Lernende Systeme
DIE PLATTFORM FÜR KÜNSTLICHE INTELLIGENZ

Mit KI sicher reisen

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

Kurzfassung

Die Mobilität der Zukunft wird digital vernetzt sein und individuelle, passgenaue Mobilitätsservices bereitstellen. Künstliche Intelligenz (KI) kann hier einen wichtigen Beitrag leisten, indem sie einerseits Infrastrukturen, die Umwelt sowie Ressourcen nachhaltig und effizient entlastet sowie andererseits Reisende zeitsparend und flexibel ans Ziel geleitet. Dies bequem mit dem intelligenten Reiseassistenten als Reiseterminal am Smartphone oder auf dem Laptop, der Angebote im Hintergrund bündelt, analysiert und individuelle Reiserouten vorschlägt, die zugleich auf eine umweltverträgliche und nachhaltige Mobilität setzen.

Wie der intelligente Reiseassistent zukünftig in die Anwendung gelangen und ein beständiger Reisebegleiter im Alltag werden kann, zeigen die Expertinnen und Experten der Arbeitsgruppe IT-Sicherheit, Privacy, Recht und Ethik sowie Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme auf. Im Fokus stehen hierbei Fragen zur IT-Sicherheit im Rahmen der Entstehung und Nutzung von Daten in KI-basierten Reiseassistenten. Denn entscheidend für den Einsatz solcher Reiseassistenten ist einerseits, wie der Umgang mit den anfallenden Daten entlang der Mobilitätsdienstleistungskette im Hinblick auf IT-Sicherheit und Datenschutz geregelt und gewährleistet ist und andererseits, ob er auf persönliche Präferenzen hin zugeschnittene Reisevorschläge liefert. Dieses Spannungsfeld zwischen Usability, Datenschutz und IT-Sicherheit gilt es abzudecken.

Funktionsweise des KI-basierten Reiseassistenten

Wie ein solcher Reiseassistent aussehen und funktionieren kann, wird zunächst anhand eines digitalen Reiseassistenten aus dem fiktiven Anwendungsszenario „Carlas Reise“ (Kapitel 2) aufgezeigt, das von der Arbeitsgruppe Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme entwickelt wurde. Das Szenario veranschaulicht, wie Reisende, alias Carla, 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 dazu lernt.

Einsatzszenarien: Das Ziel des intelligenten Reiseassistenten ist es, vor dem Hintergrund individueller Präferenzen, Auswahlmöglichkeiten und Kontextfaktoren, die optimale Reise zu ermitteln. Hierbei kann der Reiseassistent jederzeit vor, während und nach einer Reise eingesetzt werden: zur Planung, Buchung, aber auch zur Änderung der Reise bei unvorhergesehenen Einschränkungen im Verkehrsfluss. Und als weiterer Vorteil: Durch Feedback der Nutzenden entwickelt er sich zudem stets weiter (Kapitel 2.3).

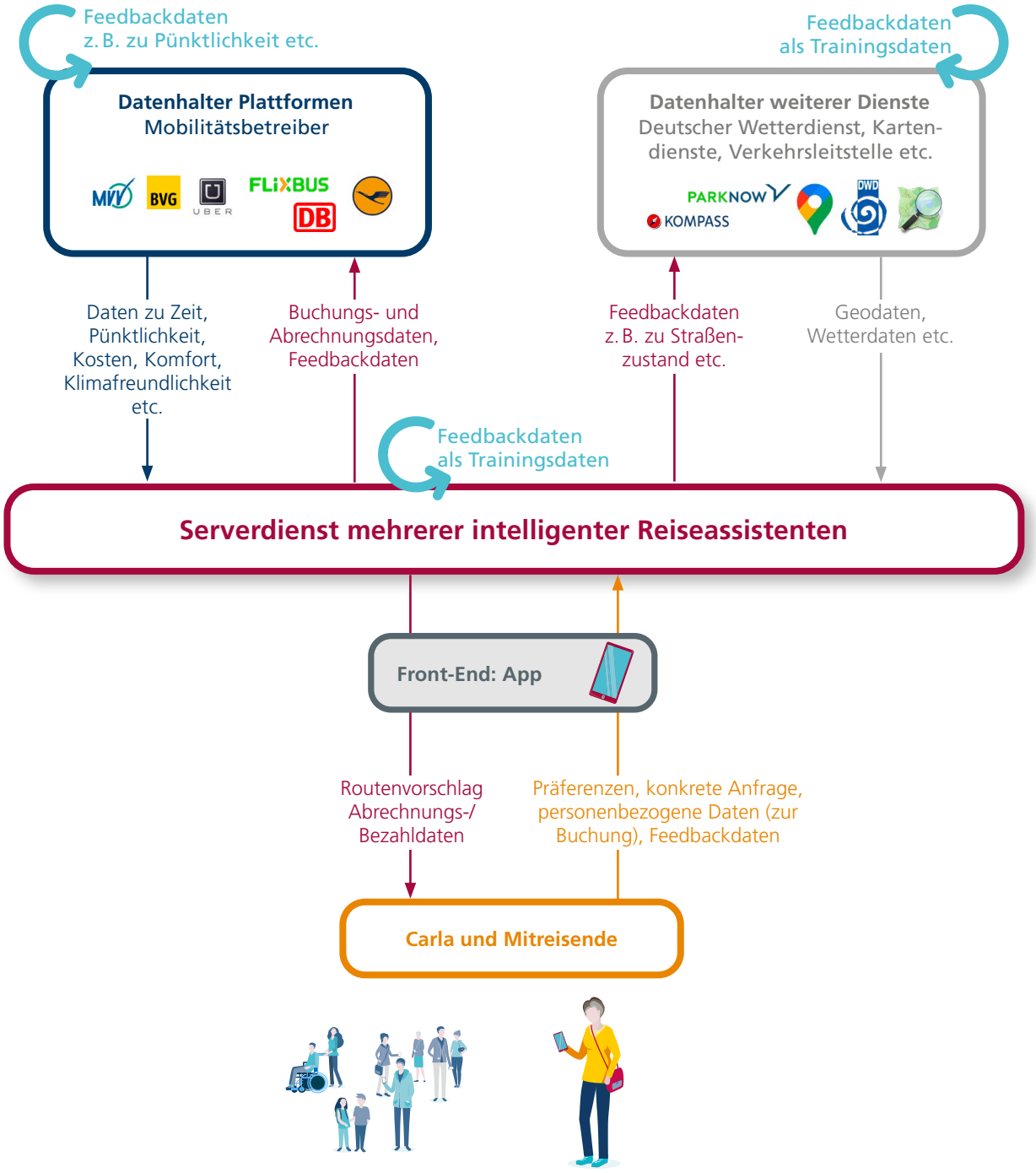
Technische Grundlage – Mobilitätsplattform: Die technische Grundlage des intelligenten Reiseassistenten bildet eine digitale Mobilitätsplattform, die Teil einer Systemarchitektur ist, über die mehrere Datenhalter, wie Mobilitätsbetreiber, Verkehrsunternehmen oder Infrastrukturbetreiber, ihre Daten freiwillig miteinander vernetzen (Kapitel 2.3.2). Die Mobilitätsplattform selbst hält keine Daten zentral vor. 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.

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).

Daten im Spannungsfeld zwischen Usability und Datenschutz

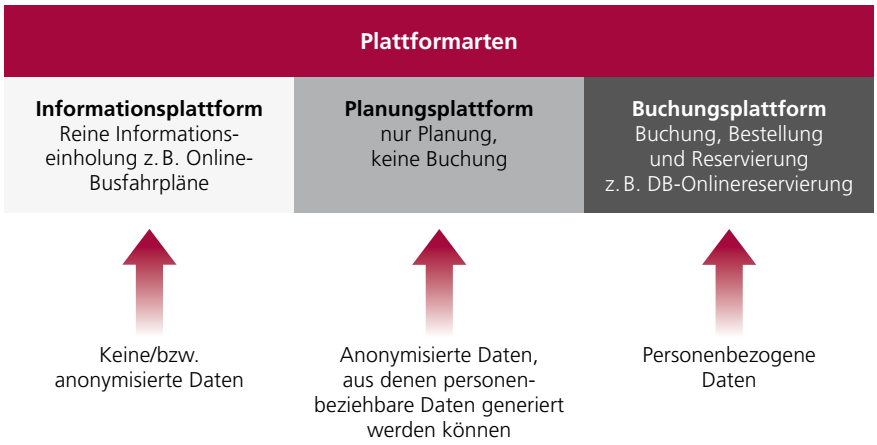
Neben möglichen Optionen der Ausgestaltung von digitalen Reiseassistenten skizziert das Autorenteam in diesem Umfeld das Spannungsfeld zwischen Usability und Datenschutz, indem es anhand des Szenarios aufzeigt, wo und wann welche Arten von Daten von welchem Akteur innerhalb des gesamten Mobilitätsökosystems anfallen (siehe Abbildung 1).

Abbildung 1: Der gesamte Datenweg sowie alle beteiligten Akteure im Mobilitätsdatenökosystem im Überblick



Sowohl die Funktionsweise intelligenter Reiseassistenten selbst als auch die zahlreich anfallenden Daten – mitunter auch sensible Kundendaten – in solch einem komplexen Datenökosystem stellen hohe Anforderungen an die IT-Sicherheit und den Datenschutz. Daher ist die Art der Daten und damit auch das Level an benötigter IT-Sicherheit auch von der jeweiligen Plattformart, auf der der intelligente Reiseassistent basiert, abhängig (siehe Abbildung 2).

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



Ziel der Verfassenden ist es daher, mögliche Risiken beim Einsatz eines KI-basierten Reiseassistenten zu identifizieren und als Antwort darauf mögliche Lösungsvorschläge aufzuzeigen (Kapitel 4). Hierbei sollte grundsätzlich der Ansatz des „Security by Design" angewandt werden, der Security-Maßnahmen insbesondere zum Schutz personenbezogener Daten bereits in der Entwicklungsphase integriert.

Mögliche Gestaltungsoptionen

Um intelligente Reiseassistenten möglichst sicher und unter Einhaltung des Datenschutzes zu realisieren, schlägt das Autorenteam konkrete Gestaltungsmöglichkeiten vor, die verschiedene Akteure adressieren:

Nutzende von KI-Reiseassistenten sollten…

- Vorkehrungen treffen, um potenzielle Risiken hinsichtlich IT-Sicherheit und Datenschutz zu umgehen. Dies setzt einen reflektierten Umgang mit den eigenen Daten bei der Nutzung von intelligenten Reiseassistenten voraus („smart trust").
- bei der Auswahl des Anbieters von intelligenten Reiseassistenten sorgfältig vorgehen.
- Datenangaben gering halten. Es gilt: „Nur so viel wie nötig."
- Bereitschaft und Offenheit mitbringen, bestehende Informationsangebote zur Funktionsweise von KI-Systemen anzunehmen.

Plattformbetreiber sollten…

- als Verantwortliche für die Qualität des Angebots dafür Sorge tragen, dass ein adäquates Datenschutz- und IT-Sicherheitsniveau eingehalten werden. Dies schließt auch die teilnehmenden Mobilitätsanbieter mit ein.
- die Auswahl von teilnehmenden Mobilitätsanbietern bewusst und gezielt treffen.
- die Einhaltung der festgelegten Vorgaben regelmäßig überprüfen.
- regelmäßige Überprüfung der eigenen Angebote inklusive der Algorithmen durch dritte Stellen beauftragen.
- eigenverantwortlich ein hohes IT-Sicherheitsniveau anstreben.

Mobilitätsanbieter sollten…

- die Überprüfungen des eigenen Systems stets ermöglichen, um Seriosität gegenüber dem Plattformbetreiber deutlich zu machen.
- ein hohes IT-Sicherheitsniveau eigenverantwortlich anstreben.

Politische Entscheidungsträgerinnen und Entscheidungsträger sollten…

- die Anbieterpluralität von intelligenten Reiseassistenten fördern, um ein hohes Qualitätsniveau zu gewährleisten.
- Aufklärung im Umgang mit KI-Systemen und Funktionsweisen fördern und durch öffentliche Projekte, die der Wissenschaftskommunikation in Bezug auf Nutzende von KI-Systemen dienen, mitvorantreiben, um Nutzende in die Lage zu versetzen, digitale Regieassistenten „richtig" bedienen zu können.

Forschung und Entwicklung sollten…

- im Hinblick auf IT-Sicherheit Lösungsansätze für das Spannungsfeld Datensparsamkeit versus Usability entwickeln.
- erklärbare KI (explainable AI, kurz: XAI) fördern.

Zudem sind gesellschaftsrelevante Fragen, die in einem breiten gesellschaftlichen und politischen Diskurs gezielt diskutiert und beantwortet werden müssen, im Hinblick auf Teilhabe, Fairness, Verantwortlichkeiten etc. zu klären.

Intelligente, persönliche Reiseassistenten sind mit den Methoden der KI und des maschinellen Lernens schon sehr bald realisierbar und einsatzfähig. Mit dem vorliegenden Papier möchte das Expertenteam Orientierung geben, wie intelligente Reiseassistenten möglichst sicher und unter Einhaltung des Datenschutzes realisiert werden können. Wenn all die genannten 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.

Impressum
Herausgeber: Lernende Systeme – Die Plattform für Künstliche Intelligenz | Geschäftsstelle | c/o acatech | Karolinenplatz 4 | D-80333 München | kontakt@plattform-lernende-systeme.de | www.plattform-lernende-systeme.de |
Folgen Sie uns auf Twitter: @LernendeSysteme | Stand: Juni 2021 | Bildnachweis: Tempura/iStock/Titel

Diese Kurzfassung entstand auf Grundlage des Whitepapers *Mit KI sicher reisen – Datenmanagement und Datensicherheit bei KI-basierten Reiseassistenten,* München, 2021. Es wurde erstellt von Mitgliedern der Arbeitsgruppen IT-Sicherheit, Privacy, Recht und Ethik sowie Mobilität und intelligente Verkehrssysteme der Plattform Lernende Systeme. Die Originalfassung der Publikation ist online verfügbar unter: https://www.plattform-lernende-systeme.de/publikationen.html

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN