pdf

B. Oehry et.al. (2002). CARDME-4: The CARDME Concept. European Commission Re-search Project ITS 1999-29053.

Baeriswyl, B. (2020). Datencrash im vernetzten Verkehr. In Datenschutz im vernetzten Fahrzeug (S. 29–38).

BAV. (2021a). Daten für eine vernetzte Mobilität: Bericht des UVEK zu Massnahmen im Rahmen des Programms für eine vernetzte und effiziente Mobilität [Entwurf].

BAV. (2021b). Konzeptpapier Multimodale Mobilität / Mobilitätsdateninfrastrukturen des Bundes—Basisdokument zum gesamtheitlichen Überblick der Inhalte zur multimodalen Mobilität.

BAV. (2021c). Open-Data-Plattform Mobilität Schweiz. https://opentransportdata.swiss/de/

BAV. (2021d). Vernetzte (multimodale) Mobilität. https://www.bav.admin.ch/bav/de/home/allgemeine-themen/mmm.html

BAV. (2022). Glossar. https://www.bav.admin.ch/bav/de/home/glossar.html

Belli, L. (2015). A heterostakeholder cooperation for sustainable internet policymaking. Internet Policy Review, 4(2), 1–21.

BMVI. (2019). Mobilitätsdaten für durchgängige Reiseinformationsdienste. https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/multimodale-reisefunktionen-flyer.html

Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T. P., Krøigaard, M., Nielsen, J. D., Nielsen, J. B., Nielsen, K., Pagter, J., Schwartzbach, M. I., & Toft, T. (2009). Secure Multiparty Computation Goes Live. In R. Dingledine & P. Golle (Hrsg.), Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers (Bd. 5628, S. 325–343). Springer. https://doi.org/10.1007/978-3-642-03549-4_20

Boneh, D., Sahai, A., & Waters, B. (2012). Functional encryption: A new vision for public-key cryptography. Communications of the ACM, 55(11), 56–64.

Bonyár, A., Géczy, A., Krammer, O., Sántha, H., Illés, B., Kámán, J., Szalay, Z., Hanák, P., & Harsányi, G. (2017). A review on current eCall systems for autonomous car accident detection. 2017 40th International Spring Seminar on Electronics Technology (ISSE), 1–8.

Borrello, P., Kogler, A., Schwarzl, M., Lipp, M., Gruss, D., & Schwarz, M. (2022). ÆPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture.

Brambilla, M., Nicoli, M., Savaresi, S., & Spagnolini, U. (2019). Inertial sensor aided mmWave beam tracking to support cooperative autonomous driving. 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 1–6.

Bundesrat. (2016). Mobility Pricing, Ansätze zur Lösung von Verkehrsproblemen für Strasse und Schiene in der Schweiz.

Bundesrat. (2018). Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73398.html

Bundesrat. (2022). Bundesrat legt nächste Schritte zur nachhaltigen Finanzierung der Verkehrsinfrastruktur fest. https://www.astra.admin.ch/astra/de/home/dokumentation/medienmitteilungen/anzeige-meldungen.msg-id-89512.html

Bundesversammlung. (2022). Bundesgesetz über die Personenbeförderung—Reform des regionalen Personenverkehrs und der Rechnungslegung. Art. 17a. https://www.parlament.ch/centers/eparl/curia/2021/20210039/Schlussabstimmungstext%201%20NS%20D.pdf

Christensen, L., & Dannberg, D. (2019). Ethical hacking of IoT devices: OBD-II dongles.

Contreras, J. L. (2019). The false promise of health data ownership. New York University Law Review, 94(4), 624–661.

Costantini, F. (2017). MaaS and GDPR: an overview. arXiv preprint arXiv:1711.02950.

Cottrill, C. D. (2020). MaaS surveillance: Privacy considerations in mobility as a service. Transportation Research Part A: Policy and Practice, 131, 50–57.

Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity: Opportunities and challenges for the digital revolution. arXiv preprint arXiv:1712.01767.

Docherty, I., Marsden, G., & Anable, J. (2018). The governance of smart mobility. Transportation Research Part A: Policy and Practice, 115, 114–125.

Drexl, J. (2017). Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz-Teil 1. NZKart-Neue Zeitschrift für Kartellrecht, 5(7), 339–344.

Eckert, M. (2016). Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten. Schweizerische Juristen-Zeitung, 112(11), 265–274.

EDRM. (2021). Information Governance Reference Model. https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/

EG. (2009). 2009/750/EG_ Entscheidung der Kommission vom 6. Oktober 2009 über die Festlegung der Merkmale des europäischen elektronischen Mautdienstes und seiner technischen Komponenten (Bekannt gegeben unter Aktenzeichen K(2009) 7547) (Text von Bedeutung für den EWR).

EG. (2020a). Delegierte Verordnung (EU) 2020/203 der Kommission vom 28. November 2019 über die Klassifizierung von Fahrzeugen, Pflichten der Nutzer des europäischen elektronischen Mautdienstes, Anforderungen an Interoperabilitätskomponenten und Mindesteignungskriterien für benannte Stellen (Text von Bedeutung für den EWR).

EG. (2020b). Durchführungsverordnung (EU) 2020/204 der Kommission vom 28. November 2019 über detaillierte Pflichten der Anbieter des europäischen elektronischen Mautdienstes, den Mindestinhalt der Vorgabe für das EETS-Gebiet, elektronische Schnittstellen und Anforderungen an Interoperabilitätskomponenten sowie zur Aufhebung der Entscheidung 2009/750/EG.

Engdahl, J., & Oehry, B. (2020). Analyse de la législation européenne relative aux STI.

Enveil. (2021). Encrypted Veil. https://www.enveil.com/

EOSC. (2019). Governance Model—Community Lead Governance. https://europeanopensciencecloud.github.io/Governance/GovernanceModel.html

EU. (2004). DIRECTIVE 2004/52/EC on the interoperability of electronic road toll systems in the Community. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.L_.2004.166.01.0124.01.ENG

EU. (2019). Directive (EU) 2019/520 of the European Parliament and of the Council of 19 March 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union (recast) (Text with EEA relevance.).

EU-ICIP. (2020). EFC - Tolling. https://www.mobilityits.eu/efc-tolling

European Data Protection Supervisor. (2016). Stellungnahme 9/2016 des EDSB zu Systemen für das Personal Information Management (PIM). https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_de

Evans, B. J. (2011). Much ado about data ownership. Harvard Journal of Law & Technology, 25(1), 69–130.

Fernandez, D., Futoransky, A., Ajzenman, G., Travizano, M., & Sarraute, C. (2020). Wibson protocol for secure data exchange and batch payments. arXiv preprint arXiv:2001.08832.

Festag, A. (2014). Cooperative intelligent transport systems standards in Europe. IEEE communications magazine, 52(12), 166–172.

Fezer, K.-H. (2017). Dateneigentum der Bürger. Ein originäres Immaterialgüterrecht sui generis an verhaltensgenerierten Informationsdaten der Bürger, 3, 99–105.

Früh, A. (2018). Datenzugangsrechte. Rechtsrahmen für einen neuen Interessenausgleich in der Datenwirtschaft. sic!: Zeitschrift für Immaterialgüter-, Informations-und Wettbewerbsrecht, 22(10), 521–539.

Gaia X. (2022). What is Gaia-X. https://gaia-x.eu/what-is-gaia-x/

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In M. Mitzenmacher (Hrsg.), Proceedings of the 41st Annual ACM Symposium on Theory of Compu-ting, STOC 2009, Bethesda, MD, USA, May 31—June 2, 2009 (S. 169–178). ACM. https://doi.org/10.1145/1536414.1536440

Goldreich, O., Micali, S., & Wigderson, A. (1987). How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. In A. V. Aho (Hrsg.), Proceedings of the 19th Annual ACM Symposium on Theory of Compu-ting, 1987, New York, New York, USA (S. 218–229). ACM. https://doi.org/10.1145/28395.28420

Grafenstein, M. (2022). Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR).

Gress, S., & Springborn, F. (2020). In Datenschutz im vernetzten Fahrzeug (S. 55–70).

Hensher, D. A., Mulley, C., Ho, C., Wong, Y., Smith, G., & Nelson, J. D. (2020). Understanding Mobility as a Service (MaaS): Past, present and future.

Hepp, M., & Stückelberger, U. (2011). Die Konzession im Strassenverkehr. In Jahrbuch zum Strassenverkehrsrecht 2011.

Heuberger, O. (2020). Profiling im Persönlichkeits-und Datenschutzrecht der Schweiz.

Hilty, L. M. (2012). Lokalisiert und identifiziert: Wie Ortungstechnologien unser Leben verändern.

Hofheinz, P., & Osimo, D. (2017). Making Europe a data economy: A new framework for free movement of data in the digital age. Lisbon Council Policy Brief, 11(1).

IDS. (2022). International Data Spaces (IDS). https://internationaldataspaces.org/

INFRAS/Rapp/Ecoplan. (2021). Konzeption einer fahrleistungsabhängigen Abgabe.

ISO 5616. (o. J.). (all parts) Intelligent transport systems—Secure interfaces Governance [Working Draft].

ISO 14813-1. (2015). Intelligent transport systems—Reference model architecture(s) for the ITS sector—Part 1: ITS service domains, service groups and services.

ISO 15408. (o. J.). ISO/IEC Standard 15408—Information technology—Security techniques—Evaluation criteria for IT security. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-15408

ISO 20077. (o. J.). (all parts) Road Vehicles—Extended vehicle (ExVe) methodology.

ISO 20078. (o. J.). (all parts) Road vehicles—Extended vehicle (ExVe) web services.

ITS CH. (2021). Daten in der Mobilität—Bericht Arbeitsgruppe Daten. https://www.its-ch.ch/publikationen/

Javed, M. A., Zeadally, S., & Hamida, E. B. (2019). Data analytics for cooperative intelligent transport systems. Vehicular communications, 15, 63–72.

Jittrapirom, P., Caiati, V., Feneri, A.-M., Ebrahimigharehbaghi, S., Alonso González, M. J., & Narayan, J. (2017). Mobility as a service: A critical review of definitions, assessments of schemes, and key challenges. 13–25.

Kamargianni, M., Li, W., & Matyas, M. (2016). A critical review of new mobility services for urban transport. Transportation Research Procedia, 14, 3294–3303.

Kamargianni, M., & Matyas, M. (2017). The business ecosystem of mobility-as-a-service. 96th Transportation Research Board.

Kerber, W. (2018). Data governance in connected cars: The problem of access to in-vehicle data. J. Intell. Prop. Info. Tech. & Elec. Com. L., 9, 310.

Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., & Yarom, Y. (2019). Spectre Attacks: Exploiting Speculative Execution. 2019 IEEE Symposium on Security and Privacy, SP 2019, San Francis-co, CA, USA, May 19-23, 2019, 1–19. https://doi.org/10.1109/SP.2019.00002

Kooper, M. N., Maes, R., & Lindgreen, E. R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. International journal of information management, 31(3), 195–200.

Koutsos, V., Papadopoulos, D., Chatzopoulos, D., Tarkoma, S., & Hui, P. (2021). Agora: A Privacy-Aware Data Marketplace. IEEE Transactions on Dependable and Secure Computing.

KRAKEN. (2020). Project Overview of the KRAKEN (BroKeRage and MArKet platform for pErsoNal data) project. https://www.krakenh2020.eu/the_project/overview

Li, T., Lin, L., & Gong, S. (2019). AutoMPC: Efficient Multi-Party Computation for Secure and Privacy-Preserving Cooperative Control of Connected Autonomous Vehicles. In H. Espinoza, S. Ó. hÉigeartaigh, X. Huang, J. Hernández-Orallo, & M. Castillo-Effen (Hrsg.), Workshop on Artificial Intelligence Safety 2019 co-located with the Thirty-Third AAAI Conference on Artificial Intelligence 2019 (AAAI-19), Honolulu, Hawaii, January 27, 2019 (Bd. 2301). CEUR-WS.org.

Lobsiger, A., & Rudin, B. (2020). Datenschutztag 2020: Zunehmende Vermessung der Privatsphäre bei der Mobilität – neues Datenschutzgesetz überfällig. https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-77914.html

López-Alt, A., Tromer, E., & Vaikuntanathan, V. (2012). On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In H. J. Karloff & T. Pitassi (Hrsg.), Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19—22, 2012 (S. 1219–1234). ACM. https://doi.org/10.1145/2213977.2214086

Lorentz, N. (2020). Profiling-Persönlichkeitsschutz durch Datenschutz?: Eine Standortbestimmung nach Inkrafttreten der DSGVO (Bd. 7).

Lyons, G., Hammond, P., & Mackay, K. (2019). The importance of user perspective in the evolution of MaaS. Transportation Research Part A: Policy and Practice, 121, 22–36.

MaaS4EU. (2018a). MaaS Policy Framework. https://www.maas4eu.eu/download-area/documents-reports/

MaaS4EU. (2018b). User Information. https://www.maas4eu.eu/download-area/documents-reports/

Medicalchain. (2018). Whitepaper 2.1. https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

Michael, O., Carsten, R., & Christian, H. (2019). DG4MaaS - Daten-Governance Regeln für Mobility-as-a-Service.

MIDATA. (2021). My Data – Our Health. https://www.midata.coop/en/home/

Morley-Fletcher, E. (2017). MHMD: My Health, My Data. EDBT/ICDT Workshops, 1810. CEUR-WS.org

Nilsson, A., Bideh, P. N., & Brorsson, J. (2020). A Survey of Published Attacks on Intel SGX. CoRR, abs/2006.13598. https://arxiv.org/abs/2006.13598

Nordic Innovation. (2022). Nordic Open Mobility and Digitalisation (NOMAD). https://www.nordicinnovation.org/programs/nordic-open-mobility-and-digitalisation-nomad

NZZ. (2021). Wissenschafter haben die 13-Milliarden-Franken-Frage untersucht: Wie man beim Verkehr für Kostenwahrheit sorgt. https://www.nzz.ch/wirtschaft/mobility-pricing-wie-man-ein-13-milliarden-franken-problem-in-den-griff-bekommt-ld.1648548

NZZ. (2022). Das EU-Parlament will ab 2035 nur noch emissionsfreie Fahrzeuge zulassen. https://www.nzz.ch/wirtschaft/eu-parlament-verbietet-verbrennungsmotoren-ab-2035-ld.1687904

Otto, B., & Burmann, A. (2021). Europäische Dateninfrastrukturen. Informatik Spektrum, 44(4), 283–291.

Paskaleva, K., Evans, J., Martin, C., Linjordet, T., Yang, D., & Karvonen, A. (2017). Data governance in the sustainable smart city. Informatics, 4(4), 41.

Pollicino, O., Lubello, V., & Stojanovic, A. (2022). Regulating Mobility-as-a-Service. Global Community Yearbook of International Law and Jurisprudence.

Priora, G., & Sganga, C. (2020). Smart Urban Mobility: A Positive or Negative IP Space? A Case Study to Test the Role of IP in Fostering Digital Data-Driven Innovation. In Smart Urban Mobility (S. 143–162).

Purtova, N. (2015). The illusion of personal data as no one's property. {Law, Innovation and Technology}, 7(1), 83–111.

Reich, A., Krämer, N. A., & Lenninger, R. (2018). Vehicle data mangement a standardized access as the basis of new business models. ATZelektronik worldwide, 13(2), 38–43.

Rittershaus, L. (2021). Mobilitäts Daten Marktplatz—Präsentation Verkehrsdatenplattform CH - Onboarding. BAST.

Rosenthal, D. (2012). Das Bauchgefühl im Datenschutz, in: Von der Lochkarte zum Mobile Computing, 20 Jahre Datenschutz in der Schweiz,. Datenschutz-Forum Schweiz.

Rosenthal, D. (2020). Das neue Datenschutzgesetz. Jusletter.

Roßnagel, A. (2017). Datenschutz im vernetzten Fahrzeug. In Autonome Systeme und neue Mobilität (S. 23–48).

Sackmann, F. (2020). Datenschutz bei der Digitalisierung der Mobilität: Eine sektorspezifische Analyse der Leistungsfähigkeit und des Weiterentwicklungsbedarfs der Datenschutzordnung.

Schulz, W., Wittner, F., Bavendiek, K., & Schupp, S. (2020). Modelling and verification in GDPR's data protection impact assessment: A case study on the AccuWeather/Reveal Mobile Case. Data protection and privacy: Data protection and democracy, 12, 145 ff.

Smith, G., Sochor, J., & Karlsson, I. M. (2020). Intermediary MaaS Integrators: A case study on hopes and fears. Transportation Research Part A: Policy and Practice, 131, 163–177.

Sochor, J., Arby, H., & Karlsson, M. I. C. (2018). A topological approach to Mobility as a Service: A proposed tool for understanding requirements and effects, and for aiding the integration of societal goals. Research in Transportation Business & Management, 27, 3–14.

Spiecker-Döhmann, I. (2019). Digitale Mobilität: Plattform Governance, IT-sicherheits- und

datenschutzrechtliche Implikationen. Gewerblicher Rechtsschutz und Urheberrecht, 4, 341–352.

swisstopo. (2021a). OGD. https://www.swisstopo.admin.ch/de/swisstopo/kostenlose-geobasisdaten.html

swisstopo. (2021b). Verkehrsnetz Schweiz. https://www.swisstopo.admin.ch/de/swisstopo/verkehrsnetz-schweiz.html

Thouvenin, F. (2016). Dynamische Preise: Eine Herausforderung für das Datenschutz-, Wettbewerbs-und Vertragsrecht. Jusletter IT, 22.09. 2016.

Thouvenin, F., & Früh, A. (2020). Zuordnung von Sachdaten, Eigentum, Besitz und Nutzung bei nicht-personenbezogenen Daten. Universität Zürich.

UN. (2009). What is Good Governance? https://www.unescap.org/sites/default/d8files/knowledge-products/good-governance.pdf

UNECE. (2020). Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

UVEK. (2007). Mobility Pricing Synthesebericht.

UVEK. (2022). Bundesgesetz über die Mobilitätsdateninfrastruktur Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens.

Wagner, J. M. S., Scholz, S., & Gennat, M. (2020). Verarbeitung, Visualisierung und Kalibrierung von Verkehrsdaten. In Neue Dimensionen der Mobilität: Technische und betriebswirtschaftliche Aspekte (S. 477–487).

Weber, R. H. (2019). Zugang zu maschinengenerierten Daten. Jusletter.

Weber, R. H., & Chrobak, L. (2018). Art. 5 lit. C UWG. In UWG Kommentar Bundesgesetz gegen den unlauteren Wettbewerb.

Weber, R. H., & Thouvenin, F. (2018). Dateneigentum und Datenzugangsrechte–Bausteine der Informationsgesellschaft? Zeitschrift für Schweizerisches Recht (ZSR), 137(1), 43–74.

Weber, R. H., Thouvenin, F., Früh, A., George, D., & Reutimann, K. (2017). Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS). Center for Information Technology, Society, and Law (ITSL).

Whim Global. (2019). Datenschutzerklärung. https://whimapp.com/de/privacy/

Wimmer, M. A., Scanlon, M., Rigole, C., Boneva, R., & Lobo, G. (2018). D03.01 Interoperability governance models. ISA Action 2016.33 EIS Governance Support. https://ec.europa.eu/isa2/news/new-report-interoperability-governance-models-published_en

Yao, A. C.-C. (1982). Protocols for Secure Computations (Extended Abstract). 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982, 160–164. https://doi.org/10.1109/SFCS.1982.38

Abkürzungsverzeichnis

Abkürzung	Bedeutung
API	Application Programming Interface
ASTRA	Bundesamt für Strassen
B2C	Business-to-Consumer
B2G2C	Business-to-Government-to-Consumer
BAV	Bundesamt für Verkehr
BehiG	Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (SR 151.3)
BGE	Bundesgerichtsentscheid
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (SR 152.3)
BMVI	Bundesministerium für Digitales und Verkehr der Bundesrepublik Deutschland
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (SR 101)
C-ITS	Cooperative Intelligent Transport Systems
CN	Cellular Network
DiDok	Dienststellendokumentation öV-Schweiz
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
DSGVO	Datenschutz-Grundverordnung der Europäischen Union
nDSG	Revidiertes Bundesgesetz über den Datenschutz (SR 235.1)
EDRM	Electronic Discovery Reference Model
EETS	European Electronic Tolling Service
EU	Europäische Union
FE	Funktionale Verschlüsselung
FHE	Fully Homomorphic Encryption (vollständig homomorpher Verschlüsselung)
GA	Generalabonnement
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile Communications
IDS	International-Data-Spaces
IFMS	Interoperable Fare Management Systems
IGRM	Information Governance Reference Model
IMI	Intermediary MaaS Integrator
IoT	Internet of Things
ISO	International Organization for Standardization
ISU	Informationssystem Strassenverkehrsunfälle
ITS	Intelligent Transport Systems
IVZ	Informationssystem Verkehrszulassung
KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (SR 251)
KTU	Konzessionierte Transportunternehmen
LSVA	Leistungsabhängige Schwerverkehrsabgabe
MaaS	Mobility-as-a-Service
MDM	Mobilitätsdaten Marktplatz (NAP in Deutschland)

MIV	Motorisierter Individualverkehr
MODI	Mobilitätsdateninfrastruktur
MODIG	Bundesgesetz über die Mobilitätsdateninfrastruktur
MPC	Multi-Party Computation
NAP	National Access Point (Nationaler Zugangspunkt)
NADIM	Nationale Datenvernetzungsinfrastruktur Mobilität
NOVA	Plattform Neue ÖV -Anbindung als zentrales Preis- und Vertriebsbasissystem
PauRG	Bundesgesetz über Pauschalreisen (SR 944.3)
PIMS	Personal Information Management Systems
PBG	Bundesgesetz über die Personenbeförderung (SR 745.1)
PBV	Verordnung über die Bekanntgabe von Preisen vom 11. Dezember 1978 (SR 942.211)
RL	EU-Richtlinie
RUC	Strassengebührenerhebung (Road User Charge)
SBB	Schweizerische Bundesbahnen
SKI	Systemaufgaben Kundeninformation
SR	Systematische Rechtssammlung
SSI	Selbstsouveräne Identität
StGB	Schweizerisches Strafgesetzbuch
SVG	Strassenverkehrsgesetz (SR 741.01)
TEE	Trusted Execution Environment
UNECE	United Nations Economic Commission for Europe
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (SR 231.1)
UVEK	Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation
UWG	Bundesgesetz gegen den unlauteren Wettbewerb (SR 241)
VAböV	Verordnung des UVEK über die technischen Anforderungen an die behindertengerechte Gestaltung des öffentlichen Verkehrs (SR 151.42)
VböV	Verordnung über die behindertengerechte Gestaltung des öffentlichen Verkehrs (SR 151.34)
VDP	Verkehrsdatenplattform Schweiz
VDSZ	Verordnung über die Datenschutzzertifizierungen (SR 235.13)
VIN	Vehicle Identification Number
VnCH	Verkehrsnetz Schweiz
VO	EU-Verordnung
VPB	Verordnung über die Personenbeförderung (SR 745.11)
ZGB	Schweizerisches Zivilgesetzbuch (SR 210)

Projektabschluss

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

FORSCHUNG IM STRASSENWESEN DES UVEK

Version vom 09.10.2013

Formular Nr. 3: Projektabschluss

erstellt / geändert am: 18.01.2023

Grunddaten

Projekt-Nr.:	MB4_20_01B_01
Projekttitel:	Data Governance for Smart Mobility ("DAGSAM")
Enddatum:	31.03.2023

Texte

Zusammenfassung der Projektresultate:

Im Projekt konnten die Smart Mobility-Anwendungen systematisiert werden, um die Datentypen sowie die Datenflüsse zwischen den involvierten Akteure zu generalisieren. Das entwickelte generische Rollenmodell erlaubt die Anwendungen sowie die Datenflüsse ausreichend genau zu beschreiben, um damit ein breit verwendbares Data Governance-Modell zu entwickeln.
Um die Data Governance auf eine juristische Grundlage zu stellen, wurden die entsprechenden juristischen Instrumente zusammengefasst. Es wurden Schemata entwickelt, mit denen sich prüfen lässt, welche Akteure in einem konkreten Mobilitätsangebot an welchen Daten berechtigt sind und wie der Datenzugang geregelt werden kann. Damit die Data Governance technologisch umgesetzt werden kann, werden ausgewählte Technologien präsentiert. Diese technologischen Instrumente dienen dazu, eine konkrete Auswahl von technologischen und kryptographischen Methoden zu treffen, um Datenschutz, Authentizität, oder Auditierbarkeit sicherzustellen. Die Instrumente erlauben es, Berechnungen auf Daten durchzuführen und gleichzeitig die Interessen der beteiligten Akteure zu wahren.
Das entwickelte generische Governance-Modell in vier Schritten berücksichtigt die Gesamtheit aller Normen und Bedingungen, die für das Funktionieren einer Smart Mobility-Anwendung massgebend sein können. Im ersten Schritt werden die Akteure identifiziert, um Zuständigkeiten und Verantwortlichkeiten zu regeln. Anschliessend folgt die Thematisierung der für den Datenaustausch notwendigen Infrastruktur. Im dritten Schritt wird der geltende Rechtsrahmen untersucht. Im letzten Schritt wird die Data Governance zum Umgang mit Mobilitätsdaten behandelt. Mittels eines Analyserasters kann ermittelt werden, welche technischen, rechtlichen oder organisatorischen Prinzipien bzw. Regeln in Bezug auf die konkrete Anwendung erforderlich sind. In diesem Analyseraster wird die gute Mobilitätsanwendung als Zielsetzung definiert. Es folgt eine Analyse der Datenzuordnung in der Ausgangslage und die Spezifizierung der Datennutzung. Abschliessend werden die bestehenden Hindernisse identifiziert und mit rechtlichen, technischen oder organisatorischen Massnahmen adressiert.
Dieses Governance-Modell wurde anhand der zwei konkreten Smart Mobility-Anwendungen Mobility-as-a-Service (MaaS) und Strassengebührenerhebung (RUC) getestet. Für MaaS wird aufgezeigt, wie der geltende Rechtsrahmen angepasst werden müsste und für RUC wird ein privatsphärenschützendes Systemdesign vorgeschlagen, welches erlaubt, hochsensible Daten für die Berechnung der Gebühr sowie deren Kontrolle zu verwenden.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

Zielerreichung:

Die folgenden, gemäss der Bewerbung formulierten Ziele konnten erreicht werden:
- In Bezug auf wissenschaftlich-rechtliche Aspekte und Governance-Fragen werden mit den entwickelten Instrumenten die verschiedenen regulatorischen Anforderungen, die sich aus öffentlich-rechtlicher und privatrechtlicher Sicht ergeben, in einem konsistenten Rahmen verknüpft.
- Die Lücke in der aktuellen Forschung in Bezug auf Data-Governance und -"Eigentum" für Smart Mobility sowie die Möglichkeiten zum Schutz dieser Daten mit modernsten kryptographischen Technologien konnte identifiziert und zumindest in Teilen geschlossen werden.
- Das ausgearbeitete Data Governance Modell bietet ein Instrument, um den Bedürfnissen der zivilen, industriellen und öffentlichen Interessengruppen zu entsprechen.
- Das entwickelte Modell konnte anhand von zwei Anwendungen geprüft werden und legt dar, wie es sich in die rechtlichen und technologischen Rahmenbedingungen einbettet.

Folgerungen und Empfehlungen:

Es zeigte sich, dass mit dem erarbeiten Governance-Modell das Zusammenspiel organisatorischer, rechtlicher und technischer Aspekte einheitlich analysiert werden kann. So lässt sich bei der Entwicklung von Dienstleistungen in der "Neuen Mobilität" jeweils eine passende Data Governance entwickeln und implementieren. Je nach Mobilitätsanwendung können dabei eher rechtliche (wie bei MaaS) oder eher technische Aspekte (wie bei RUC) im Vordergrund stehen. Eine zentrale Erkenntnis des Forschungsprojekts lautet, dass Governance-Strukturen – ganz unabhängig von der konkreten Mobilitätsanwendung – zuvorderst Vertrauen zwischen den involvierten Akteuren schaffen müssen und dass der Aufbau des Vertrauens im Idealfall die frühzeitige Integration sämtlicher Interessengruppen erfordert.

Die in diesem Forschungsprojekt entwickelten Modelle können einen Beitrag leisten, um die Data Governance für die Schweizer Mobilität zu fördern. Konkret ergeben sich aus Sicht der am Forschungsprojekt beteiligten Disziplinen drei Empfehlungen:
1. Anwendung und ggf. Weiterentwicklung des allgemeinen Governance-Modells
2. Anpassung des Rechtsrahmens für MaaS
3. Machbarkeitsstudie zu sicheren Rechenumgebungen für RUC

Publikationen:

Früh, A., Binder, N. B., & Schibli, R. (2022). Data Governance für Smart Mobility aus rechtlicher Perspektive. sui generis. https://sui-generis.ch/article/view/sg.200

Oehry, B. (2022). Data Governance für Smart Mobility. asut-Bulletin 03/2022. https://asut.ch/asut/bulletin/view.xhtml?bulletinId=46&articleId=746

Der Projektleiter/die Projektleiterin:

Name: Oehry Vorname: Bernhard

Amt, Firma, Institut: Rapp AG

Unterschrift des Projektleiters/der Projektleiterin:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

FORSCHUNG IM STRASSENWESEN DES UVEK

Formular Nr. 3: Projektabschluss

Beurteilung der Begleitkommission:

Beurteilung:

Das Forschungsprojekt DAGSAM hat die Zielsetzungen des Vorhabens vollständig erreicht. Dank des methodisch klar aufgebauten Forschungsdesign konnte das interdisziplinäre Projektteam eine umfassende Sicht herstellen und einen praktikablen "Werkzeugkasten" für die Entwicklung von spezifischen "Data-Governances" für verschiedene Anwendungsfälle in der Mobilität entwickeln. Durch die Anwendung auf zwei deutlich unterschiedliche Use Cases konnte das Verfahren verifiziert werden. Mit vier klar verständlichen Schritten kann das Verfahren breit kommuniziert und angewendet werden, wobei die Nutzniesser sowohl Unternehmen als auch Körperschaften der öffentlichen Hand sein können, aber auch Interessensvertreter von privaten Akteuren werden von diesem Modell profitieren. Zusammengefasst hat das Projektteam ein sehr gutes Ergebnis produziert.

Umsetzung:

Interdisziplinäre Forschungsprojekte stellen aufgrund der verschiedenen Arbeitsweisen und Fachsprache der Disziplinen eine grosse Herausforderung dar. Das Projektteam hat diese sehr gut bewältigt. Die Projektplanung war klar und wurde eingehalten, das Vorgehen methodisch einwandfrei. Die von fachlichen Hintergrund sehr breit aufgestellte Begleitkommission wurde aktiv einbezogen und konnte ihre jeweiligen Sichtweisen und Kenntnisse optimal einbringen. Im Review des Schlussberichts aufgetretene Differenzen zu einigen Punkte konnten in einer Sondersitzung der Begleitkommission geklärt und ausgeräumt werden, so dass der finale Bericht von der Begleitkommission vollumfänglich getragen wird.

weitergehender Forschungsbedarf:

Für sich betrachtet, ist mit dem vorliegenden Ergebnis das Forschungsziel erreicht und es bedarf keines zwingenden Anschlussprojekts. Mit der Anwendung der erarbeiteten Methode und im Blick auf angrenzende Themenfelder wie "Digitale Selbstbestimmung" oder "Digitale Souveränität" ist jedoch zu erwarten und zu wünschen, dass sich darauf aufbauende neue Forschungsfragen stellen. Diese können je nach Art der Fragestellung für das Forschungsprogramm des ASTRA oder andere Programme relevant werden.

Einfluss auf Normenwerk:

Aus Sicht der Begleitkommission betrifft das Ergebnis keine Norm. Das entwickelte Modell sollte konsequent und breit zur Entwicklung von use case spezifischen Governances in der öffentlichen Verwaltung auf Bundes- und Kantonsstufe verwendet werden und über Fachgremien privaten Akteuren als Instrument bekannt gemacht werden.

Der Präsident/die Präsidentin der Begleitkommission:

Name: Kronawitter Vorname: Andreas

Amt, Firma, Institut: Geschäftsführer its switzerland

Unterschrift des Präsidenten/der Präsidentin der Begleitkommission:

Signature: Dr. Andreas Kronawitter
Dr. Andreas Kronawitter (Jan 24, 2023 22:09 GMT+1)

Email: kronawitter@its-ch.ch