Lernende Systeme

DIE PLATTFORM FÜR KÜNSTLICHE INTELLIGENZ

Mit KI sicher reisen

Datenmanagement und Datensicherheit bei KI-basierten Reiseassistenten

WHITEPAPER

Tobias Hesse, Jörn Müller-Quade et al.
AG IT-Sicherheit, Privacy, Recht und Ethik
AG Mobilität und intelligente Verkehrssysteme

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Inhalt

Zusammenfassung

Der Trend ist klar erkennbar. Die Mobilität der Zukunft wird digital vernetzt sein und individuelle, passgenaue Mobilitätsserviceangebote liefern. Künstliche Intelligenz (KI) kann hier einen wichtigen Beitrag leisten, indem sie einerseits Infrastrukturen, die Umwelt sowie Ressourcen nachhaltig und effizient entlasten kann sowie andererseits Reisende zeitsparend und flexibel ans Ziel geleitet. Dies bequem mit dem intelligenten Reiseassistenten als Reiseterminal am Smartphone oder auf dem Laptop: verschiedene Verkehrsmittel miteinander kombinieren, optimal planen und, wenn gewünscht, auch gleich buchen. Und als weiterer Vorteil: Der intelligente Reiseassistent lernt mit jedem Male dazu, sodass persönliche Präferenzen auf Wunsch bei der nächsten Reiseplanung automatisch berücksichtigt werden. Entscheidend für den Einsatz eines solchen Reiseassistenten ist jedoch, wie der Umgang mit den anfallenden Daten entlang der Mobilitätsdienstleistungskette im Hinblick auf IT-Sicherheit und Datenschutz geregelt und gewährleistet ist.

Experten der Arbeitsgruppen IT-Sicherheit, Privacy, Recht und Ethik sowie Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme befassen sich im vorliegenden Whitepaper mit Fragestellungen zur IT-Sicherheit im Rahmen der Entstehung und Nutzung von Daten in KI-basierten Reiseassistenten. Exemplarisch wird hierzu das fiktive Anwendungsszenario eines digitalen Reiseassistenten aus Carlas Reise (Kapitel 2) herangezogen, das von der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme entwickelt wurde. Die Autoren erläutern mögliche Optionen der Ausgestaltung von digitalen Reiseassistenten und skizzieren in diesem Umfeld das Spannungsfeld zwischen Usability und Datenschutz.

Die technische Grundlage des intelligenten Reiseassistenten bildet eine digitale Mobilitätsplattform, die Teil einer Systemarchitektur ist, über die mehrere Datenhalter, wie Mobilitätsbetreiber, Verkehrsunternehmen oder Infrastrukturbetreiber, ihre Daten freiwillig miteinander vernetzen. Das Betreibermodell der jeweiligen Mobilitätsplattform, an die der intelligente Reiseassistent angebunden ist, kann dabei unterschiedlich ausgestaltet sein: Möglich sind eine übergeordnete zentrale Plattform oder eine föderierte dezentrale Plattform (Kapitel 4.3).

Mittels der Mobilitätsplattform können intelligente Reiseassistenten einen wesentlichen Beitrag zur Optimierung von Reisen leisten, indem sie den persönlichen Reisekomfort steigern und dazu beitragen, Verkehrsflüsse zu optimieren. Hierzu sind jedoch große Datenmengen notwendig. Je nach Art der Anfrage handelt es sich mitunter auch um sensible Kundendaten. So entsteht ein Spannungsfeld zwischen Usability und Datenschutz, welches es entsprechend den Wünschen und Anforderungen der jeweiligen Nutzenden bestmöglich zu gestalten gilt: Der intelligente Reiseassistent muss einerseits für die Nutzenden einfach zu bedienen und trotzdem sehr sicher sein.

Die Mobilitätsplattform selbst hält keine Daten zentral vor; vielmehr verbleiben die abgefragten Daten bei den jeweiligen Datenhaltern. Damit wird eine Grundlage für die Beteiligung aller Akteure vom Mobilitätsbetreiber über weitere Datenhalter bis hin zu den Nutzenden in einem kreativen Vertrauensökosystem geschaffen. Ein Schlüsselfaktor für die Mobilitätsplattform ist die vertrauenswürdige Identifizierung der Mobilitätsanbieter; flankiert von entsprechenden Richtlinien sowie gesetzlichen Vorgaben hinsichtlich Zugangsrechten, Datensparsamkeit, Audits oder Zertifizierungen.

Der Einsatz eines intelligenten Reiseassistenten in solch einem komplexen Datenökosystem stellt aber gleichzeitig hohe Anforderungen an die IT-Sicherheit und den Datenschutz. Ziel der Autoren ist es daher, mögliche Risiken beim Einsatz eines KI-basierten Reiseassistenten zu identifizieren und mögliche Lösungsvorschläge dafür aufzuzeigen (Kapitel 4).

Ob intelligente Reiseassistenten in die Anwendung gelangen und ein beständiger Reisebegleiter im Alltag werden, hängt im Wesentlichen von zwei Faktoren ab. Erstens: Wie passgenau sind ihre Vorschläge für uns Nutzende? Also: Haben wir ein positives Reiseerlebnis bei der Interaktion? Zweitens: Werden die Ansprüche an Zuverlässigkeit, Sicherheit sowie an rechtliche Vorgaben erfüllt? Denn nur wenn all diese Aspekte berücksichtigt und umgesetzt werden, kann dies Vertrauen in die Sicherheit von solchen KI-basierten Systemen schaffen, was wiederum Voraussetzung für die Nutzung derartiger Reiseassistenten ist. Um Akzeptanz und Zuspruch hierfür zu finden, schlagen die Autoren konkrete Gestaltungsoptionen vor – adressiert an Entwickelnde von intelligenten Reiseassistenten, mögliche Plattformbetreiber, Mobilitätsanbieter, öffentliche Hand sowie Nutzende (Kapitel 5). Für all die Genannten gilt es, für einen sicheren und vertrauenswürdigen Umgang mit allen anfallenden Daten zu sorgen. Das heißt, alle beteiligten Akteure tragen durch ihr jeweiliges verantwortungsvolles Handeln und vertrauenswürdiges Zutun zum Erfolg des Einsatzes solcher Systeme bei: sicher unterwegs zu sein – mit dem intelligenten Reiseassistenten.

1 Einleitung

Schon heute nutzen Reisende eine Vielzahl von Apps und Portalen, um ihre Reisen zu planen: DB Navigator der Deutschen Bahn für Reiseplanung und -updates, Apps von städtischen oder regionalen Verkehrsbetrieben für Fahrpläne und Fahrkartenverkauf oder Nahverkehr-Routenplaner wie Öffi oder Citymapper, die die Angebote des ÖPNV verschiedener Städte bündeln. PKWs können über Mitfahrzentralen und Carsharing-Angebote gemeinsam genutzt werden. Einige Städte, wie etwa Augsburg mit der swa Mobil-Flat und Bielefelds moBiel, bieten bereits die Möglichkeit, in einem Angebot auf unterschiedliche Verkehrsmittel zuzugreifen. Flugreisende nutzen Airline-Apps, um Flüge zu buchen, Boarding-Cards zu speichern und Updates zu erhalten. Auf Flugportalen wie Kayak oder Swoodoo lässt sich binnen kürzester Zeit die günstigste Route für Flugreisen ermitteln. Eine Fülle von Portalen und Apps steht demnach Reisenden zur Verfügung, um von A nach B zu gelangen, deren Nutzen zum einen in der zügigen Ermittlung der günstigsten und schnellsten Route liegt sowie in der Möglichkeit, die Reise bargeldlos zu bezahlen und Updates zum Reiseverlauf zu bekommen. Dennoch müssen Reisende, je nachdem, welches Verkehrsmittel sie nutzen möchten, auf jeweils unterschiedliche Portale und Navigatoren zurückgreifen.

Denn aktuell existieren noch keine Reiseassistenten, die für eine geplante Reise unter Berücksichtigung persönlicher Präferenzen sowohl verkehrsmittel- als auch abschnittsübergreifende Routenvorschläge erstellen können. Große Potenziale, solche Reiseassistenten umzusetzen, liegen im Einsatz von Künstlicher Intelligenz (KI). Mittels dieser können Angebote im Hintergrund gebündelt, analysiert und nutzerspezifische Reiserouten vorgeschlagen werden. Wie ein solcher Reiseassistent funktionieren kann, hat die Arbeitsgruppe Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme in einem Anwendungsszenario skizziert: einsetzbar zur Planung, Buchung, aber auch zur Änderung der Reise bei unvorhergesehenen Einschränkungen im Verkehrsfluss. Durch Feedback der Nutzenden entwickelt er sich zudem stets weiter.

Die Vorteile solcher Lernender Systeme liegen auf der Hand: Die Reisenden haben zunächst einen geringeren Aufwand bei der Reiseplanung. Hinzu kommen Zeitersparnis durch eine optimierte Route und persönlicher Komfort, dadurch dass persönliche Präferenzen berücksichtigt werden. Letztlich gestaltet sich die Reise damit auch ressourcenschonender. Die Nutzung solcher intelligenter Reiseassistenten erfordert jedoch die Angabe zahlreicher Daten, die für Planung, Buchung und Bezahlung notwendig sind, die teilweise beim intelligenten Reiseassistenten verbleiben und – wenn notwendig – an integrierte Netzwerk-Akteure weitergegeben werden. Sowohl die Funktionsweise intelligenter Reiseassistenten selbst als auch die zahlreich anfallenden Daten werfen Fragen zum Datenschutz und zur IT-Sicherheit auf, die es für eine gelingende Anwendung zu lösen gilt.

Lernende Systeme
Lernende Systeme sind Maschinen, Roboter und Softwaresysteme, die abstrakt beschriebene Aufgaben auf Basis von Daten, die ihnen als Lerngrundlage dienen, selbstständig erledigen, ohne dass jeder Schritt spezifisch vom Menschen programmiert wird. Um ihre Aufgabe zu lösen, setzen sie von Lernalgorithmen trainierte Modelle ein. Mit Hilfe des Lernalgorithmus können viele Systeme im laufenden Betrieb weiterlernen: Sie verbessern die vorab trainierten Modelle und erweitern ihre Wissensbasis. Lernende Systeme basieren auf Methoden der Künstlichen Intelligenz (KI), genauer: des maschinellen Lernens. Vor allem durch die Fortschritte im Deep Learning entwickelten sich Lernende Systeme in den letzten Jahren zum dynamischsten Bereich der KI-Forschung und -Anwendung (vgl. Plattform Lernende Systeme 2021).

Das Gelingen und die Akzeptanz von intelligenten Reiseassistenten hängen im Wesentlichen davon ab, wie effektiv sie einerseits Angebote nutzerspezifisch umsetzen, und den Nutzenden andererseits gleichzeitig einen sensiblen Umgang mit ihren persönlichen Daten vor, während und nach der Reise bieten. Ziel des vorliegenden Papiers ist es, Orientierung zu geben, wie intelligente Reiseassistenten möglichst sicher und unter Einhaltung des Datenschutzes realisiert werden können. Darüber hinaus werden Hinweise gegeben, welche Daten Nutzende im Sinne ihrer informationellen Selbstbestimmung für welche Verwendungszwecke preisgeben, was bei der Anwendung zu beachten ist und wie eigene Daten geschützt werden können.

2 Das Szenario „Carlas Reise“

Das vorliegende Papier behandelt Aspekte des Datenschutzes und der IT-Sicherheit von KI-Systemen in der Reiseplanung. Hierfür wird der intelligente Reiseassistent aus dem Umfeldszenario „Intelligent vernetzt unterwegs“ der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme herangezogen (siehe Plattform Lernende Systeme 2019a). Im Folgenden wird der intelligente Reiseassistent auf seine IT-Sicherheit hin überprüft und es werden zudem mögliche Maßnahmen zur Erhöhung der IT-Sicherheit aufgezeigt. Damit die IT-Sicherheit analysiert werden kann, wird das Szenario zunächst skizziert und in der weiteren Ausführung punktuell erweitert und angepasst.

2.1 Vorstellung und Relevanz

Vorstellung des Umfeldszenarios

Das Szenario „Carlas Reise“ zeigt, wie Reisende mit Hilfe KI-basierter Verkehrsmittel, Infrastrukturen und Anwendungen (z. B. Assistenzsysteme) in Zukunft einfacher, schneller, umweltschonender, sicherer und flexibler an ihr Ziel gelangen können. Unterstützt von einem intelligenten Reiseassistenten, der durch Methoden der KI ständig dazulernt, werden sich in Zukunft sowohl die individuelle Routenplanung als auch die Steuerung von Verkehrssystemen grundlegend verändern und damit den Mobilitätsfluss kontinuierlich anpassen und optimieren.

Carla Fuchs wohnt in einem Dorf in Brandenburg. Am Nachmittag hat sie einen Termin in Berlin-Mitte, zu dem sie möglichst schnell gelangen möchte. Ihr virtueller Reiseassistent schlägt hierfür vor, die Strecke mit ihrem Elektroauto zu fahren. Während der Fahrt meldet ihr intelligenter Reiseassistent: Auf der Autobahn ist soeben eine Baustelle eingerichtet worden. Noch ist zwar kein Stau entstanden, aber der Reiseassistent erlaubt trotzdem schon eine intelligente Prognose: Die Überlastung der Strecke sowie mögliche Ausweichrouten würden Carlas Ankunft um etwa eine Stunde verzögern. Damit sie ihren Termin halten kann, empfiehlt der Reiseassistent, zum Bahnhof in der rund 30 Kilometer entfernten Kleinstadt zu fahren und dort den Zug nach Berlin zu nehmen. Nach Carlas Einwilligung bucht der Reiseassistent das passende Zugticket mit Sitzplatzreservierung am Fenster und in Fahrtrichtung – so wie sie es bevorzugt. Nachdem Carla an ihrem Ziel angekommen ist, meldet sie ihrem virtuellen Reiseassistenten über die Feedbackoption, wie ihr die Reise gefallen hat und ob die prognostizierte Ankunftszeit eingehalten werden konnte. Da das System mit den neu generierten Feedback-Daten stets dazulernt, entsprechen die von ihm ausgegebenen Empfehlungen Carlas Präferenzen zunehmend treffender.

Das Szenario bezieht sich auf Carla als Privatperson. Nicht betrachtet wird Carla in ihrer beruflichen Position, beispielsweise als Vorstandsvorsitzende in einem börsennotierten Unternehmen oder als Mitglied des Deutschen Bundestags. Dies ist darin begründet, dass in diesem Zusammenhang weitere IT-Sicherheitsaspekte bedeutsam werden würden, die stark vom jeweiligen Anwendungsfall abhängig sind, wie beispielsweise eine Reise nur mit Personenschützern. Das vorliegende Szenario hat jedoch den Anspruch, eher allgemeingültig und auf eine möglichst große Zahl Reisender anwendbar zu sein.

Relevanz des Umfeldszenarios

Das Szenario veranschaulicht eine fiktive Reise von Carla, die in einem Dorf in Brandenburg beginnt und in Berlin-Mitte endet. Nicht nur für Carla, sondern auch für circa 334.000 Beschäftigte, die täglich mit dem Auto nach Berlin pendeln, ist das Zurücklegen größerer Distanzen mit dem Auto Teil ihres Alltags (vgl. Bundesagentur für Arbeit 2020). Aufgrund von Streckenüberlastungen verloren sie 2019 durchschnittlich jeweils etwa 15 Minuten im Stau pro Arbeitstag.[1] Umgerechnet ergeben sich durch diesen Zeitverlust Kosten von jährlich mindestens 587 Euro pro Person.[2]

Die Streckenüberlastungen nehmen zu, weil die Deutschen im Durchschnitt immer länger zur Arbeit fahren und die Zahl der pendelnden Personen stetig steigt: Im Jahr 2000 fuhren 14,9 Millionen Arbeitnehmerinnen und Arbeitnehmer zu ihrem Arbeitsort, im Jahr 2018 waren es schon 19,3 Millionen (vgl. Bundesagentur für Arbeit 2018). Knapp 68 Prozent der deutschen Pendlerinnen und Pendler nutzen das Auto, um Entfernungen von durchschnittlich 17 Kilometern zum Arbeitsort zurückzulegen (vgl. Statistisches Bundesamt 2016).[3] Umgerechnet auf den dadurch verursachten Treibhausgas-Ausstoß ergeben sich pro pendelnde Person jährlich 609,57 Tausend vermeidbare Tonnen CO_2-Emissionen.[4]

Mit einem intelligenten Reiseassistenten könnte die Fahrt zukünftig nicht nur schneller und ressourcenschonender werden, sondern in einer multimodalen Mobilität (d. h. vor allem im urbanen und suburbanen Umfeld mit einem hohen Anteil unterschiedlicher Verkehrssysteme) auch den persönlichen Bedürfnissen besser entsprechen. Hierfür schlägt der virtuelle Reiseassistent eine intelligent geplante Route vor. So löst er mit Hilfe von Lernenden Systemen zahlreiche komplexe Analyse-, Planungs- und Entscheidungsaufgaben. Aus anonymisierten Mobilitätsdaten der Vergangenheit entwickelt er orts- und situationsspezifische Modelle. Er erlernt selbstständig Strategien, um einen Zielort möglichst nach Carlas individuellen Bedürfnissen und persönlichen Präferenzen zu erreichen. Als intermodaler Routenplaner bezieht er nicht nur die Daten des motorisierten Individualverkehrs in seine Planungen ein, sondern auch die Angebote von Mitfahrerplattformen und des öffentlichen

1 Berechnung auf Basis von 66 Stunden Stauzeit 2019 (vgl. INRIX 2020): 66 Stunden Stauzeit ergeben umgerechnet 3.960 Minuten; diese dividiert durch die Anzahl der Wochentage (Mo–Fr) pro Kalenderjahr (261 Wochentage) ergibt 15 Minuten (gerundet).
2 Berechnung auf Basis von 66 Stunden Stauzeit und des 2019 aktuellen Mindestlohns von 8,90 € pro Person (vgl. INRIX 2020).
3 Ein Rückgang der Mobilität während der COVID19-Pandemie scheint aktuell (Mai 2021) nur vorübergehend zu sein. So nähert sich die Mobilität im Februar 2021 bereits wieder dem Niveau vor der Pandemie (vgl. Statistisches Bundesamt 2021).
4 Berechnung auf Basis von 19,3 Millionen Pendelnden in Deutschland, von denen 68 Prozent mit dem Auto zur Arbeit fahren und dabei durchschnittlich jeweils 17 Kilometer an 261 Wochentagen im Jahr zurücklegen: 58 Milliarden gefahrene Kilometer, da ein gefahrener Personenkilometer durchschnittlich 147 Gramm Treibhausgas-Emissionen (CO_2, CH_4, N_2O angegeben in CO_2-Äquivalenten) verursacht; Pendelnde verursachen jährlich 8 Millionen Tonnen Treibhausgas-Emissionen (vgl. Umweltbundesamt 2021).

Nahverkehrs. Der Routenplaner unterbreitet Carla mehrere Optionen, von denen die Autofahrt zum lokalen Bahnhof in Kombination mit einer Zugfahrt nach Berlin die in dieser Situation und auch hinsichtlich ihrer Präferenzen die passendste ist.

Multimodaler Verkehr: Bietet das Mobilitätssystem mehr als eine Möglichkeit, eine bestimmte Mobilitätsanforderung zu erfüllen, so gilt das System als multimodal (Plattform Lernende Systeme 2019b, S. 6). Als multimodaler Verkehr wird die Nutzung verschiedener Verkehrsmittel für unterschiedliche Wege beschrieben (z. B. Auto in ländlichen Gebieten, ÖPNV in städtischen Gebieten). Entscheidend für die Wahl des Verkehrsmittels sind individuelle Präferenzen (siehe difu 2018).

Intermodaler Verkehr: Wenn eine Mobilitätsanforderung in Segmente unterteilt werden kann, in denen jeweils ein bestimmter Verkehrsträger verwendet wird und am Ende eines jeden Abschnitts Wechsel zwischen verschiedenen Fahrzeugen durchgeführt werden, dann gilt das System als intermodal (Plattform Lernende Systeme 2019b, S. 6). Im intermodalen Verkehr werden für einen vorgegebenen Weg unterschiedliche Verkehrsmittel so kombiniert, dass eine aus individueller Sicht optimale Lösung entsteht (z. B. mit dem eigenen Fahrrad bis zur Trambahnhaltestelle, nach dem Ausstieg aus der Trambahn mit dem Carsharing-Auto bis ans Ziel) (siehe difu 2018).

2.2 Externe und persönliche Entscheidungsfaktoren

Carlas Reise soll vom Start- bis zum Endpunkt innerhalb einer vollumfänglich integrierten Anwendung geplant, gebucht und abgerechnet werden können. Der intelligente Reiseassistent (siehe Kapitel 2.3) wird dazu eingesetzt, vor dem Hintergrund gegebener Bedingungen, die optimale Reise für Carla zu ermitteln. Die Auswahl der Mobilitätsträger soll nach den im System hinterlegten persönlichen Präferenzen, den Auswahlmöglichkeiten und Randbedingungen getroffen werden können: Zeit, Kosten, Klimafreundlichkeit, Komfort, soziale Interaktion, gegebenenfalls körperliche Beeinträchtigungen etc.

Carlas persönliche Entscheidungsfaktoren

Carlas persönliche Entscheidungsfaktoren sind zum einen multikriteriell, weil verschiedene Perspektiven mit unterschiedlichen Anforderungen und Kriterien für die weitere Optimierung der Route berücksichtigt werden – dies in Abhängigkeit zur jeweils vorliegenden Situation, wie zur (derzeitigen) körperlichen Verfasstheit oder zu persönlichen Sicherheitsbedenken. Zum anderen multimodal, da verschiedene Verkehrsmittel wie motorisierter und nicht-motorisierter Straßenverkehr, aber auch der öffentliche und private Personennahverkehr (ÖPNV) sowie der Individualtransport einbezogen werden.

Aus dem definierten Präferenzprofil und aus dem beobachteten Mobilitätsverhalten von Carla wird ihr ein vordefiniertes Stereotyp-Schema zugeordnet. Dies geschieht in der Interaktion mit digitalen Systemen mit Hilfe von Matching-Algorithmen. Dieses Präferenzprofil

enthält auch die Handlungsfreiheiten, die Carla dem System zugesteht. Mit dem definierten Stereotyp sind für die individuelle Nutzerin Carla typische Vorlieben, Ziele und Persönlichkeitsmerkmale gespeichert, die dann in die weitere algorithmische Verarbeitung eingehen (zum Beispiel im Flugzeug: tagsüber Fensterplatz, nachts bei kurzen Flügen Gangplatz; bei mehr als 45 Minuten Zeitnachteil beim ÖPNV Bevorzugung von Carsharing etc.). Weitere Präferenzen könnten beispielsweise die Sicherheit Carlas (v. a. bei nächtlichen Reisen) betreffen. Dabei werden die Profile nicht immer als solche gespeichert, sondern es werden Ad-hoc-Ableitungen (insbesondere Verhaltensvorhersagen) dynamisch und in Echtzeit aus Rohdaten (zum Beispiel „da heute ohne schweres Gepäck Nutzung eines eScooters für die letzte Meile") generiert. Da der intelligente Reiseassistent mit jeder Eingabe dazulernt, wird Carlas Profil mit der Zeit immer genauer.

In Abhängigkeit von den Auswahlmöglichkeiten steht als Ergebnis ein vollumfänglich integriertes Angebot mit geringen bis gar keinen Umsteigewiderständen aufgrund von Reisezeit, Buchungsaufwand, Komforteinbußen und Reisekosten zur Verfügung. Die Kombination mit verlässlichen, günstigen und zeiteffizienten Alternativangeboten, die Carla während der Reise von digitalen Diensten zur Reisebegleitung vorgeschlagen werden, bietet einen deutlichen Mehrwert und optimiert die gewählte Route (z. B. Informationen zu Ladesäulenstandorten oder Bezahlmöglichkeiten etc.).

Carlas Auswahlmöglichkeiten

Grundsätzlich steht Carla zur Gestaltung ihrer Reise eine Reihe von Optionen mit entsprechenden Auswahlmöglichkeiten zur Verfügung, um von A nach B zu kommen. Dazu gehören die verfügbaren Transportalternativen, auf die Carla zugreifen kann: regionale und überregionale Verkehrsmittelangebote von Bussen und Bahnen, der eigene PKW, Car- und Ridesharing-Angebote, Taxi, Scooter, Leihfahrräder bis hin zur Möglichkeit, zu Fuß zu gehen. All diese Auswahlmöglichkeiten können auch miteinander kombiniert werden, sodass in Abhängigkeit der Angebotsdifferenzierung eine Vielzahl an Optionen zur Verfügung steht, zwischen denen sich Carla je nach vorliegender Situation und persönlicher Präferenz entscheiden kann. In der Regel entsteht so ein Mix an Entscheidungsvarianten, die mit Carlas hinterlegtem Präferenzprofil korrespondieren. Gerade hierbei können KI-gestützte Vorschlagslogiken zum Einsatz kommen, die zu Carlas Präferenzen passende Entscheidungsalternativen für Carlas Reiseassistenz berechnen.

Kontextfaktoren

Mögliche behördliche Einschränkungen infolge von Katastrophenlagen (Großschadensereignisse), pandemische Erkrankungswellen sowie mögliche Einreise-Verbote stellen für die Reisebuchung besondere sensible Randbedingungen dar. Dazu zählen auch die aktuelle Wetterlage, die Tageszeit der Reise sowie mögliche Naturkatastrophen. Verfügbare und regional spezifische Daten werden entsprechend berücksichtigt. Des Weiteren werden sowohl Angaben über den Zeitpunkt der Buchung und Reise als auch die Buchungs- bzw. Reisefrequenz mit einbezogen. So entstehen durch KI-Systeme laufend neu gelernte Informationen, für deren Schutz zu sorgen ist und deren Sicherheit gewährleistet werden muss

(siehe auch Kapitel 3.2). So lernt der intelligente Reiseassistent im Betrieb etwas über Carlas Verhalten und mögliche Bedingungsfaktoren. Ein Risiko besteht vor allem darin, dass diese Daten unzureichend pseudonymisiert oder anonymisiert sind und mit Carla verknüpft werden können.

2.3 Wie der intelligente Reiseassistent funktioniert

Wie bereits dargestellt ist das Ziel des intelligenten Reiseassistenten, vor dem Hintergrund von Carlas Präferenzen, Auswahlmöglichkeiten und Kontextfaktoren, die optimale Reise zu ermitteln. Hierbei kann der Reiseassistent jederzeit vor, während und nach einer Reise eingesetzt werden. Von seiner Funktionsweise her basiert er zudem auf unterschiedlichen technischen Lösungen (Mobilitätsplattformen, siehe Kapitel 2.3.2).

2.3.1 Drei mögliche Einsatzszenarien

Der Reiseassistent kann in unterschiedlichen Einsatzszenarien verwendet werden: Er kann sowohl für die Reiseplanung vor Reiseantritt als auch als Assistenz während der Reise genutzt werden. Zu guter Letzt kann auch Feedback zur Zufriedenheit mit der Reisegestaltung am Ende der Reise an den Reiseassistenten übermittelt werden.

Reiseplanung vor Reiseantritt

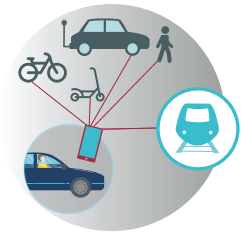
Vor Reiseantritt wird anhand Carlas persönlicher Präferenzen eine optimale Reise geplant.

Dabei werden Reiseoptionen und Eigenschaften aller verfügbaren Modalitäten wie Privat-PKW, Car- und Ridesharing, öffentlicher Straßen- und Schienenverkehr, Schiff- und Luftfahrt, Optionen als Fußgängerinnen und Fußgänger, Radfahrerinnen und Radfahrer oder weiterer Mikromobilität sowie deren Kombinationen berücksichtigt (siehe Kapitel 2.2). Der Suchraum kann daher sehr groß sowie mit zahlreichen Unsicherheiten behaftet sein und so unzähligen bekannten wie unbekannten Einflussgrößen unterliegen. Konkret: Während das Nutzerprofil dem Reiseassistenten bekannt ist, können beispielsweise die Wetterlage oder temporäre Baustellen als unbekannte Einflussgrößen die Suchanfrage bzw. die Durchführung der Reise beeinflussen.

Die Reiseplanung wird in der Regel in einer Umgebung mit guter Ressourcenverfügbarkeit, beispielsweise in einer Smart-Home-Umgebung mit einer stabilen Internetverbindung, durchgeführt und ist wenig zeitkritisch. In dieser Phase erfolgt also eine umfangreiche Optimierung aller relevanten Optionen und nach den persönlichen Präferenzen und in direkter Interaktion mit der oder dem Nutzenden.

Der Start der Reiseplanung muss nicht von Carla getriggert werden, sondern kann sogar automatisiert ausreichend früh erfolgen, wenn der Reiseassistent etwa am Kalender oder an Carlas Bewegungsmuster erkennt, dass vermutlich bald eine Reise ansteht. Hieraus können umgekehrt bereits erste individuelle Reisemuster von Carla entstehen, die geschützt bleiben müssen.

Reiseänderungsvorschlag/Alternativroute während der Reise



Unmittelbar vor Reiseantritt und während der Reise überprüft der Reiseassistent kontinuierlich die Reiseplanungsdaten sowie den Reisefortschritt daraufhin, ob die aktuelle Reiseplanung weiterhin (optimal) durchführbar ist. Ein länger dauerndes Sportereignis, ein Unfall oder eine unvorhergesehene Wetteränderung könnten nämlich die Verkehrslage und die Mobilitätsoptionen stark beeinflussen. Aber auch Carla selbst kann Alternativen notwendig machen, wenn sie sich anders verhält als vorgesehen oder angenommen. Die Situation während der Reise ist ähnlich wie vor Reiseantritt, allerdings ist die Berechnung von Optionen jetzt eher zeitkritisch und unterliegt unter Umständen stärkeren Ressourcenbeschränkungen aufgrund mangelnder Konnektivität. Der verfügbare Suchraum ist zudem deutlich eingeengter.

Feedback nach der Reise zur Verbesserung zukünftiger Vorschläge

Der Reiseassistent kann durch Feedbackfunktionen in einen direkten und interaktiven Kontakt mit dem oder der Reisenden treten und so kontinuierlich mehr über persönliche Präferenzen lernen. Gleichzeitig kann er ständig dazulernen, um Mobilitätsoptionen sowie deren Passung auf jede ihn benutzende Person möglichst gut vorherzusagen und auszuwählen. Daher ergibt es Sinn, auch nach der Reise die oder den Nutzenden interaktiv einzubinden, um die jeweiligen Präferenzen besser bewerten zu können. Dieses Feedback erfolgt entweder durch explizite Eingaben in Abfragen des intelligenten Reiseassistenten oder durch die Auswertung anderer Korrespondenz über die Reise. Das System kann vor allem aus der Kombination von möglichst vielen Rückmeldungen von verschiedenen Nutzenden dazulernen. Mögliche Lerneffekte können beispielsweise anhand einer allgemeinen Reisebewertung bei bekannten Eigenschaften der Reise die Nutzerpräferenzen betreffen – oder umgekehrt, bei bekannten Nutzerpräferenzen, die Eigenschaften der Reiseabschnitte betreffen. Hierbei können auch Veränderungen von Reiseeigenschaften und Nutzerpräferenzen betrachtet und wenn möglich vorhergesagt werden. Ebenso wie bei der Reiseplanung können auch hier Reisemuster und Profil der Reisenden verfeinert werden, die geschützt werden müssen.

2.3.2 Wie die Mobilitätsplattform dahinter funktioniert

Bei einer nahtlosen intermodalen Vernetzung verschiedener Verkehrsträger in Städten und Regionen spielen sichere digitale Mobilitätsplattformen eine Schlüsselrolle. Sie sind die technische Lösung für intelligente Reiseassistenten zum Auffinden der besten Mobilitätsdienste.

Der intelligente Reiseassistent gehört zur Mobilitätsplattform. Die Mobilitätsplattform für den intelligenten Reiseassistenten selbst hält keine Daten zentral vor. Stattdessen ist sie Teil einer Systemarchitektur, über die mehrere Datenhalter ihre Daten freiwillig miteinander vernetzen. Datenhalter sind Mobilitätsbetreiber, aber auch Verkehrsunternehmen und Infrastrukturbetreiber sowie öffentliche Stellen wie beispielsweise Verkehrsleitstellen und

der Deutsche Wetterdienst. Alle Akteure können dieselbe Plattform nutzen. So können weitere Datenhalter mit nützlichen Datensätzen einfach angebunden werden (siehe Erklärkasten). Beispielhaft für eine solche Mobilitätsplattform wäre etwa der Datenraum Mobilität, der als Exchange-Plattform einen vertrauenswürdigen und dezentralen Datenaustausch ermöglicht.

Den wesentlichen rechtlichen Rahmen für die verpflichtende öffentliche Bereitstellung mobilitätsrelevanter Daten bilden die Richtlinie 2010/40/EU (IVS-Richtlinie) und die daraus abgeleiteten delegierten Rechtsakte (siehe Erklärkasten). Mit der verkehrsträgerübergreifenden Bereitstellung und Nutzbarmachung aktueller Mobilitätsdaten schafft der Gesetzgeber ein rechtliches Gut, um die Entwicklung datenbasierter, multimodaler Mobilitätsdienste weiter voranzutreiben. Dieser Ansatz ist sowohl aus Sicht des Umwelt- und Klimaschutzes als auch mit Blick auf die Daseinsvorsorge zentral.

Anbindung weiterer Datenhalter an die Mobilitätsplattform

Weitere Datenhalter mit Datensätzen, die zur Beantwortung von Carlas Anfrage nützlich sind (wie Karten- und Wetterdienste), können angebunden werden. Eine rasche technische Integration verschiedener Mobilitätsangebote mit unterschiedlichen Legacy-Systemen[5] im intelligenten Reiseassistenten kann über „Deep Integration“[6] erfolgen. Deep Integration ist hier das „Übersetzungstool“ zwischen verschiedenen Mobilitätsanbietern und ermöglicht Carla, ihren intelligenten Reiseassistenten als Vermittler zu nutzen, über den neben der Routenplanung auch die Buchung und Abrechnung der Reise in einer App-Anwendung abgebildet werden kann.

Regulative Vorgaben zur verpflichtenden öffentlichen Bereitstellung mobilitätsrelevanter Daten

- **EU-Richtlinie 2010/40/EU:** Entsprechend dieser EU-Richtlinie sollen über den von der Bundesanstalt für Straßenwesen (kurz: BASt) betriebenen nationalen Zugangspunkt „Mobilitäts Daten Markplatz“ (kurz: MDM) Informationen verpflichtend geteilt werden. Hierzu zählen Informationen zu Parkplätzen, Baustellendaten, multimodalen Reisediensten, Messwerten von Verkehrs- und Umfelddetektoren und daraus abgeleiteten Daten über die Verkehrslage, Reisezeiten etc. sowie zur Verkehrssicherheit (Gefahren- und Ereignismeldungen) und statischen Straßen-Netzdaten. Bis Ende 2021 wird der MDM mit dem Open-Daten-Portal mCloud des Bundesverkehrsministeriums zusammengeführt.
- **Mobilitätsdatenverordnung:** Die Novelle des Personenbeförderungsrechts strebt zudem eine verpflichtende Bereitstellung von Daten durch Anbieter von Personenbeförderungsdiensten in Form einer Mobilitätsdatenverordnung an. Diese

5 Unter einem Legacy-System wird in der IT eine alte, über die Jahre etablierte Anwendung im Bereich Firmen- oder Verwaltungssoftware verstanden.

6 Deep Integration beschreibt einen ganzheitlichen Designansatz. Er stellt sowohl die Kombination und Kommunikation unterschiedlicher Subsysteme, Komponenten und Anwendungen untereinander als auch durch deren Vernetzung innerhalb eines Gesamtsystems sicher.

Verordnung sollte im Sinne der Datensouveränität dafür Sorge tragen, dass jeder geteilte Datensatz einem konkreten Anwendungsfall unterliegt. Perspektivisch sollte diese Verordnung auch für Anbieter außerhalb des Personenbeförderungsrechts gelten (wie Anbieter vom ÖPNV, Carsharing, Bikesharing, eScooter-Anbieter etc.).

- **Data Governance Act der EU (2020):** Die EU-Vorschrift für Daten-Governance bietet darüber hinaus einen regulatorischen Rahmen für den Umgang mit geschützten Daten, die im Besitz öffentlicher Stellen sind. Für Plattformbetreiber von intelligenten Reiseassistenten könnte dies relevant sein, wenn Mobilitätsanbieter des ÖPNV teilnehmen.

Der intelligente Reiseassistent verwendet, um Carlas Routenanfrage optimal zu beantworten, Informationen von Datenhaltern, beispielsweise Karten- oder Wetterdienste. Diese Informationen verbleiben bei den jeweiligen Datenhaltern und werden nicht im intelligenten Reiseassistenten gespeichert. Somit wird die Grundlage für die Beteiligung der Mobilitätsbetreiber sowie der Endkundinnen und -kunden in einem kreativen Vertrauensökosystem geschaffen, das sich stetig weiterentwickeln kann.

Ein Schlüsselfaktor für die Mobilitätsplattform ist die vertrauenswürdige Identifizierung der Mobilitätsanbieter. Bestehende Regularien wie die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) sollten hierfür berücksichtigt werden. Neben eindeutigen Zugangsrechten zur Plattform braucht Carla auch Gewissheit über die bestimmungsgemäße Verwendung ihrer Daten. Datensparsamkeit kann im Konflikt mit funktionalen Anforderungen stehen, da die vorgeschlagenen Reiserouten für die oder den Nutzenden natürlich maximal geeignet sein sollten: Mittels KI ließen sich aus personifizierten Bewegungsprofilen nützliche Informationen extrahieren. Da allerdings auch anonymisierte Bewegungsprofile verwertbare Informationen enthalten können, ist fraglich, ob personenbezogene Bewegungsprofile notwendig sind. Es ist wichtig, diese Aspekte bereits von Anfang an im Auge zu behalten, abzuwägen, die Gesetzeskonformität zu prüfen und die erzielten Kompromisse geeignet technisch umzusetzen (privacy by design).

Die Einhaltung der technischen und vertragsrechtlichen Regeln zur Nutzung der Mobilitätsplattform sollen durch unabhängige Zertifizierung und Audits auf Basis bestehender Standards und Technologien kontinuierlich geprüft werden. Wie Geschäftsmodelle hinter der Plattform aussehen könnten und wer über welche Zuständigkeiten verfügen könnte, wird in Kapitel 4.3 ausgeführt.

Im Hintergrund: Vermeidung von fehlerhaftem Schwarmverhalten

Nicht nur Carlas Anfragen gehen dem intelligenten Reiseassistenten zu, sondern zeitgleich hunderte, gar tausende weitere Reiseanfragen von Dritten. Aus dieser Flut von Anfragen muss das Reiseassistenzsystem in der Lage sein, die wahrscheinlichsten Routen und Transportmittel pro Anfragenden zu berechnen, ohne dass zu diesem Zeitpunkt bereits eine Entscheidung, eine Reservierung und eine Buchung erfolgt ist. Aus der Gesamtheit der

berechneten und zuvor durchgeführten Routen, inklusive der ermittelten Transportzeitfenster, ist das Schwarmverhalten zum Beispiel für ein Ballungsgebiet zu ermitteln. Als Ergebnis können mögliche Engpässe vorausgesagt und Alternativen für einen prozentualen Anteil der Reisenden angeboten werden. Konkret am Beispiel verdeutlicht: Es sind Zugschienen blockiert und deshalb kann ein Zug nicht weiterfahren. In dieser Situation empfiehlt der intelligente Reiseassistent nicht allen 250 Reisenden, am nächsten Bahnhof auf ein Carsharing-Angebot umzusteigen, sondern die Anzahl der Carsharing-Empfehlungen entspricht der Anzahl der vorhandenen Carsharing-Fahrzeuge an diesem Bahnhof. Falls passend und gewünscht, werden auch Mitfahrmöglichkeiten vorgeschlagen. Für die restlichen Reisenden wird eine andere Empfehlung ausgegeben. Dies gilt auch für Ausweichrouten bei Unfällen auf der Autobahn. Der intelligente Reiseassistent berechnet hier eine mögliche Überlastung einer Ausweichroute. Deshalb werden auch weitere Ausweichrouten empfohlen. Positiv an der Systemarchitektur ist der als „Schwarmintelligenz" bezeichnete mathematische Algorithmus, der die Widerstandsfähigkeit gegen Ausfälle durch dynamische Transportkapazitätsberechnungen erhöhen kann. Größter Nachteil sind mögliche Botnetzangriffe, die das Gesamtsystem leicht zu einem fehlerhaften Schwarmverhalten führen können oder sogar zum kompletten Ausfall. Daher sind entsprechende Gegenmaßnahmen zu treffen. Welchen Reisenden Alternativen angeboten werden und welche Alternativen – zum Beispiel im Vergleich mit der ursprünglichen Route eine längere und/oder teurere oder aufwendigere Route – für diese ausgesucht werden, ist eine Designfrage, die in das System implementiert werden kann. Ob die KI hierbei nach dem „First-come-first-serve-Prinzip" oder nach anderen Fairnessgesichtspunkten, wie beispielsweise der körperlichen Verfassung der Nutzenden, entscheidet, ist aktuell noch offen.

KI-Algorithmen mit **Schwarmintelligenz** gibt es seit vielen Jahren. Schwarmintelligenz (auch kollektive Intelligenz genannt) beschreibt das Phänomen, dass mehrere Individuen durch Zusammenarbeit intelligente Entscheidungen treffen können. Einige KI-Algorithmen mit Schwarmintelligenz sind modellhaft dem Schwarmverhalten aus der Tierwelt nachgebildet. Bekannt ist der Ameisenalgorithmus. Dieser ahmt mit einem stark vereinfachten mathematischen Verfahren den Weg nach, mit dem Ameisenkolonien den besten Weg zur Futterquelle finden: So scheiden Ameisen auf dem Weg zur Futterquelle einen Duftstoff (Pheromone) aus. Die Ameisen auf dem kürzeren Weg sind schneller und können deshalb öfter zwischen Futterquelle und Ameisenhaufen hin- und herlaufen. Dies führt zu einer höheren Pheromon-Konzentration auf der kürzeren Route. Die nachfolgenden Ameisen wählen eher den Weg mit einer höheren Pheromonkonzentration – eine Ameisenstraße entsteht.

3 Daten im Szenario

Im Szenario „Carlas Reise“ fallen an vielen unterschiedlichen Stellen Daten an, die notwendig sind, um die erforderlichen Mobilitätsdaten zu generieren. Daher wird das Szenario im Weiteren auf seine technischen Komponenten hin betrachtet. Hierfür wird das gesamte Mobilitätssystem mit seinen vielen Reisenden, Reisen, Mobilitätsbetreibern und natürlich auch intelligenten Reiseassistenten analysiert.

3.1 Reisestationen der Daten

Ein Überblick über die Datenwege wird im Folgenden abgebildet. Die Datenflüsse sind in einem vereinfachten Modell eines intelligenten Reiseassistenten dargestellt. Die intelligenten Reiseassistenten der Nutzenden geben Daten und Anfragen verschlüsselt an die Mobilitätsanbieter weiter. Die KI, das Lernen und die dafür notwendigen und daraus gelernten Daten liegen im System des intelligenten Reiseassistenten.

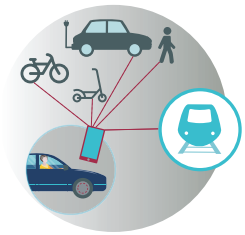
Planung/Buchung der Reise

Im ersten Schritt übermitteln die Reisenden über die App an ihren intelligenten Reiseassistenten ihre Präferenzen und konkreten Anfragen.

In einem zweiten Schritt greift der angefragte intelligente Reiseassistent auf Daten der unterschiedlichen Datenhalter – Mobilitätsbetreiber, Verkehrsleitstellen etc. – zu.

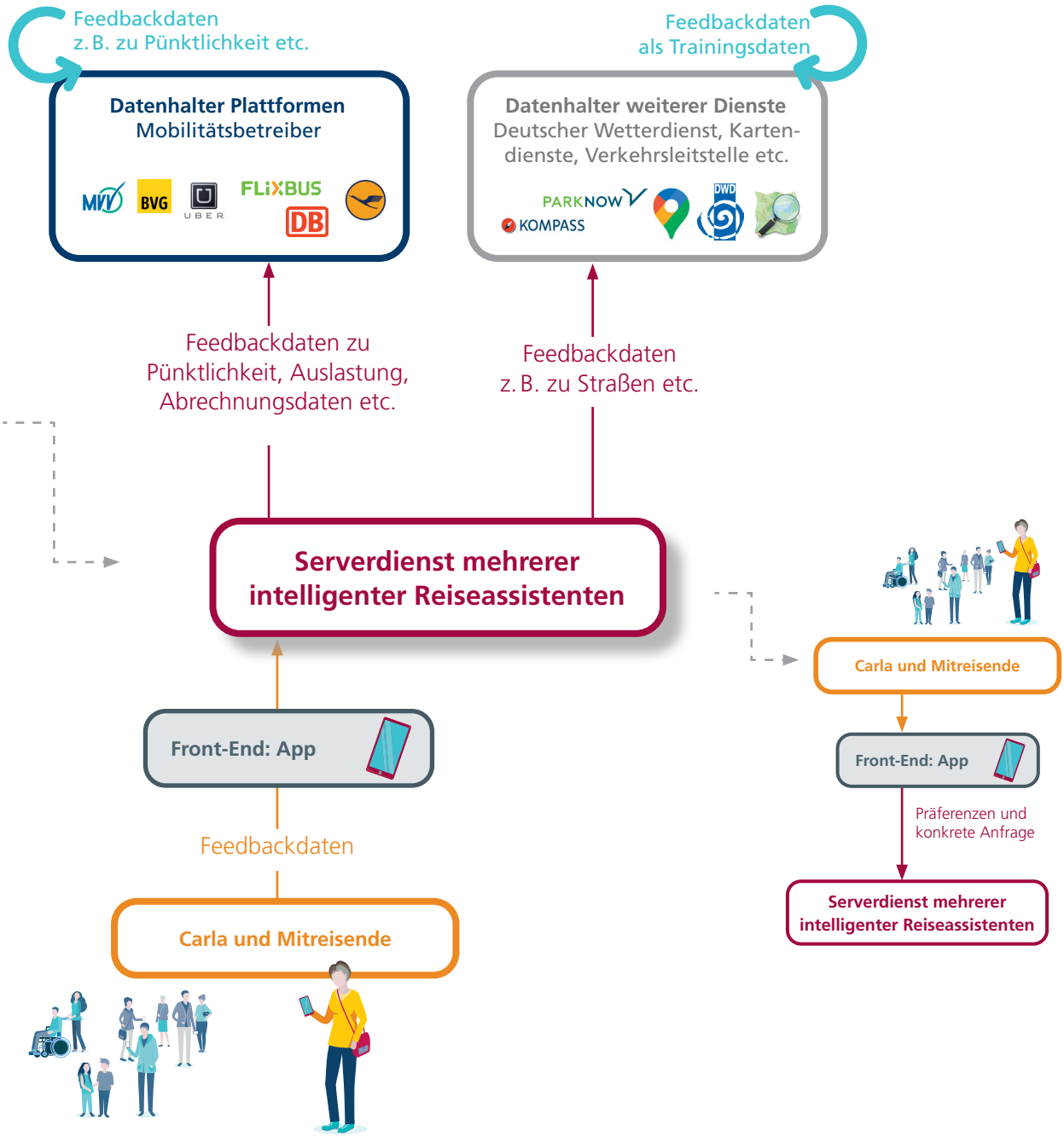
Aus den unterschiedlichen Informationen berechnet der intelligente Reiseassistent dann die optimale Route und übermittelt den Anfragenden unterschiedliche Optionen inklusive der Abrechnungs- oder Bezahldaten über die App. Die Anfragenden wählen über die App die bevorzugten Optionen bzw. äußern Änderungswünsche und übermitteln personenbezogene Daten zur Buchung: Schritt 3.

Zur Buchung gibt der intelligente Reiseassistent wiederum Buchungsdaten an die Mobilitätsbetreiber weiter: Schritt 4.

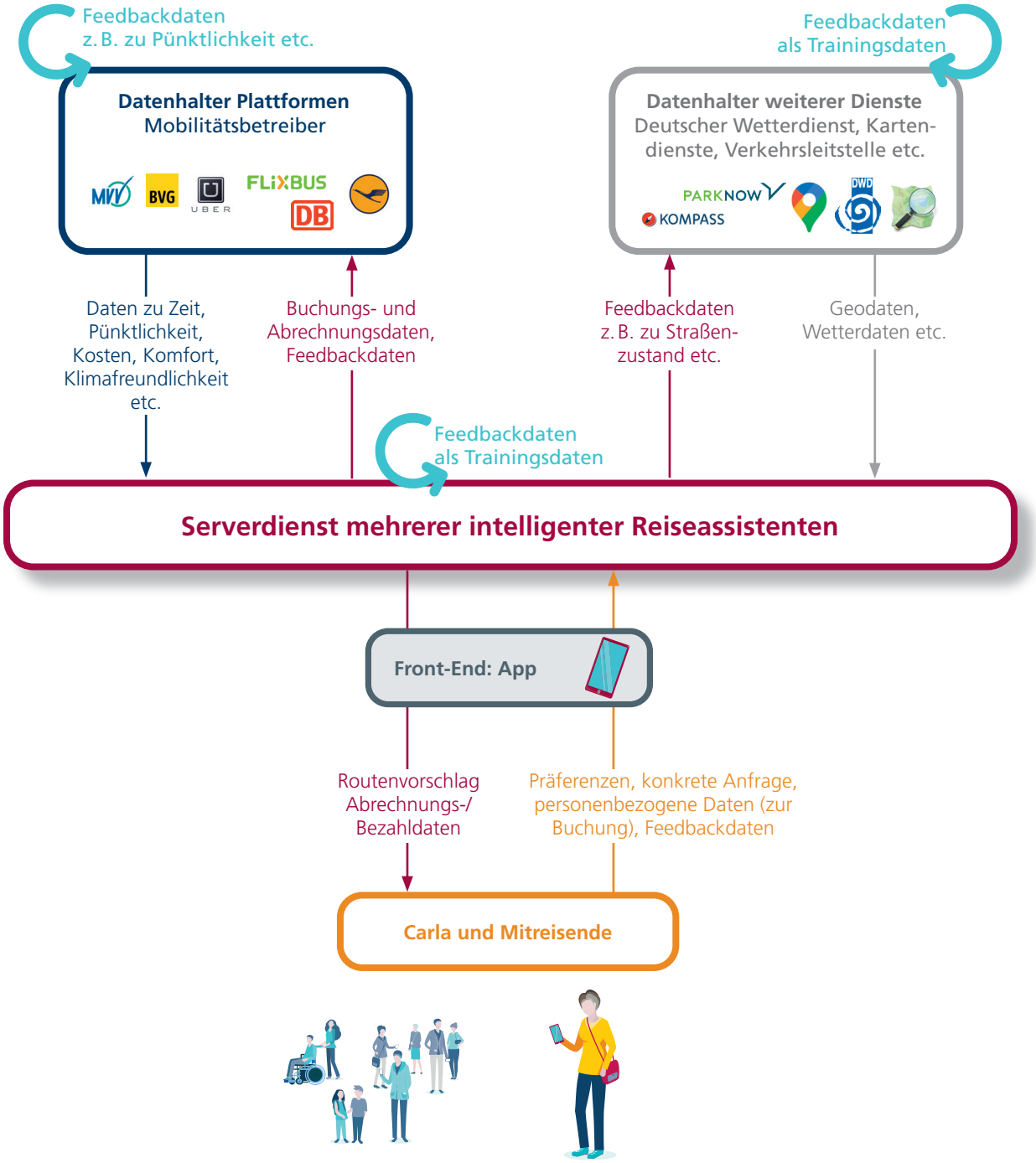


Alternativroute während der Reise
Treten während der Reise Komplikationen auf, die eine Reiseplanänderung erforderlich machen, laufen die Schritte 1–4 erneut ab.

Feedback nach der Reise
Nach der Reise übermitteln die Reisenden ihr Feedback über die App an ihren intelligenten Reiseassistenten, der diese Informationen an die Datenhalter weitergibt. Die Feedbackdaten fungieren dort – wie auch im intelligenten Reiseassistenten – als Trainingsdaten: Schritt 5 (siehe Seite 19).


Feedbackdaten
z. B. zu Pünktlichkeit etc.
Feedbackdaten
als Trainingsdaten
Datenhalter Plattformen
Mobilitätsbetreiber
MVV
BVG
UBER
FLIXBUS
DB
Datenhalter weiterer Dienste
Deutscher Wetterdienst, Karten-
dienste, Verkehrsleitstelle etc.
PARKNOW
KOMPASS
DWD
Feedbackdaten zu
Pünktlichkeit, Auslastung,
Abrechnungsdaten etc.
Feedbackdaten
z. B. zu Straßen etc.
Serverdienst mehrerer
intelligenter Reiseassistenten
Front-End: App
Feedbackdaten
Carla und Mitreisende
Carla und Mitreisende
Front-End: App
Präferenzen und
konkrete Anfrage
Serverdienst mehrerer
intelligenter Reiseassistenten

Der gesamte Datenweg sowie alle beteiligten Akteure im Mobilitätsdatenökosystem im Überblick:



3.2 Wo entstehen welche Daten und welche Datenarten?

Daten der Reisenden und deren Personenbezogenheit

Hinsichtlich der Daten im Datenpool des Serverdienstes ist zuerst zwischen personenbezogenen Daten und nicht-personenbezogenen Daten zu unterscheiden (siehe Infobox). Während beispielsweise eine Fahrplanauskunft ohne personenbezogene Daten durchführbar wäre, kann schon eine einfache Servicefunktion einen Personenbezug herstellen. Dies geschieht sowohl über das hinterlegte Präferenz- und Planungs-Profil vor der Reisebuchung inklusive Start- und Zieladresse, Datum, Wunsch-Ankunftszeit etc. als auch über die voraussichtliche Engpassmeldung (aus der Schwarmintelligenz). Auch das Änderungsprofil während der Reise sowie das Rückmelde-Profil tragen dazu bei. Allein die einfache Abfrage des Standortes etwa, um Mobilitätsangebote rund um diesen Standort abzufragen, fällt bereits unter die Begriffsbestimmung des Datenschutzrechtes. Personenbezogene Daten sind auch erforderlich, um Transaktionen abzuwickeln. Damit fallen intelligente Reiseassistenten regelmäßig in den Anwendungsbereich des Datenschutzrechtes und erfordern einen entsprechenden Erlaubnistatbestand (vgl. Europäische Union 2018a). Dieser wird in den allermeisten Fällen über eine informierte Einwilligung hergestellt, die im Rahmen eines Registrierungsprozesses abgefragt wird (vgl. BMJV 2018b; Europäische Union 2018b). Dieser Registrierungsprozess erfasst meist auch alle erforderlichen Daten für Transaktionen. Dazu zählen Buchung, Reservierung, Stornierung und Bezahlung.

Personenbezogene Daten
Unter personenbezogenen Daten werden „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen" (vgl. BMJV 2018a), verstanden. Beispiel: die Angabe des Namens „Carla Fuchs", die Angabe des Geburtsdatums oder auch eine IP-Adresse.

Personenbeziehbare Daten
Diese Daten können einer natürlichen Person zugeordnet werden. Beispiel: Bewohner im Einfamilienhaus in der Hauptstraße 1 in Werder (Havel). Im Falle von Carlas Anfrage können drei Informationsklassen ein „Profil" ergeben: a) Carlas Präferenz, b) Carlas bevorzugte Auswahl und c) Carlas konkrete Routenabfrage. Dieses Profil könnte eine anonym erscheinende Anfrage zu einem personenbeziehbaren Datensatz weiterentwickeln lassen.

Anonymisierte Daten
Die betroffene Person kann nicht oder nur mit unverhältnismäßigem Aufwand identifiziert werden. Beispiel: Bewohner in Werder (Havel), im Besitz eines gültigen Führerscheins (siehe auch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2020).

Verkehrssystemspezifische Planungsdaten

Grundlage für alle intelligenten Reiseassistenten sind verkehrssystemspezifische Planungsdaten, die sowohl für die Reiseplanung als auch für Reiseanpassungen während der Reise erforderlich sind. Vor allem Geodaten[7] sind hier vielfach die hauptsächliche Angebotsgrundlage. Dazu zählen u.a. Straßen- und Schienenkarten sowie sonstige relevante Infrastrukturdaten. Bei der Integration öffentlicher Verkehrsmittel sind für die Reiseplanung Fahrplandaten essenziell. Für Reservierungen und Buchungen sind zudem Daten zur Verfügbarkeit von Reisemitteln zu einem bestimmten Zeitpunkt der Reiseplanung erforderlich.

Um über die Planungsfunktion hinaus ein intelligentes, intermodales Routing zu ermöglichen, sind Echtzeitdaten unerlässlich. Dazu zählen Daten zum Verkehrsgeschehen wie beispielsweise Staus, Baustellen, Umleitungen oder Unfälle, aber auch zur Verfügbarkeit von Sharing-Verkehrsmitteln oder auch Mitfahrgelegenheiten. Hierbei ist zwischen statischen und dynamischen Daten zu unterscheiden. Dabei gilt grundsätzlich, je statischer die Linienführung der Fortbewegungsmittel (z. B. Schienenverkehr), desto kleiner die Anzahl möglicher dynamischer Datenpunkte. Umgekehrt gilt, je offener ein Verkehrssystem, desto höher die Anzahl möglicher dynamischer Datenpunkte. So stellt das Verkehrssystem „Straße" in dieser Hinsicht wohl die höchste Komplexität dar. Dies betrifft zum einen die Anzahl der Verkehrsteilnehmenden, die sich nicht zwingend entlang einer vorab festgelegten Linie bewegen, als auch die Anzahl der dabei zum Einsatz kommenden individuellen (Autos, Krafträder, LKW, Fahrräder etc.) sowie kollektiven Verkehrsmittel (Busse des ÖPNV, Sammeltaxen etc.).

Daten der Reisenden, Planungsdaten und deren Statik oder Dynamik

Es ist notwendig, Daten hinsichtlich ihrer statischen oder dynamischen Natur zu unterscheiden (siehe Abbildung 1). Statische Daten (sogenannte Stammdaten) sind Daten, die persistent sind, das heißt immer gleich und unveränderlich unabhängig vom Zeitpunkt. Sie sind Voraussetzung für das Anmieten und Buchen bestimmter Verkehrsmittel, genauer gesagt zur Feststellung der Identität der oder des Nutzenden. Dynamische Daten (sogenannte Transaktions- oder Bewegungsdaten) sind Daten, die regelmäßig aktualisiert werden. Dies ist abhängig davon, ob und wann neue Informationen zur Verfügung stehen.

Abbildung 1 gibt einen Überblick, welche Daten im intelligent vernetzten Mobilitätsraum als dynamische Daten im engeren Sinne und welche Daten als statische Daten klassifiziert werden. Die Tabellen 1 und 2 erheben hierbei keinerlei Anspruch auf Vollständigkeit, enthalten aber ein breites Spektrum an Daten, um die Reisen von Reisenden so intelligent und vernetzt wie möglich abzubilden.

7 Die Deutsche Bahn stellt zum Beispiel umfangreiche Geo-Daten öffentlich zur Verfügung (vgl. Deutsche Bahn 2021).

Abbildung 1: Überblick über Datenarten

Eine Schlüsselfunktion für die Realisierung eines intelligent vernetzten Mobilitätsraums haben zum einen die Echtzeit-Daten zur gebuchten Strecke, zur Reisebegleitung und zu deren Beeinflussung und zum anderen die Angaben zu den individuellen Reisepräferenzen der oder des Reisenden. Mit einer zunehmenden Anzahl von Reisen liegen immer mehr Daten vor. Damit können sowohl die Echtzeit-Daten als auch die Reisepräferenzen deutlich verfeinert werden, sodass der intelligente Reiseassistent bei der Ermittlung der optimalen Reise noch besser unterstützen kann.

Je genauer die Eingabedaten von Carla sind, desto schneller lässt sich ein individuelles Profil ihrer Person und damit der Reisenden erstellen. Dieses individuelle Profil könnte im nächsten Schritt von Angreifern missbraucht werden (siehe Kapitel 4.1).

Daten in der Plattform/dem intelligenten Reiseassistenten

Der intelligente Reiseassistent basiert auf verschiedenen Plattformen. Die Art der Daten und somit auch das Level an benötigter IT-Sicherheit ist auch von der Art der Plattform abhängig (siehe Abbildung 2).

Abbildung 2: Zusammenhang zwischen Art der Plattform und Art der Daten

Informationsplattform

Bei einer reinen Informationsplattform fallen in der Regel keine personenbezogenen Daten an; in Ausnahmefällen anonymisierte Daten der oder des Reisenden. Weitere Akteure dieser Plattformart stellen nur allgemeine Daten bereit. Ein Beispiel hierfür sind Busfahrpläne, die online abgebildet und aufgerufen werden, egal an welcher Haltestelle man auf der Linie einsteigt. Alle Daten sind öffentlich verfügbar und müssen daher nicht weiter geschützt werden.

Planungsplattform

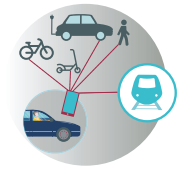
Eine Planungsplattform hingegen befindet sich in einer „Grauzone". Hier fallen im intelligenten Reiseassistenten im ersten Schritt nur anonymisierte Daten der oder des Reisenden an – in einem zweiten Schritt können aus diesen anonymisierten Daten möglicherweise aber personenbeziehbare Daten abgeleitet werden und letztlich damit ein Profil. Deshalb ist bereits bei einer Planungsplattform der Aspekt der IT-Sicherheit sehr wichtig. Dazu zählt zum Beispiel die Dateneinstufung als schutzwürdig, wenn eine genaue Abfahrts- und/oder Zieladresse beim Reiseassistenzsystem angegeben wird.

Schutzwürdig eingestufte Daten sollten,…

- wenn ein mögliches Reiseprofil ableitbar ist, nur verschlüsselt zwischen dem intelligenten Reiseassistenten und den angeschlossenen Dienstleistern ausgetauscht werden.
- wenn darin personenbezogene oder personenbeziehbare Daten enthalten sind, nicht an die angeschlossenen Dienstleister übermittelt werden.

Tabelle 1 gibt einen Überblick über die Daten im intelligenten Reiseassistenten der oder des Reisenden im Fall einer Planungsplattform.

Tabelle 1: Datenübersicht zum intelligenten Reiseassistenten (RA) als Lupenfunktion für die Planungsplattform

Anlass	Carlas Daten im RA	Daten im RA, bezogen auf Carlas Anfrage	Daten im RA von Dritten, durch RA angefragt
Erst-Registrierung	• Name, Vorname • allg. Präferenzen	• keine	• keine
Reiseplanung/Anfrage vor Reiseantritt 	• Datum, gewünschte Ankunftszeit • Start-/Ziel-Adresse • Konkrete Reise-Präferenz	• Auswahl Mobilitäts-Anbieter (Filter = Präferenz-Daten) • Berechnung möglicher Engpässe (aus Schwarmanalyse) • Mindestens drei Routenangebote	• Daten-Anfrage Mobilitätsanbieter 1 bis N (ohne Namensnennung) • Wetterdienst • Verkehrsinformation öffentl. Raum • Verkehrsinformation der Mobilitätsanbieter • Besonderheiten (z. B. Reisebeschränkung)
Reiseänderung während der Reise 	• Reisestatus melden inkl. momentanes Verkehrsmittel, Ort	• Auswahl Mobilitäts-Anbieter (Filter = verbleibende Alternativen)	• Daten-Anfrage Mobilitätsanbieter 1 bis (N-1) • Verkehrsinformation öffentl. Raum • Verkehrsinformation der Mobilitätsanbieter • Besonderheiten (z. B. Reisebeschränkung)
Feedback 	• Zufriedenheit • Komfort • Pünktlichkeit	• Scoring der Mobilitätsanbieter	Pünktlichkeit alternativer Mobilitätsanbieter für • Reise-Tag, • Start-/Zieladresse • vorgegebene Ankunfts-Uhrzeit

Buchungsplattform

Bei einer Buchungsplattform fallen zusätzlich zu den in Tabelle 1 dargestellten Daten weitere personenbezogene Daten der oder des Reisenden an, da ohne diese keine Buchung, Bestellung oder Reservierung vorgenommen werden kann. Ein Beispiel dafür wäre das Onlineportal der Deutschen Bahn – in diesem Onlineportal können Zugverbindungen gebucht oder Sitzplätze reserviert werden.

Tabelle 2 gibt einen Überblick über die Daten im intelligenten Reiseassistenten der oder des Reisenden im Fall einer Buchungsplattform.

Tabelle 2: Datenübersicht zum intelligenten Reiseassistenten (RA) als Lupenfunktion für die Buchungsplattform

Anlass	Carlas Daten im RA	Daten im RA, bezogen auf Carlas Anfrage	Daten im RA von Dritten, durch RA angefragt
Buchung/ Reservierung  	• Name/Vorname • Bankverbindung • Kreditkarten-Nummer • Smartphone-App • Bonus-Karte /Voucher etc.	• Bankverbindung • Kreditkarten-Nummer • Smartphone-App • Bonus-Karte/ Voucher etc.	Weitergabe von • Bankverbindung • Kreditkarten-Nummer • Smartphone-App • Bonus-Karte/Voucher der Mobilitätsanbieter

Buchungsplattformen sind hinsichtlich möglicher IT-Sicherheitsprobleme kritisch zu betrachten. Kriminelle können beispielsweise versuchen, die Anfragedaten zu nutzen, um um die oder den Anfragenden eine gefälschte Buchungsplattform anzuzeigen, um so Finanztransaktionen umzuleiten. Die optischen Unterschiede zwischen einer Original- und einer nachgemachten Webseite einer Buchungsplattform können so gering sein, dass sie nicht erkannt werden. Dies trifft besonders dann zu, wenn die oder der Nutzende dem System einen großen Handlungsspielraum vorgegeben hat (siehe auch Kapitel 2.2) oder durch kurzfristige Umbuchungsmaßnahmen den Reisenden kaum Zeit für eine gewissenhafte Überprüfung bleibt. Dieses Risiko könnte durch die Einbindung von treuhändischen Instanzen, z. B. PayPal, oder die Anomaliedetektion durch KI-Systeme gelöst werden.

Darüber hinaus können unseriöse Anbieter versuchen, sich als neue Partner an die Mobilitätsplattform anzuschließen, um Buchungsdaten der Nutzenden abzugreifen. Diesem Bestreben müssen Plattformbetreiber entgegenwirken. Hierfür brauchen sie Mechanismen für die Qualitätskontrolle. Schlagen diese Mechanismen fehl, sollte auch das Feedback der Nutzenden auf einen unseriösen Partner hinweisen – dies unabhängig von den Mechanismen des Anbieters.

3.3 Spannungsfeld zwischen Usability und Datenschutz

Damit intelligente Reiseassistenten bestmöglich funktionieren können, sind große Datenmengen notwendig. Gleichzeitig handelt es sich bei diesen Daten unter anderem auch um sensible Kundendaten. Folgender Abschnitt skizziert das Spannungsverhältnis zwischen Usability und Datenschutz.

Eine Reiseanfrage an den Reiseassistenten kann durch folgende Angaben sehr allgemein gehalten werden:

- Abreise/Ort: Stadt Potsdam, Bahnhof/Zielort: Hauptbahnhof Berlin, Ankunftszeit: spätestens 9:30 Uhr, Reisetag: kommender Montag.
  - ➔ Bei dieser Anfrage kann im Regelfall nicht auf eine einzelne Person rückgeschlossen werden, da sehr viele Reisende diese Verkehrsknoten in dem genannten Zeitpunkt passieren werden. Ein Restrisiko bleibt, wenn Angreifern die IP-Adresse bekannt ist.

Dennoch gibt es bereits hier einige Besonderheiten zu beachten, um Rückschlüsse auf die eigene Person zu unterbinden. Dazu zählen:

- Wiederkehrende Anfragen, mit denselben Start- und Endpunkten, gegebenenfalls sogar demselben Wochentag und demselben Wunschzeitpunkt für die Ankunft.
  ➔ Wenn diese Daten mit früheren Abrechnungen (z. B. einzelner Transportdienstleister) verglichen werden, ist der Rückschluss auf eine Person bzw. auf einen kleinen Personenkreis möglich.

- Präziser Startpunkt, der auf einen sehr kleinen Kreis von Anwendern schließen lässt, wie die Stadt Werder (Havel), Hauptstr. 1.
  ➔ Möglicherweise leben nur 5 Personen in diesem Gebäude bzw. im Nachbargebäude. Damit fällt der mögliche Personenkreis sehr klein aus.

- Präziser Zielpunkt wie Friedrichstr. 219, in 10969 Berlin.
  ➔ Da sich an dieser Adresse eine Polizeiwache befindet, ist auch hierbei der mögliche Personenkreis als klein zu bewerten. Der Kreis könnte in zwei Gruppen zerfallen:
  a) beschäftigte Person, b) Besucher, der z. B. eine Meldung abgeben möchte.

- Die oder der Reisende wählt ständig als Wunsch-Transportmittel Bus und Bahn.
  ➔ Das könnte den Rückschluss erlauben, dass die oder der Reisende momentan oder dauerhaft nicht im Besitz eines Führerscheins ist.

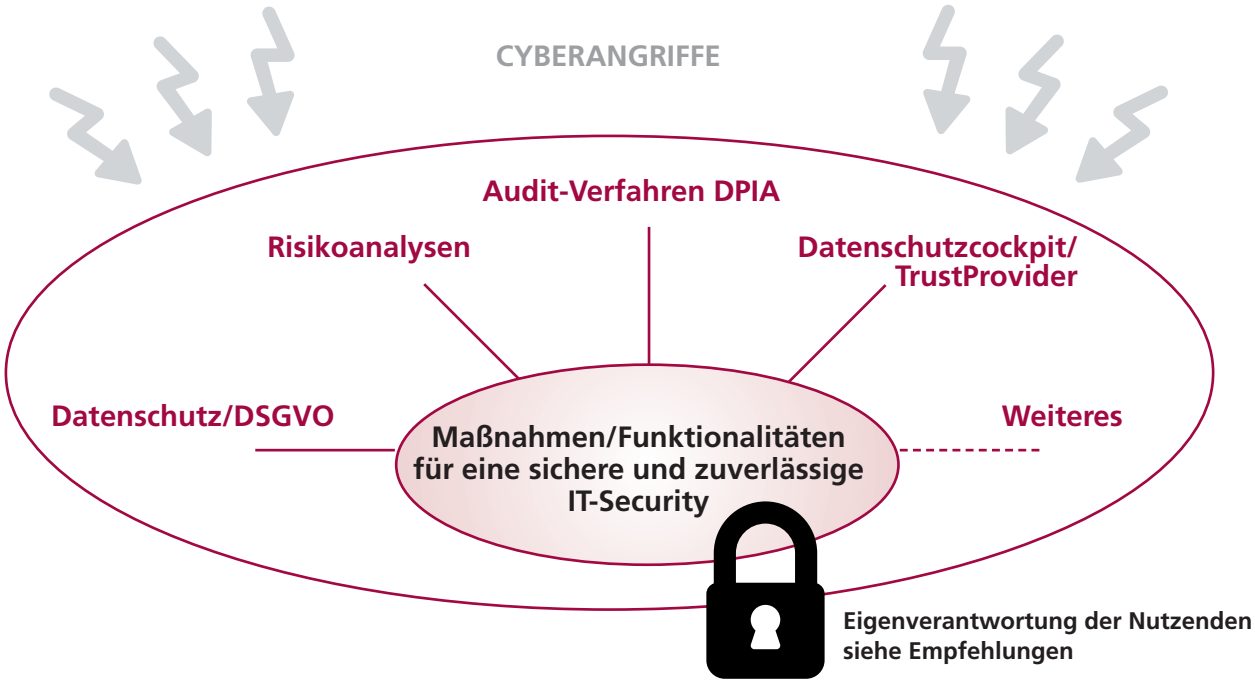
- Die oder der Reisende möchte barrierefrei von A nach B reisen, d. h. keine Treppen, Stufen, Absätze usw. auf der gesamten Reisestrecke.
  ➔ Wenn dieser Reisewunsch mit einer genauen Abreiseadresse verbunden ist, wie die Stadt Werder (Havel), Hauptstr. 1, ist der oder die Anfragende sehr leicht zu identifizieren.

Um möglichst großen persönlichen Komfort und Service genießen und gleichzeitig die Privatsphäre schützen zu können, stehen den Nutzenden eine Reihe an möglichen Maßnahmen zur Verfügung. Die Autoren empfehlen den Nutzenden folgende Maßnahmen zur Erhöhung der Datensicherheit:

1. So wenig wie nötig individuelle Wünsche in die Anfrage eingeben.
2. Nicht alle Abfragepunkte akribisch genau ausfüllen, sofern dies die Reiseplanung und den Bezahlvorgang nicht beeinflusst.
3. Sofern es weder die vorgeschlagene Reiseroute ändert noch deren Komfort mindert, Abreise- und Ankunfts-Adresse möglichst ungenau eingeben, wenn damit ein kleiner Personenkreis an potenziellen Nutzenden verbunden sein könnte.
4. Möglichst verschiedene anfallende Reisen (konkret: nicht nur private, sondern auch berufliche Reisen) über das Jahr buchen, bestätigen und bezahlen.

Die Einhaltung dieser Empfehlungen ist ein wichtiger Aspekt bei Sicherstellung der Sicherheit des intelligenten Reiseassistenten (siehe Abbildung 3).

Abbildung 3: Maßnahmen und Funktionalitäten für eine sichere und zuverlässige IT-Sicherheit.



4 IT-Sicherheit und Datenschutz im Umfeldszenario

Zur Sicherstellung einer angemessenen IT-Sicherheit und Minimierung von Cyberrisiken müssen bei der Entwicklung eines digitalen Reiseassistenten diejenigen Systemkomponenten und Daten identifiziert werden, die eines besonderen Schutzes bedürfen. Die IT-Lösung darf daher nicht nur die Anwendungsfälle einer intermodalen Mobilität umfassen, sondern muss auch die „Misuse Cases" berücksichtigen wie Identitätsdiebstahl, Empfang falscher Sprachkommandos etc. Da die Anzahl der „Misuse Cases" meist viel größer als die Anzahl der definierten Anwendungsfälle ist, macht es allerdings wenig Sinn, diese alle aufzulisten und für die IT-Lösung zu betrachten. Stattdessen sollte jede IT-Lösung IT-Security-Funktionalitäten enthalten, die Daten gegen Cybersecurity-Angriffe schützen, wie beispielsweise datenbezogene Zugriffskontrollen, Rollen- und Rechtedefinitionen oder die Authentisierung von Nutzenden, Geräten und Prozessen. Falls dieser Schutz nicht greift, sollten Angriffe vom System selbst oder vom Anbieter her wenigstens erkannt werden, um mit geeigneten Gegenmaßnahmen darauf reagieren zu können. Es sollte hierbei ein „Security by Design"-Prinzip verfolgt werden. Die Security-Domäne umfasst auch eine Reihe von Security-Maßnahmen zum Schutz personenbezogener Daten, die von Carla erzeugt und durch Dritte gesammelt, verarbeitet und/oder gespeichert werden (siehe Kapitel 4.2).

Die Datenschutzgrundverordnung (DSGVO) muss eingehalten werden, um Datenschutzprobleme zu vermeiden. Datenschutz-Folgenabschätzungen (DPIA) oder andere gleichwertige Audit-Verfahren müssen unter Berücksichtigung des Verwendungszwecks durchgeführt werden, um etwaige Datenschutzanforderungen zu identifizieren. Der Einsatz von Algorithmen kann so realisiert werden, dass eine Analyse der Daten beispielsweise zur Erstellung von Bewegungsprofilen auch ohne die Zusammenführung in einem zentralen Datenbestand möglich ist und dabei die Rechte und Interessen der oder des Datenschutzberechtigten gewahrt werden können. Daher ist ein zweckgebundener, bestimmter Datenaustausch notwendig. Er hat stets einen konkreten Anlass und zielt auf die Erbringung einer bestimmten Mobilitätsdienstleistung. Schlüsselfaktoren sind hierfür die zuverlässige Authentisierung und Authentifizierung von Carlas Identität. Carlas Buchungsvorgänge sollten je nach Verkehrsmittel anonym durchgeführt werden, unbeschadet einer Authentisierung mittels eines Identity-Providers. Auf Dienstanbieterseite wird durch Nutzung eines Pseudonyms einer Profilbildung von Carla vorgebeugt. Durch eine vertrauenswürdige dritte Instanz (sog. Datenschutzcockpit oder TrustProvider) muss für Carla in diesem Rahmen transparent gemacht werden, von welchem Akteur in welchem Zusammenhang ihre personenbezogenen Daten verarbeitet werden. Hinsichtlich notwendiger Schnittstellen zwischen einzelnen Systemen muss der Datenaustausch standardisiert in einheitlichem und sicherem Format erfolgen.

4.1 Klassifizierung von möglichen Angreifern und deren Motiven

Die Identifikation und Klassifizierung möglicher Angreifer, ihrer Motive und Angriffsziele hilft, die Resilienz intelligenter Reiseassistenten zu erhöhen. In Tabelle 3 nennen wir typische Beispiele inklusive möglicher Auswirkungen entsprechender unberechtigter Cyber-Angriffe.[8] Um den technischen IT-Schutzbedarf des KI-basierten Reise-Assistenzsystems zu ermitteln, sollten für KI-basierte Systeme Risikoanalysen herangezogen werden, die sich unbedingt auf die Integrität und Authentizität der KI-Datenbasis, Datenquellen, Lernzustände und Algorithmen von intelligenten Reiseassistenten erstrecken. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, solche Risikoanalysen auf den IT-Grundschutz aufzusetzen (vgl. BSI 2021).

Tabelle 3: Mögliche Beispiele für Täter-Typen und -Motive, um einen intelligenten Reiseassistenten für nicht vorgesehene unberechtigte Zwecke zu nutzen

Angreifer-Typ	Technische Angriffs-intensität	Motiv, Zielsetzung	Auswirkungen auf Mobilitätsszenarien
Kriminell	Mittel bis hoch	• Monetäre Vorteile • Eigeninitiativ als auch im Auftrag Dritter (Wettbewerber, staatliche Stellen)	• Ausspähen von KI-Modellen und Datenbasen zum Weiterverkauf • Manipulation zum Vorteil der Auftraggeber (z. B. Transport-Anbieter etc.)
Terroristisch	Mittel bis hoch	• Gesellschaftliche Unsicherheit erzeugen durch Herbeiführen von Katastrophen und Panik	• Überkritische Menschenansammlungen verursachen • Belegte Transportmittel blockieren oder zerstören
Wettbewerber	Mittel	• Monetäre Vorteile • Hohe Furcht vor Attribution, daher dezentes Vorgehen und Beauftragung Dritter	• Gezielte Umlenkung der Mobilitätsnachfrage auf bestimmte Anbieter durch Angebots-, Kapazitäts- und Preismanipulation
Ausländische staatliche Stellen (z. B. Nachrichtendienste)	Hoch bis sehr hoch	• Auffinden von gesuchten Personen wie potenzielle Terroristen • Schaffung von Sabotage-Potenzial	• Datenschutzverletzungen durch Abgreifen individueller Nutzungsinformationen wie Anfragen von Routen-Optionen, Buchungen, Platzreservierung und Zahlungsdaten • Identifikation und Filterung individueller Bewegungsmuster • Filterung und Manipulation individueller Reiseplanungen
Nutzende	Gering bis mittel	• Monetäre und weitere Vorteile (z. B. Zeitersparnis)	• Schwarmintelligenzalgorithmus kann nur eingeschränkt funktionieren • Manipulation individueller Reiseplanung • Überlastung einzelner Verkehrsmittel

8 Nationale staatliche Stellen können auf legalem Weg Zugriff auf die Plattform erhalten, z. B. per richterlichen Beschluss.

4.2 Intermodalitätsbedingte Besonderheiten vernetzter KI-Systeme

Natürlich sind die in der Einführung in dieses Kapitel und in Kapitel 4.1 beschriebenen Gefährdungen und Risiken auch für intermodale vernetzte IT-Systeme mit KI-Funktion zu berücksichtigen, ebenso wie allgemeine IT-Sicherheitsanforderungen. So müssen die Datensätze an ihrem Speicherort und auf den Übertragungsstrecken gegen unbefugtes Auslesen (personenbezogene Daten) und unbemerkte Veränderungen zuverlässig geschützt werden. Ebenso müssen zwischen interagierenden Systemen ausgetauschte Informationen und Auskünfte (Reisevorschläge) an den intelligenten Reiseassistenten zuverlässig authentisiert werden. Hierfür stehen geeignete kryptographische Verfahren zur Verfügung.

Wie im Szenario der Datenwege dargestellt ist, ist der intelligente Reiseassistent mit folgenden Informations-Datenquellen verbunden:

- mehrere Mobilitätsbetreiber bzw. deren Plattformen
- Geodaten, Meldungen von Straßensperren oder möglichen Großereignissen und dem zu erwartenden Wetter
- Carlas Anfrage-Daten mit Tag, Start, Ziel, Zeitpunkt der Zielerreichung etc.
- Trainings- und Feedback-Daten aus früheren Reisen

Weniger offensichtlich ist, ob sich die Nutzenden des intelligenten Reiseassistenten gegenüber den Mobilitätsanbietern bzw. deren Plattformen authentisieren sollten. Die Bewertung dieser Frage hängt zweifellos davon ab, welche Informationssysteme in die Antwort einbezogen werden.

Wir beleuchten kurz drei exemplarische Lösungsmöglichkeiten:

Lösungsmöglichkeit 1 verlangt eine sichere Authentisierung des bzw. der Nutzenden, etwa mit Hilfe der eID-Funktion des Personalausweises. Allerdings können Probleme auftreten, wenn Reiseauskünfte und Reisemittelbuchungen für Dritte (z.B. Kinder, Personen ohne Internetzugang) erbeten werden, ohne dass explizite Berechtigungen vorliegen.

Lösungsmöglichkeit 2: Durch die Erstregistrierung werden Stammdaten hinterlegt wie Angaben zur Person, Reisepräferenzen sowie Angaben zu bestehenden Verträgen (siehe auch Tabelle 3). Ein Beispiel wäre der Besitz einer gültigen BahnCard 25. Eine besondere Stellung nimmt dabei der Führerschein ein. Nach gültigem Gesetz muss vor jeder Übernahme eines Carsharing-Fahrzeugs die Vorlage eines gültigen Führerscheins erbracht werden. Dies könnte durch ein Video-Verfahren erfolgen oder durch den Führerschein-Datensatz auf dem Smartphone, wie er in der Passauer Erklärung im Dezember 2020 von den Verkehrsministerinnen und Verkehrsministern der EU-Mitgliedsstaaten angekündigt wurde.

9 Die eID-Funktion im Personalausweis beschreibt einen eingebauten Chip, mit Hilfe dessen sich Personen im Internet ausweisen können. Sie ist seit 2017 in jedem Personalausweis aktiviert.

Lösungsmöglichkeit 3 verlangt überhaupt keine Nutzerauthentisierung. Dies könnte zu Datenschutzproblemen führen, falls in die Antwort sensitive Informationen einfließen. Beispiel: Eine dritte (von Carla nicht autorisierte) Person fragt für Carla Reisepläne ab. Diese Person weiß, dass Carla ein Auto besitzt. Die Ergebnisse der unautorisierten Abfrage schlagen ausschließlich die Nutzung öffentlicher Verkehrsmittel vor – und das, obwohl die Nutzung des Autos aufgrund des Reiseziels oder der aktuellen Verkehrssituation durchaus sinnvoll wäre. Die Ergebnisausgabe könnte darauf hinweisen, dass Carla (zurzeit) keine Fahrerlaubnis besitzt oder unter krankheitsbedingten Einschränkungen leidet. Diese personenbezogenen Informationen könnten in einer Datenbank gespeichert sein oder das KI-System könnte so reagieren, weil Carla in den vergangenen zwei Monaten alle Reisevorschläge mit PKW-Nutzung abgelehnt hat. Für weitere Überlegungen in diese Richtung sei auf Kapitel 3.3 verwiesen.

Für die Reiseplanung stehen unterschiedliche Verkehrsmittel zur Verfügung, die auch innerhalb einer Reise kombiniert werden können. Müssen für eine Reiseanfrage mehrere KI-Systeme/Datenbasen verknüpft werden, kann dies zusätzliche Probleme aufwerfen: Müssen die oder der Reisende für alle Systeme Einverständniserklärungen (DSGVO) unterzeichnen (Positivliste)? Wie sähe das bei lokalen Datenbasen aus, die reiseabhängig eingebunden werden (sollten)? Möglicherweise enthält man aus der Verknüpfung mehrerer Systeme mehr Informationen als die Summe der Informationen aus den lokalen Datensätzen. Dies wirft insbesondere bei Lösungsmöglichkeit 3 Fragen auf, wie man solche indirekten, unerwünschten (und z. T. auch schwer vorhersehbaren) Erkenntnisse ausschließen kann.

DSGVO-Konformität zum Umgang mit der notwendigen Erhebung personenbezogener Daten

Die Verarbeitung personenbezogener Daten erfordert für die verarbeitende Stelle, bezogen auf unseren Fall: das Gesamtsystem des Reiseassistenten, eine entsprechende Rechtsgrundlage gem. Art. 6 DSGVO, da die Verarbeitung personenbezogener Daten zunächst nicht erlaubt ist. Daher muss ein sogenannter „Erlaubnistatbestand" erfüllt sein, um eine rechtmäßige Verarbeitung zu ermöglichen. In dem hier behandelten Szenario kommen grundsätzlich zwei Erlaubnistatbestände in Betracht:

1. Einwilligung der betroffenen Person: Eine der häufigsten Erlaubnistatbestände im Kontext von digitalen Plattformen ist die Einwilligung. Basierend auf leicht zugänglichen und klaren Informationen ist die betroffene Person über den Umfang der erhobenen Daten, den Verarbeitungszweck und in diesem Kontext auch über die dienstbezogene, erforderliche Weitergabe von Daten an Dritte – hier die einzelnen Mobilitätsanbieter – zu informieren. Auf ein entsprechendes Widerrufsrecht ist vor der Einwilligung hinzuweisen. Gleichzeitig darf an die Einwilligung keine über den Zweck hinausgehende Datenverarbeitung als Bedingung gekoppelt werden. Im Wesentlichen erstreckt sich die Einwilligung auf die Datenverarbeitung durch den Reiseassistenten selbst und je nach Ausgestaltung (z. B. integriertes Ticketing) auch auf die angeschlossenen Mobilitätsanbieter. Dabei dürften die-

se aber nur Zugang zu jenen personenbezogenen Daten erhalten, die für ihren spezifischen Verwendungszweck erforderlich sind.

2. Vertragserfüllung: Dieser Erlaubnistatbestand wäre beispielsweise bei Buchungsvorgängen/Ticketing sinnvoll, da ohne die Verarbeitung von Zahlungsinformationen die Buchung nicht erfolgen kann. Dabei ist es von der Architektur der Plattform abhängig, ob die Buchung durch den Reiseassistenten erfolgt oder durch den Mobilitätsanbieter. Würde die Buchung durch den Mobilitätsanbieter durchgeführt, würde die Reiseassistenz-Plattform selbst keine buchungsrelevanten personenbezogenen Daten erheben. Andersherum wäre dies jedoch gegeben und entsprechend wären Nutzende über Art und Umfang sowie Zweck der Datenerhebung ebenfalls zu informieren.

Generelle technische Maßnahmen bei der Einbindung mehrerer Informationssysteme zur Beantwortung einer Reiseanfrage bestehen darin, an die einzelnen Systeme nur Teildatensätze (relevante Einträge) zu versenden oder den gesamten Datensatz verschlüsselt an alle Systeme zu senden. Hierbei kann jedes System aber nur die für es relevanten Teile entschlüsseln (vergleichbar mit dem SET-Protokoll, das in den 90er Jahren zur Absicherung von Finanztransaktionen im Internet designt wurde). Beispielsweise müsste ein Informationssystem der Bahn AG nicht wissen, ob die oder der Nutzende einen PKW besitzt und ihn auch fahren darf.

Komplizierter wird es, wenn nicht nur die Antworten der einzelnen Informationssysteme kombiniert werden, sondern die Gesamtantwort von (personenbezogenen) Inhalten der einzelnen Datenbasen abhängt. Dann stellt sich die Frage, wie und wo der finale Reisevorschlag erarbeitet wird.

Mehrere Anfragen bei kleineren Transportmittelanbietern oder für bestimmte Strecken könnten ein KI-System veranlassen, hier einen Engpass oder eine Überlastung zu vermuten und entsprechend bevorzugt andere Routen vorzuschlagen. Dies trifft insbesondere auf Anfragen in die Zukunft zu. Bei nichtauthentisierten Reiseanfragen könnten Mitbewerber massenhaft gezielte Anfragen platzieren, die dem Konkurrenten schaden und somit das eigene Unternehmen begünstigen (vgl. Kapitel 4.1).

4.3 Betreibermodell der Plattform

Die im weiteren Verlauf dargestellten Funktionsumfänge werden maßgeblich von der Angebotsgestaltung determiniert. Zur Ausgestaltung einer Plattform sind mehrere Umsetzungsszenarien denkbar.[10] Im Folgenden werden zwei ausgewählte Möglichkeiten vorgestellt, die aus IT-Sicherheitsperspektive wichtig sind (siehe Tabelle 4).

10 In diesem Abschnitt wird auf das Betreibermodell der Plattform fokussiert. Für Informationen zu den Geschäftsmodellen im Szenario Carlas Reise siehe Susanne Boll-Westermann et al. 2020.

Tabelle 4: Übergeordnete zentrale Plattform versus föderierte dezentrale Plattform

Übergeordnete zentrale Plattform Alle Mobilitätsanbieter docken daran an	**Föderierte dezentrale Plattform** Von vielen Mobilitätsanbietern betrieben
• Plattformbetreiber hat die Hoheit über die Konditionen, zu denen sich Mobilitätsanbieter and die Plattform anschließen • **Vorteil für die Gesellschaft:** Bewerbung von gesellschaftlich relevanten Themen • **Vorteil für Nutzende:** ggfs. positive Preis-Wettbewerbsdynamik • **Risiken:** Zugang des Plattformbetreibers zu einem großen Datenschatz, Gefahr von Absprachen und von Angebots-, Preis- und Qualitätsmanipulationen	• Keine Hierarchie unter den Mobilitätsdienstleistern • **Vorteil für Nutzende:** Versuch, umfassende Mobilitätsketten abzubilden • **Risiken:** „The winner takes it all"-Effekte, wenn jeder Mobilitätsanbieter vollständigen Zugang zu den anfallenden Daten hat

1. Übergeordnete zentrale Plattform

Der Reiseassistent wird als von den Mobilitätsanbietern unabhängige, zentrale Plattform betrieben. Eine Ausprägung könnte zum Beispiel ein Public-Private-Partnership-Ansatz (kurz: PPP-Ansatz) sein, an dem die Stadt, die Gemeinde oder das Bundesland beteiligt ist. In dieser Konstellation hat der Plattformbetreiber die Hoheit über die Konditionen, zu denen sich Mobilitätsanbieter der Plattform anschließen. In einer PPP verlangt der Plattformbetreiber von den angeschlossenen Diensteanbietern regelmäßige Provisionszahlungen. Weitere Einnahmen könnten durch Einblendungen von Hinweisen (Werbeblöcke) über bevorstehende Großveranstaltungen in den Bereichen Sport, Kultur und Musik etc. sowie mit empfohlenen Anfahrtswegen und optimalen Zeitfenstern entstehen. Die zentrale Plattform würde gesellschaftlich relevante Themen wie Attraktivität eines Ballungsgebietes (schnelle Verbindung, Pünktlichkeit etc.), Klimaneutralität eines Transportwegs (geringere Umweltverschmutzung, weniger Treibhausgase) oder Effekte auf die Gesundheit (geringerer Ozonwert im Hochsommer, geringere Todeszahlen durch Luftverschmutzung) stärker bewerben als ein föderiertes Modell. Ziel dürfte hierbei die individuelle Gewinnmaximierung sein. Deshalb kann aus Verbrauchersicht eine positive Preis-Wettbewerbsdynamik dadurch entstehen, dass in diesem Modell konkurrierende Mobilitätsanbieter eher aufgenommen werden können als bei einer föderiert dezentralen Plattform. Gleichzeitig aber dürfte der Plattformbetreiber Zugang zu einem zunehmenden Datenschatz erhalten, den es entsprechend abzusichern gilt. In Ergänzung dazu könnten – verglichen mit einer dezentralen föderierten Plattform – stärkere Angebots-, Preis- und Qualitätsmanipulationen durch angeschlossene Anbieter entstehen. So könnten Entscheidungen der Nutzenden durch künstliche Verknappungen der Transportkapazitäten manipuliert werden. Darüber hinaus könnten einzelne Anbieter gemeinsam mit den Plattformbetreibern die

Konditionen für sich verbessern und gleichzeitig für die Nutzenden verschlechtern. Zur Vorbeugung könnten Angebote und Konditionen entsprechend transparent gemacht werden.

2. Föderierte dezentrale Plattform

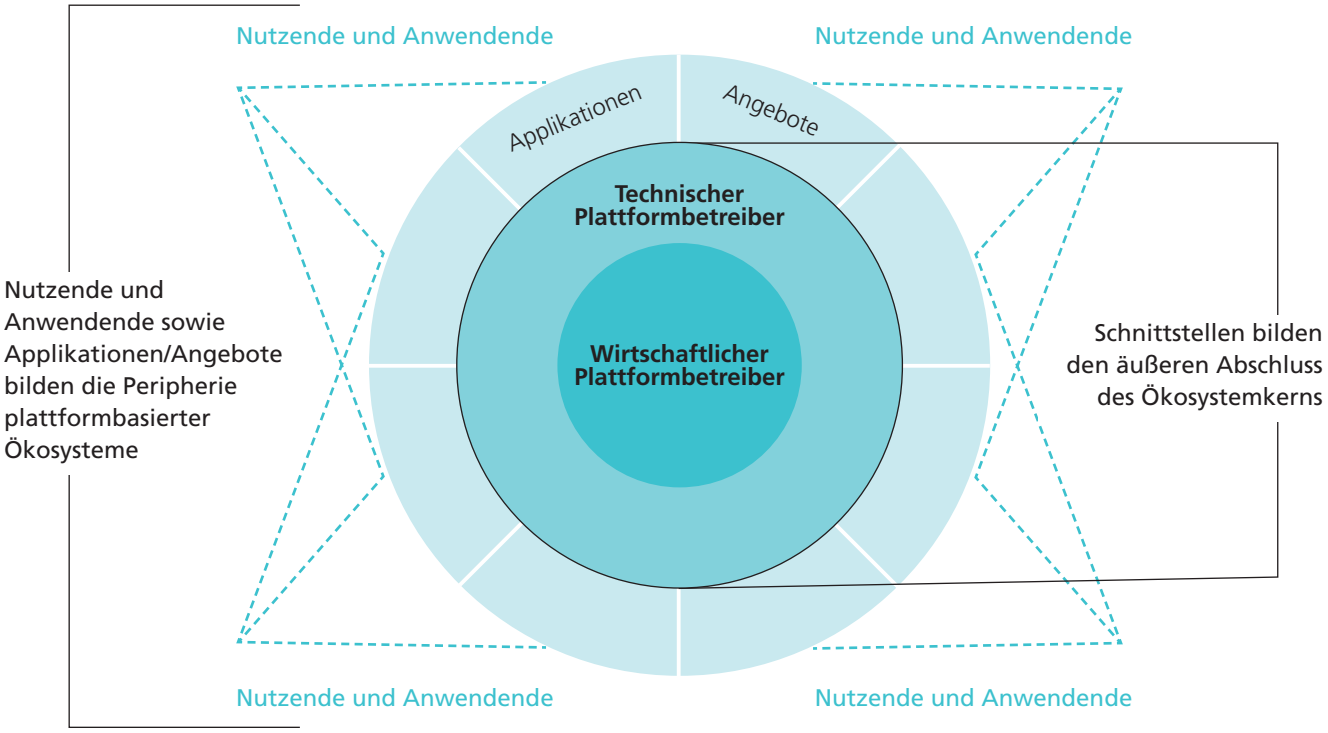
Der Reiseassistent wird als ‚föderiertes' System betrieben, bei dem alle angeschlossenen Mobilitätsdienstleister als gemeinsame Betreiber fungieren und anteilig die Kosten tragen. In dieser Konstellation existiert keine Hierarchie unter den Mobilitätsdienstleistern und es kommt im Regelfall zu keiner Konkurrenz unter den Mobilitätsdienstleistern, da man im jeweiligen Segment versucht, seine eigene Exklusivität gegenüber konkurrierenden Anbietern zu sichern. Ein Vorteil für Nutzende ist, dass die Plattformanbieter in diesem Modell eher versuchen, umfassende Mobilitätsketten abzubilden. Ihre Angebote könnten vor allem in weniger wettbewerbsintensiven Räumen interessant sein. Möglicherweise könnten in Ausnahmefällen jedoch mächtige Mobilitätsanbieter in der Plattform ihre Mobilitätsbandbreite immer weiter ausdehnen und so kleinere Mobilitätsbetreiber, die auf eine Nische spezialisiert sind, aus diesem föderierten System schrittweise herausdrängen („The winner takes it all"-Gefahr). Dieses Risiko besteht vor allem, wenn jeder beteiligte Mobilitätsanbieter vollständigen Zugang zu allen Anfragen, inklusive personenbezogener Daten, hätte und sich die Plattformbetreiber nicht selbst beschränken würden.

4.4 IT-Sicherheit und Integrität bei Plattformen

Ausgehend von der Diskussion über das entsprechende Betreibermodell erfolgt hier zunächst eine Betrachtung auf der Gesamtsystemebene. Diesbezüglich stellen die Autoren einige konturierende Prämissen vorweg: Es wird aus mehreren Perspektiven, konkret aus IT-Sicht, Kundensicht und im Sinne des öffentlichen Interesses, davon ausgegangen, dass eine Plattform favorisiert wird, die gegenüber einzelnen Anbietern und Transportwegen neutral agiert und sich finanziell trägt, aber keine reine Gewinnmaximierung verfolgt, um etwaige Marktverzerrungen durch unterschiedliche Konditionen für einzelne Anbieter zu vermeiden. Damit dürfte eher die föderierte dezentrale Plattform im Fokus stehen, die beispielsweise genossenschaftlich organisiert ist und unter der Hoheit der öffentlichen Hand stehen würde. Dies würde zudem die Fokussierung auf die an Allgemeingütern orientierte Erbringung von Mobilitätsdiensten nebenstehende Effekte wie Umweltschutz und Luftreinheit, Staureduzierung sowie Vermeidung von Wartezeiten ermöglichen. Damit dürfte zunächst auf der Ebene der wirtschaftlichen Betreiber ein möglichst hohes Maß an Angebotsintegrität sichergestellt werden können.

Wie eine Plattform ausgestaltet sein kann, wird in Abbildung 4 dargestellt.

Abbildung 4: Schematische Darstellung eines plattformbasierten digitalen Ökosystems



Quelle: eigene Darstellung nach Baums (2013), Dobusch et al. (2012), Schauf (2012)
https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3).

Die Aggregation der unterschiedlichen Mobilitätsangebote erfolgt auf der Ebene des technischen Plattformbetreibers. Anwendende greifen auf die von den technischen Plattformbetreibern bereitgestellten Informationen zur Reiseplanung und gegebenenfalls -buchungen über die Ebene der technischen Plattform des intelligenten Reiseassistenten zu. Wichtig ist, bereits an der Stelle anzumerken, dass davon ausgegangen wird, dass seitens der Mobilitätsanbieter dieser Bereich ihrer Dienste nicht unter den Anwendungsbereich kritischer IT-Infrastrukturen fällt und damit auch nicht in den Anwendungsbereich des IT-Sicherheitsgesetzes, da die Funktionalitäten des Reiseassistenten vom eigentlichen Mobilitätsdienst getrennt betrachtet werden können. Gleichwohl müssen die verschiedenen Akteure im Ökosystem ihrer jeweiligen spezifischen Verantwortung gerecht werden.

Somit ist grundsätzlich jeder Anbieter verantwortlich, die Integrität und Authentizität sowie Verfügbarkeit der von ihm übermittelten Informationen und/oder Funktionalitäten (z. B. Ticketing, Tracking, Fahrplanauskunft) sicherzustellen. Darunter fallen im Wesent-

lichen gewöhnliche Risiken, wie sie etwa von DDoS-Angriffen auf einzelne Mobilitätsanbieter ausgehen. Dabei erfolgen von einem Botnetz massenhafte Serveranfragen, um zu versuchen, die Verfügbarkeit einzelner Anbieter einzuschränken. Denkbar sind auch Angriffe, um Angaben über Feedbackschleifen zu verzerren, beispielsweise mit dem Ziel, Scoring oder Fahrplandaten zu verändern.

Dem technischen Betreiber obliegt dann wiederum die Verantwortung für den sicheren Betrieb der übergeordneten technischen Plattform sowie der entsprechenden Schnittstellen zu den angeschlossenen Applikationen. Auch hierzu zählt die Abwehr von Standardrisiken, die die Integrität der Plattform gefährden könnten. Gleichzeitig besitzt die Plattform eine Metaebene gegenüber allen einzelnen angeschlossenen Subsystemen (Applikationen) und bündelt für diese die Nutzeranfragen. Der Plattformbetreiber gewährt die Qualitätssicherung, indem er beispielsweise eine Anfragen-Anomalie-Erkennung etabliert (z. B. Programm gibt vor, ein Mensch zu sein; „Austricksen" des Systems). Ein solches System definiert unterschiedliche Kategorien von Anomalien anhand von Normverhalten, sodass auch eine lernende Komponente neu auftretende Anomalien erkennen kann. In Ergänzung dazu sollte er Datenschutzmaßnahmen wie Datensparsamkeit und Anonymisierungs- oder Pseudonymisierungsmechanismen in seinem System etablieren. Ebenso sollte der technische Betreiber ein besonderes Augenmerk auf den Schutz der Identitäten legen, da nicht nur den Datensicherheitsaspekten der DSGVO Rechnung zu tragen ist, sondern vielmehr die aus den Identitäten resultierenden Nutzungsprofile wiederum Grundlage der Selbstlernmechanismen sind. Gleichzeitig kann der technische Plattformbetreiber Vorgaben an die angeschlossenen Mobilitätsanbieter aufstellen und besitzt somit eine zusätzliche, zumindest normative Verpflichtung zur Einhaltung eines adäquaten IT-Sicherheitsniveaus. Bei einer gemeinsamen wirtschaftlichen Betreiberperspektive geht diese Verpflichtung einher mit der auch existierenden Gemeinwohlorientierung und dürfte daher ein grundsätzlicher konstitutiver Anspruch des Reiseassistenten sein.

Aus der Perspektive der Nutzenden dürfte es indes schwierig sein nachzuvollziehen, welche konkreten Anstrengungen Plattformbetreiber und angeschlossene Mobilitätsdienstleister unternehmen, um das IT-Schutzniveau möglichst konsistent zu gewährleisten. Oftmals bleibt diesen nichts anderes übrig, als dem Anbieter einfach zu vertrauen. Für Plattformbetreiber rückt damit ein Sicherheitsverständnis in den Fokus einer Angebotsdifferenzierung. Diese zusätzliche IT-Sicherheit kann man aus Verbraucherperspektive als „Security as a Feature" beschreiben. Für die Anwendenden entsteht dadurch Transparenz hinsichtlich etwaiger IT-Unsicherheiten bzw. (unvermeidbarer) Risiken. Sofern sogar Qualitätskriterien für Mobilitätsplattformen entwickelt werden würden, anhand derer die Sicherheitsparameter mess- und vergleichbar wären, könnten Verbraucherinnen und Verbraucher die verschiedenen Angebote miteinander vergleichen. Ausgangspunkt sämtlicher Überlegungen in diesem Zusammenhang ist die ISO 27001. Grundlage dieser internationalen Norm bildet eine Anforderungsbeschreibung zur Implementierung eines Informationssicherheits-Managementsystems, das Besonderheiten berücksichtigt und an die jeweiligen Gegebenheiten angepasst werden kann.

Über die weiter oben beschriebenen Anforderungen des Plattformbetreibers gegenüber den Mobilitätsanbietern hinaus besitzt der Betreiber eine Unterstützungsfunktion beim „Security as a Feature"-Ansatz. Aufgrund seiner Integrationskraft kann er entsprechende Qualitätskriterien für Datenverschlüsselung und Datensicherheit festlegen. Auch könnte er eine entsprechende Zertifizierung nach ISO 27001 als verpflichtendes Element zur Teilnahme an der Plattform bestimmen. Dadurch würde es auch offensichtlich für den Plattformbetreiber einfacher, seiner Sorgfaltspflicht gegenüber den Nutzenden nachzukommen. Einheitlich hohe und nachvollziehbare Standards, die jedes angeschlossene IT-System ebenfalls abdecken, bilden damit in Summe die informationstechnische Sicherheitsgrundlage für den Betrieb von intelligenten Reiseassistenten.

5 Gestaltungsoptionen

Intelligente Reiseassistenten können einen wesentlichen Beitrag zur Optimierung von Reisen leisten: den persönlichen Reisekomfort steigern und Verkehrsflüsse optimieren. Für bestmöglich funktionierende intelligente Reiseassistenten sind jedoch große Datenmengen notwendig. Je nach Art der Anfrage handelt es sich mitunter auch um sensible Kundendaten (siehe Kapitel 3). So entsteht ein Spannungsfeld zwischen Usability und Datenschutz, welches es entsprechend den Wünschen und Anforderungen der jeweiligen Nutzenden bestmöglich zu gestalten gilt. Hierzu können sowohl die Nutzenden selbst als auch alle weiteren beteiligten Stakeholder einen Beitrag leisten.

Nutzende von intelligenten Reiseassistenten

Je mehr Informationen die oder der Reisende an den intelligenten Reiseassistenten übergibt, desto besser werden die Angebote auf sie oder ihn zugeschnitten sein. Die Angabe personenbezogener Daten sollte jedoch stets das Ergebnis einer persönlichen Abwägung sein. Um potenzielle Risiken hinsichtlich IT-Sicherheit und Datenschutz zu umgehen (siehe Kapitel 3 und 4), können die Nutzerin oder der Nutzer unterschiedliche Vorkehrungen treffen. In diesem Sinne ist „smart trust" angebracht, also ein reflektierter Umgang mit den eigenen Daten bei der Nutzung von intelligenten Reiseassistenten:

- Die Nutzenden sollten – wenn möglich – den Anbieter des intelligenten Reiseassistenten sorgfältig auswählen und darauf achten, ihre Daten nur seriösen Anbietern zur Verfügung zu stellen, die deren datenschutzgerechte Anonymisierung oder Pseudonymisierung sicherstellen. Hierbei sollten die Nutzenden beispielsweise auf Zertifizierungen achten. Um der Bildung monopolartiger Strukturen vorzubeugen, sollte – wenn möglich – auch mehr als ein intelligenter Reiseassistent verwendet werden.

- Wenn aus persönlichen oder beruflichen Gründen die Preisgabe personenbezogener Daten oder die Standortbestimmung vermieden werden soll, können Nutzende entsprechende Vorsichtsmaßnahmen treffen, also beispielsweise nicht alle Abfragepunkte akribisch genau ausfüllen oder Angaben zu individuellen Wünschen und Standorten ungenau eingeben (siehe Kapitel 3.2). Es empfiehlt sich hierbei, die Anfrage rechtzeitig vor Reiseantritt zu starten, um ohne Zeitdruck darüber entscheiden zu können, welche Daten angegeben werden sollen, und frühzeitig von den besten Reiseoptionen zu profitieren.

- Nutzende sollten die Bereitschaft mitbringen, bestehende Informationsangebote zur Funktionsweise von KI-Systemen anzunehmen, um reflektierte Entscheidungen (beispielsweise zur Angabe von Daten) treffen zu können. Darüber hinaus können sie regelmäßig die durch das System gelernten Daten anfragen, überprüfen und gegebenenfalls durch die Betreiber anpassen lassen (siehe Kapitel 3.2).

Plattformbetreiber

Der jeweilige Plattformbetreiber ist für die Qualität des Angebots verantwortlich und muss dafür Sorge tragen, dass ein adäquates Datenschutz- und IT-Sicherheitsniveau eingehalten wird. Dies schließt auch die teilnehmenden Mobilitätsanbieter mit ein. Dazu stehen dem Plattformbetreiber unterschiedliche Mittel zur Verfügung:

- Der Plattformbetreiber sollte die teilnehmenden Mobilitätsanbieter bewusst auswählen. Ergänzend sollte er konkrete Vorgaben an die angeschlossenen Mobilitätsanbieter zur Einhaltung der IT-Sicherheit formulieren (beispielsweise: Mindestsicherheitsniveau und Verbleib der Daten im europäischen Wirtschaftsraum).

- Der Plattformbetreiber sollte die Einhaltung der festgelegten Vorgaben regelmäßig überprüfen (ggf. auch mit Unterstützung durch KI-Systeme). Im Idealfall sollte der Plattformanbieter auch die Qualitätsversprechen der angeschlossenen Mobilitätsanbieter mit Hilfe von empirischen Tests oder dem Einholen von Feedback seitens der Nutzenden stichprobenartig überprüfen.

- Der Plattformbetreiber sollte das eigene Angebot inklusive der Algorithmen regelmäßig durch dritte Stellen überprüfen lassen. Damit können Plattformbetreiber die Qualität des Angebots sicherstellen sowie Vertrauen bei den Nutzerinnen und Nutzern schaffen und langfristig somit aufrechterhalten (siehe auch Heesen/Müller-Quade/Wrobel et al. 2020).

- Der Plattformbetreiber sollte dafür Sorge tragen, dass der intelligente Reiseassistent und die zugehörige App möglichst datensparsam entwickelt und betrieben werden („privacy by design“, „privacy by default“). Es sollen nur die Daten abgefragt werden, die für die Leistungserbringung zwingend notwendig sind.

Mobilitätsanbieter

Mobilitätsanbieter stehen auch untereinander in Konkurrenz. Künftig könnte ein ausschlaggebendes Kriterium für ihren Erfolg auch ihre Integrierbarkeit in intelligente Reiseassistenten sein. Eine Voraussetzung hierfür ist ebenfalls ein hohes Maß an IT-Sicherheit:

- Mobilitätsanbieter sollten hierfür dem Plattformbetreiber als Schnittstelle zu den Kundinnen und Kunden oder sonstigen dritten Stellen Überprüfungen des eigenen Systems ermöglichen, um Seriosität gegenüber dem Plattformbetreiber deutlich zu machen.
- In Ergänzung dazu sollten Mobilitätsanbieter eigenverantwortlich ein hohes IT-Sicherheitsniveau anstreben, um als verlässlicher und attraktiver Partner zu gelten.

Politische Entscheidungsträgerinnen und Entscheidungsträger

Die öffentliche Hand kann Rahmenbedingungen schaffen, um Plattformen sowie einen Anschluss der Mobilitätsanbieter an diese zu ermöglichen. Mögliche Ansatzpunkte sind:

- Politische Entscheidungsträgerinnen und Entscheidungsträger sollten die Anbieterpluralität, also die Einrichtung und den Betrieb mehrerer intelligenter Reiseassistenten fördern. Im Idealfall existiert auf dem Markt eine Anbieterpluralität, die zu einem höheren Qualitätsniveau – auch mit Blick auf die Sicherheit der Angebote – führt.

- Es ist wichtig, dass Nutzende über Funktionsweisen von und im Umgang mit KI-Systemen stärker aufgeklärt werden. So wären sie selbst in der Lage, Nutzen von KI-Systemen einerseits und mögliche Risiken im Umgang mit intelligenten Reiseassistenten andererseits zu bewerten und ihr Handeln an dieser Risikobewertung zu orientieren. Die öffentliche Hand kann hier Projekte, die der Wissenschaftskommunikation in Bezug auf Nutzende von KI-Systemen dienen, finanziell und organisatorisch unterstützen.

Forschung und Entwicklung

Die Autoren haben zudem Forschungsbedarfe identifiziert, die in einer erweiterten Analyse von intelligenten Reiseassistenten zu betrachten wären:

- **Spannungsfeld:** Datensparsamkeit versus Usability. Hier gilt es für alle Akteure, IT-Sicherheit zu gewährleisten und gleichzeitig Datensparsamkeit durch „privacy by design“ und „privacy by default“ anzustreben. Letztere sollte jedoch nicht die Usability von intelligenten Reiseassistenten einschränken. So bleibt zu klären, wie dieses Spannungsfeld aufgelöst werden kann.

- **Erklärbare KI (explainable AI, kurz: XAI) fördern:** KI-Methoden und Algorithmen zur Eigenschaftsprüfung, zur Erläuterung von Entscheidungen und zu deren Absicherung erforschen und entwickeln, die die Qualitätssicherung intelligenter Reiseassistenten erleichtern und auch zu ihrer Evaluierung eingesetzt werden können.

Viele der vorgestellten Sicherheitsprobleme werden sich künftig technisch lösen lassen. Daneben existieren noch zu klärende gesellschaftsrelevante Fragen, die in einem breiten **gesellschaftlichen und politischen Diskurs** gezielt diskutiert und beantwortet werden müssen. Dies betrifft vor allem folgende Fragen:

- **Fairness-Gesichtspunkte bei Schwarmintelligenz:** Welche der Reisenden bekommen bei Überlastungen eine Ausweichroute angeboten und wer darf auf der „dann wieder freien“ Strecke weiterfahren? Wer bekommt das letzte freie Carsharing-Auto angezeigt? Dies sind komplexe Entscheidungen, die sowohl Ausgewogenheits- als auch Fairnessaspekte umfassen. Möglichkeiten wären die Anwendung des „First-come-first-serve-Prinzips“ (ähnlich der Sitzplatzvergabe im Flugzeug) oder eines komplexeren

Verfahrens, das über zusätzlich eingegebene Daten die mögliche Belastbarkeit der Reisenden mit in die Entscheidung einfließen lässt.

- **Fairness-Gesichtspunkte in Bezug auf die Nutzer-Qualifikation:** Nutzende wie Digital Natives, die im Einsatz Lernender Systeme geübt sind und diese schnell und intuitiv nutzen, könnten bessere Ergebnisse und Reiseoptionen erhalten als Menschen, die mit intelligenten Systemen wenig vertraut sind. Wie kann die Diskrepanz in der Nutzer-Qualifikation zwischen erfahrenen und ungeübten Nutzenden ausgeglichen werden? Wie können in diesem Kontext Diskriminierung und Benachteiligung bestimmter Nutzender vermieden werden?

- **Standardeinstellungen des intelligenten Reiseassistenten:** Wie verhält sich der intelligente Reiseassistent in einer anforderungsarmen Situation, also wenn eine Nutzende oder ein Nutzender nur sehr wenig Präferenzen und Anforderungen angibt? Sollten bestimmte Präferenzen, wie beispielsweise möglichst geringe CO_2-Emissionen oder die gleichmäßige Auslastung der Verkehrsmittel, dann standardmäßig hinterlegt sein oder sollte die KI nach klassischen Parametern wie Dauer entscheiden?

- **Erklärbarkeit und Marktmacht des intelligenten Reiseassistenten:** Wie erklärbar soll das KI-System sein? Wie viel Auskunftsrecht brauchen die Nutzenden mindestens über ihre Daten und die an sie ausgegebenen Vorschläge? Wie mächtig soll und darf ein Plattformsystem werden (zum Beispiel hinsichtlich der Komplexität, der Zahl der Nutzenden und der Betreibenden)? Die Forderung an Forschung & Entwicklung, erklärbare KI anzustreben, geht somit mit einer gesellschaftlichen Debatte zu Auskunftsrechten der Nutzenden und Auskunftspflichten der Dienstanbieter einher.

- **Wer trägt das Risiko:** Was passiert im Falle einer Fehlfunktion? Wer trägt die Verantwortung für mögliche durch Fehlfunktionen des Systems verursachte Schäden?

Abschließend ist festzuhalten, dass der Einsatz von intelligenten Reiseassistenten von großem öffentlichen Interesse ist, da sie viele Vorteile bieten und langfristig einen Beitrag zur nachhaltigen, intelligent vernetzten Mobilität leisten können: Den Nutzenden selbst bieten die intelligenten Reiseassistenten einen geringeren Aufwand bei der Reisebuchung, mehr Reisekomfort und Zeitersparnis. Darüber hinaus haben sie das Potenzial, zur Attraktivität von Großstädten und Ballungsräumen beizutragen, indem sie intermodale Transportmöglichkeiten optimal verknüpfen, und so etwa Staus und Umweltbelastungen vermeiden helfen. Langfristig können über die in den Plattformen bereitstehenden Daten auch Rückschlüsse auf den Bedarf an Mobilitätsinfrastruktur gezogen werden. Solche Erkenntnisse können beispielsweise in der Städteplanung und bei der Weiterentwicklung von Verkehrswegen relevant sein.

Der Erfolg von intelligenten Reiseassistenten wird jedoch von der Akzeptanz durch die Nutzenden abhängen. Die Usability sollte mit einer sicheren IT-Infrastruktur vereinbar sein, die mit den Daten der Reisenden sicher und vertrauenswürdig umgeht. Dieses Whitepaper

bietet verschiedene Lösungsansätze für die Ausgestaltung von intelligenten Reiseassistenten. So haben die Autoren in diesem Whitepaper beispielsweise herausgearbeitet, welche Anforderungen die Plattformbetreiber, die hinter intelligenten Reiseassistenten stehen, erfüllen müssen, damit die Plattformen sicher funktionieren (siehe Kapitel 4). Letztendlich sind alle beteiligten Stakeholder gefordert, Rahmenbedingungen zu schaffen, die eine sichere und vertrauenswürdige Anwendung von intelligenten Reiseassistenten ermöglichen.

Literatur

BMJV (2018a): Bundesdatenschutzgesetz (BDSG), § 46. https://dejure.org/gesetze/BDSG/46.html (abgerufen am 20.04.2021).

BMJV (2018b): Bundesdatenschutzgesetz (BDSG), § 51. https://dejure.org/gesetze/BDSG/51.html (abgerufen am 20.04.2021).

BMWI (2019): Digitale Souveränität im Kontext plattformbasierter Ökosysteme. Plattform „Innovative Digitalisierung der Wirtschaft", Fokusgruppe „Digitale Souveränität" im Rahmen des Digitalgipfels 2019. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3 (abgerufen am 20.04.2021).

Boll-Westermann, S. et al. (2020): KI-Geschäftsmodelle für Reisen und Transport: Mehr Wirtschaftlichkeit und Nachhaltigkeit in der Mobilität der Zukunft. Whitepaper aus der Plattform Lernende Systeme, München. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG4_5_Geschaeftsmodelle_Reisen_Transport.pdf (abgerufen am 20.04.2021).

BSI (2021): IT-Grundschutz. Informationssicherheit mit System. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (abgerufen am 20.04.2021).

Bundesagentur für Arbeit (2018): Pendlerverflechtungsmatrix. https://statistik.arbeitsagentur.de/Statistikdaten/Detail/202006/iiia6/beschaeftigung-pendler-blxbl/blxbl-d-0-202006-xls.xlsx?__blob=publicationFile&v=2 (abgerufen am 20.04.2021).

Bundesagentur für Arbeit (2020): Pendleratlas. https://statistik.arbeitsagentur.de/DE/Navigation/Statistiken/Interaktive-Angebote/Pendleratlas/Pendleratlas-Nav.htm (abgerufen am 20.04.2021).

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2020): Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche. https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf;jsessionid=2CA38A5E082E4148C0FC5D7277A835E0.1_cid329?__blob=publicationFile&v=2 (abgerufen am 20.04.2021).

Deutsche Bahn (2021): Infrastrukturregister. https://geovdbn.deutschebahn.com/isr (abgerufen am 20.04.2021).

Deutsches Institut für Urbanistik (2018): Was ist eigentlich ... Intermodaler und multimodaler Verkehr? https://difu.de/nachricht/was-ist-eigentlich-intermodaler-und-multimodaler-verkehr (abgerufen am 20.04.2021).

Europäische Union (2018a): Datenschutz-Grundverordnung (DSGVO), Art. 6. https://dejure.org/gesetze/DSGVO/6.html (abgerufen am 20.04.2021).

Europäische Union (2018b): Datenschutz-Grundverordnung (DSGVO), Art. 7. https://dejure.org/gesetze/DSGVO/7.html (abgerufen am 20.04.2021).

European Commission (2020): Proposal for a regulation of the European Parliament and of the Council (Data Governance Act). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767 (abgerufen am 20.04.2021).

Heesen J./Müller-Quade, J./Wrobel, S. et al. (2020): Zertifizierung von KI-Systemen. Impulspapier. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/Zusammenfassungen/AG3_Impulspapier_Kurzfassung_200507.pdf (abgerufen am 20.04.2021).

INRIX (2020): Traffic Scorecard Report. Berlin. https://inrix.com/scorecard-city/?city=Berlin&index=76 (abgerufen am 20.04.2021).

Nationale Plattform Zukunft der Mobilität (2020): Dritter Zwischenbericht. Plattformbasierte Intermodale Mobilität und Handlungsempfehlungen zu Daten und Sicherheit. https://www.plattform-zukunft-mobilitaet.de/wp-content/uploads/2020/07/NPM-AG-3-Plattformbasierte-intermodale-Mobilität-und-Handlungsempfehlungen-zu-Daten-und-Sicherheit.pdf (abgerufen am 20.04.2021).

Plattform Lernende Systeme (Hrsg.) (2019a): Anwendungsszenario Carlas Reise. https://www.plattform-lernende-systeme.de/umfeldszenario-intelligent-vernetzt-unterwegs.html (abgerufen am 20.04.2021).

Plattform Lernende Systeme (Hrsg.) (2019b): Auf dem Weg zu einem intelligenten Mobilitätsraum – Bericht der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG5_Bericht_280619.pdf (abgerufen am 20.04.2021).

Plattform Lernende Systeme (2021): Glossar. https://www.plattform-lernende-systeme.de/glossar.html (abgerufen am 20.04.2021).

Statistisches Bundesamt (2016): Erwerbstätigkeit. Berufspendler. https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Erwerbstaetigkeit/Tabellen/pendler1.html (abgerufen am 20.04.2021).

Statistisches Bundesamt (2021): Mobilität nähert sich in der zweiten Februarhälfte 2021 dem Vorkrisenniveau. https://www.destatis.de/DE/Presse/Pressemitteilungen/2021/03/PD21_100_p001.html (abgerufen am 20.04.2021).

Umweltbundesamt (2021): Emissionsdaten. https://www.umweltbundesamt.de/themen/verkehr-laerm/emissionsdaten#HBEFA (abgerufen am 20.04.2021).

Über dieses Whitepaper

Die Autoren des Whitepapers sind Mitglieder der Arbeitsgruppen IT-Sicherheit, Privacy, Recht und Ethik sowie Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme.

Als eine von insgesamt sieben Arbeitsgruppen thematisiert die Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik Fragen zur Sicherheit (Security), Zuverlässigkeit (Safety) und zum Umgang mit Privatheit (Privacy) bei der Entwicklung und Anwendung von Lernenden Systemen. Sie analysiert zudem damit verbundene rechtliche sowie ethische Anforderungen und steht in engem Austausch mit allen weiteren Arbeitsgruppen der Plattform Lernende Systeme. Die Arbeitsgruppe Mobilität und intelligente Verkehrssysteme untersucht, wie Lernende Systeme unsere Mobilitätsstrukturen verändern und welche Eigenschaften sie haben müssen, um den größten Nutzen für das Individuum und die Gesellschaft zu erzielen. Die Arbeitsgruppe hinterfragt, wie Infrastrukturen und Systemarchitekturen im Mobilitätssektor weiterentwickelt werden müssen, um Lernende Systeme darin sinnvoll zu integrieren.

Autoren

Mitglieder der Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik
Prof. Dr. Jörn Müller-Quade, Karlsruher Institut für Technologie
Dr. Detlef Houdeau, Infineon Technologies AG
Peter Rost, secunet Security Networks AG
Thomas Schauf, Deutsche Telekom AG
Prof. Dr. Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Mitglieder der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme
Dr. Tobias Hesse, Deutsches Zentrum für Luft- und Raumfahrt (DLR)
Dr. Rudolf Felix, PSI FLS Fuzzy Logik & Neuro Systeme GmbH

Autoren mit Gaststatus
Richard Goebelt, Verband der TÜV e. V. (VdTÜV)

Redaktion
Stephanie Dachsberger, Geschäftsstelle der Plattform Lernende Systeme
Rebecca Ebner, Geschäftsstelle der Plattform Lernende Systeme
Dr. Erduana Wald, Geschäftsstelle der Plattform Lernende Systeme
Christine Wirth, Geschäftsstelle der Plattform Lernende Systeme

Über die Plattform Lernende Systeme

Lernende Systeme im Sinne der Gesellschaft zu gestalten – mit diesem Anspruch wurde die Plattform Lernende Systeme im Jahr 2017 vom Bundesministerium für Bildung und Forschung (BMBF) auf Anregung des Fachforums Autonome Systeme des Hightech-Forums und acatech – Deutsche Akademie der Technikwissenschaften initiiert. Die Plattform bündelt die vorhandene Expertise im Bereich Künstliche Intelligenz und unterstützt den weiteren Weg Deutschlands zu einem international führenden Technologieanbieter. Die rund 200 Mitglieder der Plattform sind in Arbeitsgruppen und einem Lenkungskreis organisiert. Sie zeigen den persönlichen, gesellschaftlichen und wirtschaftlichen Nutzen von Lernenden Systemen auf und benennen Herausforderungen und Gestaltungsoptionen.

Impressum

Herausgeber
Lernende Systeme –
Die Plattform für Künstliche Intelligenz
Geschäftsstelle | c/o acatech
Karolinenplatz 4 | 80333 München
www.plattform-lernende-systeme.de

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
Juni 2021

Bildnachweis
Tempura/iStock/Titel

Bei Fragen oder Anmerkungen zu dieser Publikation kontaktieren Sie bitte Johannes Winter (Leiter der Geschäftsstelle):
kontakt@plattform-lernende-systeme.de

Folgen Sie uns auf Twitter: @LernendeSysteme

Empfohlene Zitierweise
Tobias Hesse, Jörn-Müller-Quade et al. (Hrsg.): Mit KI sicher reisen. Datenmanagement und Datensicherheit bei KI-basierten Reiseassistenten. Whitepaper aus der Plattform Lernende Systeme, München 2021