IKEM

Studie des Projekts EDDY (AP 1300)

Rechtsfragen der Datenökonomie – Empfehlungen aus der Stakeholderperspektive

19.08.2024

Im Auftrag des
Bundesministeriums für Digitales und Verkehr

Institut für Klimaschutz,
Energie und Mobilität e.V.

Rechtsfragen der Datenökonomie – Empfehlungen aus der Stakeholderperspektive

Diese Studie behandelt die rechtliche Einordnung von hochauflösenden, dynamischen Karten, die unter anderem zur unterstützenden Navigation von autonomen und automatisierten Fahrzeugen verwendet werden sollen. Die Karte, die Urban Dynamic Map (UDM), kann in ein intelligentes Verkehrssystem eingebettet werden. Die Studie fokussiert sich auf den Umgang mit Daten, die für den Betrieb einer solchen Karte (UDM) benötigt werden. Daten sind mangels Haftungsregelungen nicht verbindlich genug, damit Fahrzeuge nur mit der UDM betrieben werden können. (Öffentliche) Betreiber:innen einer UDM müssen insbesondere auf die Einhaltung der Grundrechte aller Verkehrsteilnehmenden, der Datenschutz-Grundverordnung und von Informationsauskunftsrechten achten. Durch den Betrieb einer UDM können Städte und Kommunen die Hoheit über die Verkehrsplanung zurückerlangen und dadurch gleichzeitig der Verkehrssicherheit und dem Umweltschutz dienen.

Studie zu Rechtsfragen der Datenökonomie, konsistente Handlungsempfehlungen aus der Stakeholderperspektive im Projekt „EDDY“ zu dem Arbeitspaket 1300

Zitiervorschlag

IKEM (2024): *Rechtsfragen der Datenökonomie – Empfehlungen aus der Stakeholderperspektive*: Studie des Projekts EDDY (AP 1300)

Autor:innen

Laura-Marie Schaudel
laura-marie.schaudel@ikem.de

Jane Emily von Grabe
jane.grabe@ikem.de

Lenia Linette Werner
lenia.werner@ikem.de

Matthias Hartwig
matthias.hartwig@ikem.de

Auftraggeber

Bundesministerium für Digitales und Verkehr

Förderhinweis

Diese Studie entstand im Rahmen des vom Bundesministerium für Verkehr und digitale Infrastruktur durch den „mFund“ geförderten Projekts „EDDY“.

Disclaimer

Für den Inhalt der Studie zeichnen sich die Studienautor:innen verantwortlich. Der Inhalt stellt nicht zwingend die Auffassung des Auftrag- oder Fördergebers dar.

Geschlechterneutrale Sprache

In dieser Studie wird, soweit möglich, eine geschlechterneutrale Sprache verwendet. In Fällen, in denen dies nicht möglich ist, wird der sogenannte „Gender-Doppelpunkt" verwendet (z.B. Expert:innen). Sofern es sich allerdings um die Wiedergabe von Werken und Gesetzestexten handelt, welche nur das generische Maskulinum verwenden, wird der Text in dieser Form wiedergegeben. Diese Quellen beziehen sich, sofern nicht anders kenntlich gemacht, auf alle Geschlechter.

Institut für Klimaschutz, Energie und Mobilität e.V.

Magazinstraße 15-16
10179 Berlin

+49 (0)30 408 1870 10
info@ikem.de

www.ikem.de

Inhaltsverzeichnis

1 Zusammenfassung und Allgemeines

1.1 Hinweise zur Nutzung des Gutachtens

Jedem Kapitel ist eine Zusammenfassung vorangestellt. Die Zusammenfassung konzentriert sich auf die Umsetzbarkeit technischer Fragen aus einer rechtlichen Perspektive. Eine genauere juristische Ausarbeitung der im Projekt aufgeworfenen Fragen findet sich in den jeweiligen Kapiteltexten. Wer vor allem technisch interessiert ist, kann die jeweiligen Kapitelzusammenfassungen lesen; wer sich für die rechtswissenschaftlichen Ausarbeitungen der Fragestellungen interessiert, liest die Kapitel selbst.

Die verwendeten Rechtsquellen sind auf dem Stand des 31. Juli 2024.

1.2 Projektbeschreibung EDDY

Hochaufgelöste, dynamische Karten bilden eine wichtige Voraussetzung für die weitere Optimierung des urbanen Verkehrs mit dem Ziel der Reduktion von Emissionen, dem Schutz von vulnerablen Verkehrsteilnehmer:innen, sowie der Ermöglichung höherer Stufen des automatisierten Fahrens. Bislang liegen diese in der Hoheit von großen Fahrzeughersteller:innen und Navigationsanbieter:innen. Städte und Kommunen als Verantwortliche des öffentlichen Verkehrsraums erfahren demnach einen Verlust der (Verkehrs-)Planungshoheit über die betriebene Infrastruktur.

Ziel des Projekts EDDY ist es, die Grundlagen zu liefern, damit Städte und Kommunen statische und dynamische Daten gemeinwohlorientiert und diskriminierungsfrei in einer Urban Dynamic Map (UDM) bereitstellen können. Die datenbasierte Einflussnahme kommunaler Bedarfsträger:innen auf das Verkehrsmanagement wird verbessert, und die Datensouveränität wird aufrechterhalten. Benötigte technische und rechtliche Vorgaben sowie einheitliche Standards werden den Akteuren in Gesetzgebung, Verwaltung und Wirtschaft bereitgestellt. Die UDM kann zukünftig auch Teil eines Entscheidungscockpits sein, welches Verkehrsmanagement in Echtzeit möglich macht.

In diesem Gutachten wird dargestellt, welche Rechtsfolgen eintreten, wenn der Aufbau einer UDM realisiert wird, mit dessen Hilfe auch autonome Fahrzeuge navigiert werden und damit die in EDDY entwickelten Systemelemente operativ eingesetzt werden. Der Fokus der Prüfungsperspektive liegt auf der Darstellung des geltenden (europäischen und nationalen) Rechtsrahmens und welche Maßnahmen aus rechtlicher Sicht eingehalten werden müssen, um die operative Umsetzung des Projekts zu ermöglichen.

Auf lange Sicht schafft EDDY damit eine geordnete und faire Basis für innovative Produkte und Dienstleistungen und unterbindet hierdurch langfristige schädliche Monopolstrukturen. Beteiligte kleine und mittelständische Unternehmen (KMUs) können neuartige, skalierbare Geschäftsmodelle entwickeln. Die Datensouveränität der kooperierenden europäischen Partnerstädte und Anwendungspartner wird gestärkt.

1.3 Kurzfassung des Gutachtens zu AP 1300

Ziel des AP 1300 ist es, rechtliche Handlungsempfehlungen für ein konkretes Betreibermodell zu entwickeln. Allerdings hat sich im Verlauf des Projekts abgezeichnet, dass es kein einheitliches Betriebsmodell für ein EDDY-System geben wird. Vielmehr ist die Ausgestaltung des Betriebs einer UDM von

der späteren Anwendung dieser abhängig. Die einzelnen Anwendungsfälle sind allerdings nicht Gegenstand des Projekts. Daher beinhaltet dieses Gutachten Handlungsempfehlungen, die für eine Vielzahl von Betreiber:innen relevant sind, unabhängig vom konkreten Betriebsmodell.

Dieses Gutachten beantwortet die Fragen, welche Pflichten und Anforderungen an Hersteller:innen und Betreiber:innen einer UDM gestellt werden. Dabei wird in den Blick genommen, wofür die UDM genutzt werden soll sowie ob und inwiefern dies rechtlich möglich ist. Weiterhin wird untersucht, wie mit den Daten, die für die UDM genutzt werden, umgegangen werden muss und welche Konsequenzen diese Ergebnisse für das Projekt EDDY haben.

Es werden erste rechtliche Handlungsempfehlungen an die Betreiber:innen der UDM ausgesprochen, so wie Handlungsmöglichkeiten für den Gesetzgeber aufgezeigt, um den Aufbau der UDM zu unterstützen. Diese sollen sicherstellen, dass die geplante UDM zu einem größtmöglichen Nutzen realisiert werden kann.

Um einen verfassungsmäßigen Schutz von besonders gefährdeten Verkehrsteilnehmenden (VRU) zu wahren, müssen Betreiber:innen und Hersteller:innen Maßnahmen zum Schutz von VRU konsequent bei der Entwicklung und dem Betrieb der UDM umsetzen. Der Zugang zur UDM sowie deren Ausgestaltung muss diskriminierungsfrei gegeben sein. Weiterhin müssen immer alle technisch möglichen Sicherheitsmaßnahmen genutzt werden, die zur Verfügung stehen.

Betreiber:innen der UDM müssen sich bewusst sein, dass die Daten der UDM nicht verlässlich genug sind, damit autonome und automatisierte Fahrzeuge nur mit Hilfe der UDM navigiert werden können. Für die inhaltliche Richtigkeit von Daten wird nicht gehaftet. Für Soft- und Hardware der UDM gilt das Produkthaftungsrecht hingegen. Daraus lässt sich in der Regel aber keine Haftung für die inhaltliche Richtigkeit der Daten ableiten. Solange keine entsprechende Rechtsgrundlage besteht, kann die öffentliche Hand auch nicht vertraglich die Haftung für die Richtigkeit der Daten übernehmen.

Die Daten der UDM können aber für andere Zwecke, vor allem von staatlichen Betreiber:innen, für verwaltungsinterne Anwendungen genutzt werden. Städte und Kommunen können so die Hoheit über die Verkehrsplanung zurückerlangen und ihr Verkehrsmanagement verbessern. Die Verwaltung kann durch die Datensätze in Entscheidungsprozessen unterstützt werden („IT-Legal-Enforcement-Support“). Um das Potenzial der UDM aber über eine verwaltungsinterne Anwendung hinaus zu etablieren, bedarf es einer Haftungsregelung für sicherheitsrelevante Daten.

Wenn personenbezogene Daten weitergegeben werden, müssen die Vorschriften der DS-GVO eingehalten werden. Solange natürliche Personen anhand der Daten (ggf. unter Zuhilfenahme weiterer Informationen) re-identifizierbar sind, liegt Personenbezug vor und die DS-GVO ist anwendbar. Sowohl Live-Standortdaten, Kamera- und LiDAR-Daten gelten als personenbezogen. Betreiber:innen müssen wirksam die Einwilligung zur Datenweitergabe der betroffenen Person einholen. Dies gilt insbesondere für die Weitergabe der erfassten Daten an Dritte, die andere Anwendungen zur Verkehrsoptimierung/-steuerung betreiben. Wenn möglich, sollte die Anwendbarkeit der DS-GVO umgangen werden (sonst folgen weitere Pflichten, z.B. Hinweispflicht). Dies ist möglich durch eine automatische Anonymisierung oder die Verwendung geschlossener Systeme, beides ist aber bei der Datenverarbeitung im Rahmen der UDM wohl nicht umsetzbar.

Der Landesgesetzgeber kann das Straßen- und Wegerecht so anpassen, dass der stationslose E-Roller-Verleih nicht unter den genehmigungsfreien Gemeingebrauch fällt. In einem Sondernutzungsvertrag kann dann die Erteilung der notwendigen Sondernutzungserlaubnis an die Pflicht zum Teilen von Daten des E-Scooter-Verleihers geknüpft werden.

Die UDM kann als digitale Karte in ein sog. „Intelligentes Verkehrssystem (IVS)“ eingebettet sein, ist selbst aber kein IVS. Sowohl IVS untereinander als auch die UDM als Teil eines IVS sollten mit anderen IVS interoperabel sein. Diese Interoperabilität ermöglicht es z. B. Verkehrsdaten effizient zu teilen, Verkehrsstaus zu meiden und komplexe Verkehrsmuster zu analysieren, um präzise Verkehrslenkung in Echtzeit zu ermöglichen. UDM-Betreiber:innen müssen sich regelmäßig informieren, ob die EU-Kommission neue Spezifikationen erlassen hat, die auch für sie relevant sind. Datenplattformen, wie der deutsche nationale Zugangspunkt, die „Mobilithek“, oder der noch im Aufbau befindliche European Mobility Data Space (EMDS), können von den Betreiber:innen der UDM genutzt werden, um auf eine Vielzahl von Datensätzen zuzugreifen und so die UDM zu optimieren.

Hersteller:innen und Betreiber:innen der UDM sind nicht verpflichtet, Daten an die „Mobilithek“ zu liefern, sind aber in Deutschland dazu aufgefordert eine Eigenerklärung gegenüber der Nationalen Stelle für Verkehrsdaten abzugeben (nur Kontrollpflicht, keine Datenlieferpflicht). Eine freiwillige Bereitstellung von Daten in der „Mobilithek“ und dem EMDS ist möglich.

Neben der Aufforderung zur Abgabe der Eigenerklärung unterliegen staatliche Betreiber:innen weiteren Informationspflichten. Sie sind gegebenenfalls verpflichtet, Daten diskriminierungsfrei (und ggf. anonymisiert) weiterzugeben. Dies gilt insbesondere, wenn die Betreiber:innen die Daten bereits an andere Stellen weitergegeben haben (Selbstbindung der Verwaltung aus Art. 3 Abs. 1 GG).

Die UDM ist keine kritische Infrastruktur. Die Betreiber:innen müssen nicht die Voraussetzungen der Cybersecurity-VO einhalten. Trotzdem ist empfohlen, mindestens „technisch-fehlerhafte“ Daten durch eine automatisierte Kontrolle vor Einspeisung in die UDM auszusortieren und den Anforderungen der DS-GVO nachzukommen.

Auch wenn der Betrieb einer UDM viele gesamtgesellschaftliche Vorteile bietet (besseres Verkehrsmanagement, weniger CO2- und Lärmemissionen, etc.), besteht keine Verpflichtung für Bund oder Länder eine UDM aufzubauen. Auch wenn die UDM, Stand jetzt, nicht allein für die automatisierte Navigation von Fahrzeugen genutzt werden kann, bietet sie andere Vorteile für staatliche Betreiber:innen. Insbesondere können diese so die kommunale Hoheit über die Verkehrsplanung zurückerlangen. Dies dient dem öffentlichen Interesse, insbesondere im Hinblick auf die Verkehrssicherheit und den Umweltschutz.

2 Verzeichnisse

2.1 Abkürzungsverzeichnis

Abs.	Absatz
AFGBV	Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung
Art.	Artikel
B2C	Business-to-Consumer (Unternehmer-zu-Verbraucher)
BayDSG	Bayerisches Datenschutzgesetz
BDSG	Bundesdatenschutzgesetz
BMDV	Bundeministerium für Digitales und Verkehr
BSI-KritisVO	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BVBS	Ehemals: Bundesministerium für Verkehr, Bau und Stadtentwicklung
bzw	beziehungsweise
C-IST	Cooperative Intelligent Transport-Systems, Teilmenge der IVS
CAM	Cooperative Awareness Message
CAV	Connected and Automated Vehicles
CPM	Collective Perception Messages
DA	Delegierter Rechtsakt
DNG	Datennutzungsgesetz
DS-GVO	Datenschutz-Grundverordnung
EMDS	European Mobility Data Space/Gemeinsamer Europäischer Mobilitätsdatenraum
ErwG	Erwägungsgrund
etc	Et cetera
EU	Europäische Union
ff.	folgende
GG	Grundgesetz
GNSS	Global Navigation Satellite System
HmbTG	Hamburgisches Transparenzgesetz
IP	Internet Protokoll
i.S.d.	im Sinne des
IFG	Informationsfreiheitsgesetz
ISO	International Organization for Standardization
i.S.v.	im Sinne von
IVS/ ITS	Intelligente Verkehrssysteme/Intelligent Transport Systems
KI	Künstliche Intelligenz
KMUs	Kleine und mittelständische Unternehmen
LDM	Local Dynamic Map
LiDAR	Light Detection and Ranging
Lit.	literae
MDM	Mobilitäts-Daten-Marktplatz
MDV	Mobilitätsdatenverordnung
NAP	National Access Points/Nationale Zugangspunkte
Nr.	Nummer
ODD	Operational Design Domain
OwiG	Gesetz über Ordnungswidrigkeiten
PBefG	Personenbeförderungsgesetz
ProdHaftG	Produkthaftungsgesetz

RSU	Road Side Unit
S.	Satz/Seite
sog.	Sogenannte
StGB	Strafgesetzbuch
u.A.	Unter Anderem
UDM	Urban Dynamic Map
V2X	Vehicle to Everyhting
Var.	Variante
Vgl.	Vergleiche
VRU	Vulnerable Road User
z. B.	Zum Beispiel

2.2 Abbildungsverzeichnis

3 Use Cases und rechtliche Würdigung

In diesem Kapitel werden unterschiedliche Use Cases aus der Betriebsperspektive dargestellt. Anschließend werden die rechtlichen Probleme und Fragestellungen, die sich in Bezug auf jeden Use Case stellen, herausgearbeitet und beantwortet. Der erste Use Case beschäftigt sich mit dem Schutz von vulnerablen Personen im Straßenverkehr. Der zweite Use Case setzt sich mit der zivilrechtlichen Haftung für Daten in der UDM auseinander. Besonderer Fokus liegt auf dem unionsrechtlich geprägten Produkthaftungsrecht. Im dritten Use Case geht es um die rechtmäßige Erhebung und Weitergabe von Mobilitätsdaten, insbesondere in Bezug auf die Nutzung von sog. „E-Scootern". Der vierte Use Case beleuchtet die Echtzeit-Analyse von Fahrzeugtrajektorien und die Umsetzung der Analyseerkenntnisse zur Optimierung des Verkehrsmanagements.

3.1 Use Case 1: Schutz vulnerabler Personen

In diesem Abschnitt wird der Umgang mit besonders gefährdeten Verkehrsteilnehmenden (VRU) aus rechtlicher Perspektive untersucht. VRU dürfen nicht aufgrund ihrer Vulnerabilität gegenüber Nicht-VRU diskriminiert werden. Das bedeutet, die im Straßenverkehr einem höheren Verletzungsrisiko ausgesetzte Gruppe der VRU darf nicht genauso (gleich) wie Nicht-VRU behandelt werden, die einem geringeren Schadensrisiko ausgesetzt sind. Daher werden durch Datenübertragungen VRU-Hotspots ermittelt und in der UDM gespeichert. Zu jeder Zeit müssen alle Verkehrsteilnehmenden durch die UDM den technisch-bestmöglichen Schutz erfahren. Connected und Non-Connected VRU werden rechtlich nicht unterschieden. Eine Diskriminierung der VRU darf weder durch die Fahrzeuge noch durch die UDM vorgenommen werden.

3.1.1 Sachverhalt

In dem geplanten EDDY-System[1] werden Collective Perception Messages (CPM)[2] über die Urban Dynamic Map (UDM) ausgetauscht. Die UDM dient in dieser Hinsicht zum einen als Relay-Station und zum anderen dazu, den Fahrzeugen, ein umfassenderes Gesamtbild zu bieten, als sich durch den direkten Austausch zweier oder auch mehrerer Fahrzeuge in Netzwerken zwischen Fahrzeugen erreichen ließe. Dies sieht konkret so aus, dass mehrere Fahrzeuge (A und B) und die Infrastruktur, Informationen **über die und mit der UDM** zu besonders gefährdeten Verkehrsteilnehmenden (engl. Vulnerable Road

[1] Ein eigenständiges abgeschlossenes System wird im Projekt EDDY nicht entwickelt, sondern vielmehr Systemelemente entwickelt. Der Bezug auf ein EDDY-System ist hier also im Sinne eines möglichen zukünftigen Intelligenten Verkehrssystems zu verstehen, das die im Projekt EDDY entwickelten und getesteten Systemelemente verwendet.

[2] Collective Perception Messages (CPM) ermöglichen die Weitergabe von Informationen über erkannte Objekte. Die Nachricht enthält die generischen Datenelemente zur Beschreibung der erkannten Objekte im Rahmen des Verkehrssystems, der UDM. Die CPM wird zyklisch mit adaptiver Nachrichtengenerierungsrate übertragen, der Schwerpunkt liegt auf der Meldung von Veränderungen in der dynamischen Straßenumgebung, vgl. https://www.etsi.org/deliver/etsi_tr/103500_103599/103562/02.01.01_60/tr_103562v020101p.pdf.

Users, VRU[3]) untereinander per ITS-G5[4] CPM (Schnittstelle) plus Mobilfunk austauschen und auf diese zugreifen können.[5]

Dadurch ist es insbesondere möglich, Standortinformationen zu den VRU, die im Sichtschatten der jeweiligen Fahrzeuge liegen, auszutauschen. Weil Fahrzeuge und Infrastrukturen auf die Informationen der UDM zugreifen können, können auch weiter von der gefährlichen Situation entfernte Fahrzeuge früher die notwendigen Informationen erhalten und bei der Planung ihres Bewegungspfades (Trajektorie) berücksichtigen, sodass sie notwendige Maßnahmen zum Schutz von VRU ergreifen können.

Die **notwendigen Maßnahmen** könnten wie folgt ausgestaltet sein:

- die vorsorgliche Reduzierung der Geschwindigkeit eines Fahrzeugs bei VRU in der „kritischen" Trajektorie (d.h. bei Kollisionsgefahr),
- Versetzung eines autonomen oder automatisierten Fahrzeugs in eine erhöhte Alarmbereitschaft und Fokus der Sensorik auf den kritischen Bereich, sobald in dessen Nähe,
- Versetzung anderer Fahrzeuge in der Umgebung von VRU in erhöhte Alarmbereitschaft,
- Senden eines Signals an VRU zur erhöhten Alarmbereitschaft, bei zahlenmäßig hohem VRU-Aufkommen in einem Bereich (sog. Hotspots), Anpassung der Routenplanung und Umfahrung des Bereichs.

Dabei sendet das UDM-System lediglich Daten über VRU aus und hat keinen Einfluss darauf, wie diese Daten durch die Verkehrsteilnehmenden und ihre IT-Systeme weiterverwendet werden.

In Bezug auf die Vernetzung von VRU an die UDM werden zwei Arten der VRU unterschieden: Connected und Non-Connected VRU. **Connected VRU** sind Verkehrsteilnehmer:innen, die über Technologien verfügen, um mit anderen Fahrzeugen und der Verkehrsinfrastruktur zu kommunizieren und Daten zu übermitteln. Sie zeichnen sich dadurch aus, dass die VRU durch die Versendung und den Empfang sog. CAM, Informationen über ihre Position und Geschwindigkeit erhalten kann. **Non-connected VRU** hingegen besitzen keinerlei geeignete Sensorik, Sende- oder Empfangsgeräte, um selbst an der Kommunikation teilhaben zu können. Sie können also zu ihrem Schutz nur passiv beitragen und sind daher bisher auf die "traditionellen" Sicherheitsmaßnahmen der Verkehrsinfrastruktur angewiesen. Die eben beschriebenen Vorgänge werden für Connected und Non-Connected VRU gleichsam durchgeführt. Connected VRU senden darüber hinaus noch eine CAM aus, die in der UDM wie die CPM eines zusätzlichen Sensors behandelt wird. Die CPM der Fahrzeuge und der Infrastruktur, die CAM der Connected-VRU, sowie die darin enthaltenen Objektinformationen, werden in der UDM gespeichert. Durch diese Datenübertragungen werden **Hotspots von VRU** ermittelt, indem die erkannten VRU-Objekte nach Erfüllung bestimmter Kriterien auf der UDM zusammengefasst werden. Diese Hotspots

---

[3] VRU sind „nicht motorisierte Verkehrsteilnehmer wie z. B. Fußgänger:innen und Fahrradfahrer:innen sowie Motorradfahrer:innen und Personen mit Behinderungen oder eingeschränkter Mobilität und eingeschränktem Orientierungssinn" (Art. 4 Nr. 7 IVS-Richtlinie).

[4] ITS-G5 ist ein technischer W-Lan Standard für die Fahrzeugvernetzung. Er ist der Standard für Konzepte wie die Vehicle-to-Everything- und Car-to-car-Kommunikation, vgl. https://www.elektronik-kompendium.de/sites/net/2407231.htm#:~:text=ITS%2DG5%20ist%20ein%20Standard,WLAN%2DSpezifikation%20IEEE%20802.11a.

[5] Um Anwendungen zu ermöglichen, die die Position von VRU lokalisieren, sollen zu den entsprechenden Objekten Zeitreihen gespeichert werden. Diese Zeitreihen sollen die Basis für eine Echtzeitkollisionsvorhersage bilden. Innovativ ist der Zugriff von Fahrzeugen und Infrastruktur auf die Daten aus der UDM. Dabei werden die CPM über 5G an den EDDY-Server gesendet und in der UDM in zweierlei Hinsicht gespeichert: Durch die Speicherung als CPM direkt und die separate Speicherung der Objekte aus der CPM-Objektliste können die CPM und/oder die Objekte auch von Fahrzeugen abgerufen werden, die außerhalb der Reichweite von ITS-G5 für einen direkten Austausch liegen.

werden dann als separate Objekte ebenfalls in der UDM gespeichert. Dies geschieht zusätzlich zur Weiterleitung einzelner VRU an den Daten-Broker, welche ebenfalls als einzelne Objekte enthalten bleiben. Parallel hierzu können Orte an denen VRU typischerweise vermehrt am Verkehr teilnehmen, wie in der Nähe von Schulen, Krankenhäusern oder stark frequentierten Fußgängerzonen, automatisch als Hotspots in die UDM eingespeist werden.

Intention der Technik/dieses Use Cases ist der (verbesserte) Schutz von VRU. Ziel der Technik ist, dass (1) **Informationen über den Standort von VRU vermittelt werden können.** Darüber hinaus können bereits auf der UDM die (2) **Objektinformationen der VRU auf Plausibilität geprüft, verglichen und zu Hotspots agglomeriert werden**. Die Kenntnis über die Historie einzelner VRU ermöglicht es, typisches (3) V**erhalten zu analysieren** und den Fahrzeugen als zusätzliche Information zur Verfügung zu stellen.

3.1.2 Diskriminierung von VRU

VRU dürfen gegenüber anderen Verkehrsteilnehmenden bei dem Design, der Ausgestaltung und dem Betrieb der UDM nicht diskriminiert werden.

Dieser Use Case ist vor allem in Bezug auf den Anwendungsfall der Steuerung von autonomen Fahrzeugen relevant. Generell muss im Straßenverkehr zwischen der Sicherheit und Leichtigkeit des Verkehrs immer eine optimale Fahrstrategie gefunden werden. Dabei müssen hoch-, vollautomatisierte und autonome Fahrzeuge jederzeit in der Lage sein, „den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen."[6] Die StVO[7] legt fest, dass „*wer ein Fahrzeug führt, muss sich gegenüber Kindern, hilfsbedürftigen und älteren Menschen, insbesondere durch die Verminderung der Fahrgeschwindigkeit und durch Bremsbereitschaft so verhalten, dass eine Gefährdung dieser Verkehrsteilnehmer ausgeschlossen ist."*[8] Da an ein automatisiertes Fahrzeug die gleichen Anforderungen zu stellen sind, müssen auch diese sich gegenüber den genannten Personen besonders sensibel verhalten. Doch auch an die UDM selbst sind konkrete Diskriminierungsverbote gegenüber VRU geknüpft, diese folgen in Bezug auf den Zugang zu einem solchen System, insbesondere aus den Regulierungen zur IVS[9] und in Bezug auf die Ausgestaltung aus Art. 3 Abs. 1 GG[10].

Das untenstehende Bild zeigt, wie ein autonomes Fahrzeug mithilfe von Kamera und LiDAR, VRU, wie Fußgänger:innen und Fahrradfahrende, erfasst.

[6] Vgl. §§ 1a Abs. 2 Nr. 2; 1e Abs. 2 Nr. 2 StVG.

[7] Straßenverkehrs-Ordnung vom 6. März 2013 (BGBl. I S. 367), die zuletzt durch Artikel 2 der Verordnung vom 28. August 2023 (BGBl. 2023 I Nr. 236) geändert worden ist.

[8] Vgl. § 3 Abs. 2a StVO.

[9] Genaueres zum Verhältnis von IVS und UDM kann in Kapitel 44 „Die UDM als Teil eines Intelligenten Verkehrssystem" gefunden werden.

[10] Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100- 1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2478) geändert worden ist.

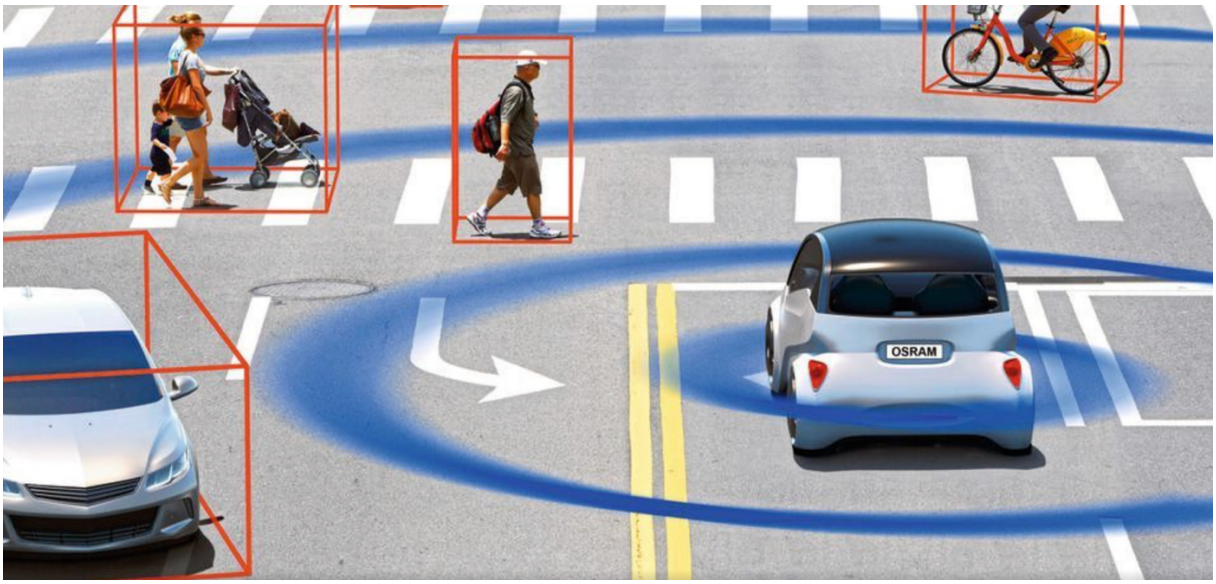

Abbildung 1: Der Verkehr soll mit (teil-)autonomen Fahrzeugen sicherer gestaltet werden.[11]

3.1.2.1 Verhältnis von IVSG und Art. 3 Abs. 1 GG

Die Grundrechte[12] von VRU müssen bei dem Betrieb einer UDM berücksichtigt werden. Einer Diskriminierung durch die UDM und deren Navigation muss vorgebeugt werden. Dies ist teilweise in der IVS-Richtlinie[13] verankert. Danach soll der gleichberechtigte Zugang von gefährdeten Verkehrsteilnehmenden zu IVS-Anwendungen und -Diensten gefördert und nicht verhindert werden. Maßnahmen sollen hinsichtlich des Zugangs Diskriminierung entgegenwirken.[14] Das bedeutet jedoch nicht, dass jedes Fahrzeug in IVS-Anwendungen berücksichtigt werden muss. Schließlich kann von Betreiber:innen nicht erwartet werden, jedes Fahrzeug mit der notwendigen Technologie auszustatten.

Die IVS-Richtlinie adressiert nur den diskriminierungsfreien Zugang zu IVS-Diensten. Nicht erfasst ist allerdings der diskriminierungsfreie Betrieb und die diskriminierungsfreie Entwicklung von IVS. Da die IVS-Richtlinie samt des IVSG[15] als einfaches Recht keine Vorgaben machen, kommt es vor allem auf Art. 3 Abs. 1 GG in Bezug auf die Diskriminierungsfreiheit an. **Der Schutzbereich für VRU der IVS-Richtlinie ist erheblich kleiner als der des Art. 3 Abs. 1 GG**, da Art. 3 Abs. 1 GG sich nicht nur auf einen diskriminierungsfreien Zugang beschränkt.

---

[11] Quelle Bild: Osram Opto Semiconductors, vgl. https://www.elektronikpraxis.de/lidar-und-die-sensorfusion-fuer-mehr-sicherheit-beim-autonomen-fahren-a-c888fb6d5c075c52b21599e3a76df390/ (zuletzt aufgerufen am 31. Juli 2024).

[12] Der Gesetzgeber der EU und ihre anderen Organe sind an die Charta der Grundrechte der Europäischen Union und der deutsche Gesetzgeber zusätzlich an die Grundrechte der deutschen Verfassung gebunden.

[13] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern; zuletzt geändert durch Richtlinie (EU) 2023/2661 des Europäischen Parlaments und des Rates vom 22. November 2023 zur Änderung der Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

[14] Vgl. Anhang II h) IVS-Richtlinie; Erwägungsgrund 11 IVS-Richtlinie.

[15] Intelligente Verkehrssysteme Gesetz vom 11. Juni 2013 (BGBl. I S. 1553), das zuletzt durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2640) geändert worden ist.

Art. 3 Abs. 1 GG ist allerdings **nicht in Bezug auf eine Schutzpflichtverletzung** der staatlichen Betreiber:innen betroffen. Es geht nicht um die Frage, ob der Betrieb einer UDM zum Schutz von VRU geboten ist. Vielmehr müssen alle Grundrechte bei dem Betrieb der UDM – gerade durch staatliche Betreiber:innen – geachtet werden. Dazu gehört auch, dass einzelne Verkehrsteilnehmende gegenüber anderen Verkehrsteilnehmenden nicht diskriminiert werden dürfen (vgl. Art. 3 Abs. 1 GG).

3.1.2.2 Achtung von Art. 3 Abs. 1 GG bei Betrieb der UDM

Insbesondere ist eine Diskriminierung zum einen zwischen Nicht-VRU und VRU möglich, aber auch zwischen Connected und Non-Connected VRU.

Die UDM wird durch staatliche Träger:innen betrieben. Daher sind bei dem Betrieb der UDM und deren Anwendung die Grundrechte zu achten, vgl. Art. 1 Abs. 3 GG.

Art. 3 Abs. 1 GG enthält den allgemeinsten Diskriminierungsschutz und setzt fest, dass alle Menschen vor dem Gesetz gleich sind. Art. 3 Abs. 1 GG verbietet die unterschiedliche Behandlung zweier vergleichbarer Sachverhalte und die Gleichbehandlung von wesentlich Ungleichem ohne sachlichen Grund.[16] Dazu sind Vergleichsgruppen zu bilden.[17] Vorliegend kommen als mögliche ungleiche Vergleichsgruppen Nicht-VRU und VRU, sowie Connected und Non-Connected VRU in Betracht. Wenn die ungleichen Vergleichspaare gleichbehandelt werden, liegt ein Verstoß gegen Art. 3 Abs. 1 GG vor.

Zwar sind sowohl **VRU als auch Nicht-VRU** beide Straßenverkehrsteilnehmende, allerdings ergeben sich im Hinblick auf die Sicherheit im Verkehr beider Gruppen erhebliche Unterschiede. VRUs sind im Straßenverkehr einem wesentlich höheren Verletzungs- und Tötungsrisiko ausgesetzt. Somit stellen Nicht-VRU und VRU wesentlich Ungleiches dar, welches nicht gleichbehandelt werden darf.

Im Projekt wurden einige Maßnahmen eingeführt, die eine Gleichbehandlung von VRU und anderen Verkehrsteilnehmenden innerhalb der UDM verhindern und so ein erhöhtes Schutzniveau für die VRU garantieren sollen.

Zwar werden die Trajektorien der VRUs nicht gesondert in der UDM dargestellt. Dennoch können die oben genannten Schutzmaßnahmen frühzeitig ergriffen werden, um VRUs zu schätzen. Außerdem können die angezeigten VRU-Hotspots umfahren werden und so das Risiko für die VRU reduziert werden.

Die Maßnahmen sind damit im Einklang mit den Vorgaben der Ethik-Kommission für automatisiertes und vernetztes Fahren, wonach die erhebliche Steigerung der Verkehrssicherheit das Ziel sein soll, und zwar bereits in der Auslegung und Programmierung (der Fahrzeuge) zu defensivem und vorausschauendem, schwächere Verkehrsteilnehmende (VRU) schonendem Fahren.[18] Die gleichen Programmierungsgrundsätze sind auf die UDM als Navigationsstruktur übertragbar. Die geplanten Maßnahmen setzen schon bei der Programmierung und Auslegung an. Es sind erhöhte Schutzmaßnahmen in Bezug auf VRU ergriffen worden, insbesondere im Vergleich zu Nicht-VRU.

Demnach werden Nicht-VRU und VRU im Projekt nicht gleichbehandelt. Infolgedessen liegt kein Verstoß gegen Art. 3 Abs. 1 GG vor, da Ungleiches nicht gleichbehandelt wird. Voraussetzung dafür ist jedoch, dass die oben genannten Maßnahmen konsequent schon bei der Programmierung, Auslegung

---

[16] BVerfGE 112, 268 (279); st. Rspr.

[17] Vgl. *Jarass* in Jarass/Pieroth, GG, Art. 3 Rn. 10.

[18] *Ethik-Kommission des BMVI*, Automatisiertes und vernetztes Fahren, Bericht Juni 2017, S. 10.

und der Anwendung der UDM ergriffen werden. Die geplanten Maßnahmen zum Schutz von VRU dürfen daher nicht vernachlässigt werden.

Connected und Non-Connected VRU stellen Untergruppen der VRU an sich dar. Hier ist schon fraglich, ob die beiden Untergruppen so verschieden sind, dass eine Vergleichbarkeit nicht gegeben ist. Vorliegend könnten Connected-VRU durch die Technologien Vorteile in Bezug auf ihre Sicherheit haben, da sie in Echtzeit sowohl Informationen über Gefahren erhalten als auch versenden können. Dadurch können sich autonome Fahrzeuge sowie die Verkehrsinfrastrukturen zunehmend auf die Bedürfnisse von Connected-VRU ausrichten. Non-Connected-VRU profitieren insoweit nur mittelbar aufgrund der gezogenen Lehren der Infrastrukturen aus dem Umgang mit Connected-VRU. Insoweit werden Connected-VRU gegenüber Non-Connected-VRU bevorteilt. Allerdings werden Grundrechtsträger:innen in ihren Gleichheitsgrundrecht nach Art. 3 Abs. 1 GG nur dann beeinträchtigt, wenn die (Un-)Gleichbehandlung zu einem Nachteil führt.[19] Da die Non-Connected-VRU ihre Daten nicht mit der UDM teilen können, sähe eine Gleichbehandlung beider Gruppen so aus, dass auch die Connected-VRU ihre Daten nicht mehr mit der UDM teilen dürften. Der Schutz von VRU insgesamt würde geschwächt werden. Damit ergibt sich kein Nachteil der Non-Connected, sodass ihnen aus der Gleichbehandlung per se kein Nachteil i. S. d. Art. 3 Abs. 1 GG entsteht. In Bezug auf Connected und Non-Connected VRU ist damit der Schutzbereich des Art. 3 Abs. 1 GG nicht beeinträchtigt.

3.1.2.3 Exkurs: Alarmmodus

In Bezug auf die Achtung der Grundrechte aller Verkehrsteilnehmenden führt der Alarmmodus zu Komplikationen. Die UDM selbst versetzt die Fahrzeuge nicht in den Alarmmodus, eine **solche Nutzung der UDM hängt von dem jeweiligen Anbieter ab.** Daher wird auf die Problematik des Alarmmodus nur in diesem Exkurs verwiesen.

Der Alarmmodus eines autonomen Fahrzeugs ist ein spezieller Betriebszustand, der (automatisch oder manuell) aktiviert wird, um die Sicherheitsmaßnahmen zu verstärken und das Fahrzeugverhalten anzupassen. So soll die Wahrscheinlichkeit von Unfällen oder gefährlichen Situationen minimiert werden und die Sicherheit in potenziell gefährlichen Situationen oder Umgebungen erhöht werden.

Wesentliche Merkmale und Funktionen des Alarmmodus stellen die Anpassung des Fahrverhaltens an die konkrete Situation, wie das Einhalten erweiterter Abstände und das Fahren mit reduzierter Geschwindigkeit und damit präventive Maßnahmen dar. Zudem kann die Sensibilität der Sensoren erhöht werden, um genauere und häufigere Überprüfungen der Umgebung durchzuführen. Weiter kommt es zu einer verstärkten Kommunikation des Fahrzeugs mit anderen Fahrzeugen und der Infrastruktur sowie der Datenerfassung und -analyse, um gegenwärtige und zukünftige Gefahren besser vorhersehen und vermeiden zu können.

Im Umkehrschluss bedeutet dies, dass autonome Fahrzeuge, wenn diese nicht im Alarmmodus fahren, Verkehrsteilnehmende schlechter schützen als ihnen technisch möglich wäre. Zwar kann der Alarmmodus helfen, VRU(-Hotspots) besser zu schützen, allerdings werden **andere Verkehrsteilnehmende**, die sich außerhalb der Hotspots bewegen, **strukturell und regelmäßig schlechter gestellt** als solche, die sich innerhalb der Hotspots bewegen. Insbesondere wenn die UDM durch die öffentliche Hand betrieben wird, müssen aus verfassungsrechtlicher Sicht alle technisch möglichen Maßnahmen ergriffen werden, die den höchstmöglichen Schutz aller Verkehrsteilnehmenden zu jeder Zeit garantieren.

---

[19] *Jarass* in Jarass/Pieroth, GG, Art. 3 Rn. 14.

Dass die mit der UDM navigierten Fahrzeuge, wenn sie nicht im Alarmmodus operieren, die Verkehrsteilnehmenden weniger schützen als sie technisch könnten, ist nicht mit den Grundrechten der Verkehrsteilnehmenden vereinbar. Berührt sein können insbesondere Art. 1 Abs. 1, Art. 2 Abs. 2 und Art. 3 Abs. 1 GG. Die Fahrzeuge müssen demnach grundsätzlich **immer alle technischen Mittel nutzen, die sie im Alarmmodus nutzen**, um ihre Anwendung so sicher wie (technisch) möglich zu machen. Insoweit scheidet eine Rechtfertigung des Schutzbereichseingriffs in Art. 2 Abs. 2 GG, sowie der Ungleichbehandlung nach Art. 3 Abs. 1 GG aufgrund eines unterschiedlichen Risikoprofils in und außerhalb von VRU-Hotspots aus.

Aus verfassungsrechtlicher Sicht ist es zwar nicht notwendig, alle Risiken für Leben und körperliche Unversehrtheit vollständig auszuschließen. So erlaubt Art. 2 Abs. 2 S. 3 GG Eingriffe in diese Schutzgüter durch Gesetz. Verbleibende Risiken müssen somit minimiert werden, es ist aber nicht erforderlich, die Möglichkeit zukünftiger Schäden vollständig auszuschließen.[20] Insbesondere wäre ein absoluter Risikoausschluss nur durch ein vollständiges Verbot des autonomen Fahrens möglich. Zudem birgt der automobile Straßenverkehr allgemein ein großes Risiko für die Schutzgüter Leben und körperliche Unversehrtheit, wird aber aufgrund seiner Bedeutung für Mobilität und Gesellschaft als Lebensrealität akzeptiert.

Allerdings handeln Fahrzeuge, die in Risikogebieten wie VRU-Hotspots strengere Sicherheitsvorkehrungen treffen, insoweit unverhältnismäßig, als sie außerhalb dieser Hotspots hinter den möglichen Sicherungsmöglichkeiten bewusst zurückbleiben. Eine Anpassung des Fahrverhaltens an das jeweilige Risikoniveau ist zwar grundsätzlich zu fordern, eine bewusste Erhöhung des Risikos für andere Verkehrsteilnehmer durch vorsätzliches Zurückbleiben hinter den technischen Fähigkeiten, stellt aber gerade keine derartige Anpassung dar. So könnten autonome Fahrzeuge, anders als Menschen, theoretisch immer ihre vollen technischen Möglichkeiten ausschöpfen, um die Sicherheit aller Verkehrsteilnehmer:innen zu maximieren. Ein bewusstes Zurückhalten der Sicherheitsmaßnahmen außerhalb von VRU-Hotspots kann daher nicht gerechtfertigt werden. Insbesondere tragen auch autonome Fahrzeuge die ethische Verantwortung, die größtmögliche Sicherheit für Verkehrsteilnehmer:innen zu garantieren. Existieren Technologien, die Leben retten oder schwere Verletzungen verhindern könnten, sind diese, unabhängig vom Risikoniveau des Standorts, zu nutzen.

Aus eben dieser Argumentation heraus kann keine Rechtfertigung der Ungleichbehandlung von Verkehrsteilnehmer:innen in und außerhalb VRU-Hotspots durch einen sachlichen Grund i. S. d. Art. 3 Abs. 1 GG erfolgen. Genießen Verkehrsteilnehmer:innen außerhalb von VRU-Hotspots nicht denselben Schutz, wie jene innerhalb, stellt dies eine unzulässige Ungleichbehandlung dar. Der Annahme, dass außerhalb von Hotspots ein geringeres Risiko besteht, und lediglich eine Anpassung des Fahrverhaltens an die konkrete Risikosituation besteht, kann insoweit nicht gefolgt werden, da gerade das bewusste Zurückbleiben des Fahrzeugs hinter den technischen Möglichkeiten zu einer Erhöhung des Risikos für die Verkehrsteilnehmer:innen führt.

Als Konsequenz müsste der Alarmmodus dauerhaft aktiviert sein, oder es dürfte einen solchen Alarmmodus gar nicht geben, da stets alle technischen Funktionen zur Risikominimierung genutzt werden müssen. Diese Verpflichtung gilt besonders dann, wenn der oder die Anbieter:in ein öffentlicher Hoheitsträger ist, da diese:r im Rahmen der staatlichen Schutzpflichten nach Art. 1 Abs. 1, 2 Abs. 2 GG und Art. 3 Abs. GG gehalten ist, die körperliche Unversehrtheit und das Leben der Bürger:innen zu schützen und Ungleichbehandlungen zu unterlassen. Eine Reduktion der technisch möglichen Schutzmaßnahmen außerhalb von Hotspots widerspricht diesem Schutzauftrag. Zudem hat der Staat sicherzustellen, dass private Anbieter:innen die Grundrechte der Bürger nicht verletzen. Dies erfolgt im

[20] Schulz: NZV 2017, 548 (550).

Rahmen der mittelbaren Drittwirkung der Grundrechte[21], wonach Grundrechte bei der Auslegung und Anwendung des einfachen Rechts u.U. berücksichtigt werden müssen. In diesem Zusammenhang könnte der Staat private Anbieter:innen verpflichten, dass ihre Fahrzeuge während der Fahrt dauerhaft ihre vollen technischen Möglichkeiten ausschöpfen und somit konstant im Modus maximaler Sicherheit, dem "Alarmmodus", navigieren.

3.1.2.4 Exkurs: Diskriminierende Quelldaten

Staatliche Betreiber:innen haben für einen diskriminierungsfreien Betrieb der UDM zu sorgen, um die Grundrechte aller Verkehrsteilnehmenden zu wahren. Eine Diskriminierung kann sich auch daraus ergeben, dass die in die UDM eingespeisten Quelldaten selbst diskriminierend sind, z. B. indem bestimmte Gruppen unterrepräsentiert werden oder systematische Vorurteile verarbeiten. Staatliche Betreiber:innen geben Verantwortung nicht ab, indem sie die UDM mit externen Daten betreiben. Durch die Auswahl der Datenquellen tragen die Betreiber:innen eine Mitverantwortung über die Auswahl der Quellen. Die staatlichen Betreiber:innen müssen in dieser Hinsicht sensibilisiert sein und dies bei der Auswahl der Datenquellen berücksichtigen. Insbesondere, wenn sich bei dem Betrieb der UDM zeigt, dass eine Datenquelle regelmäßig diskriminierende Daten einspeist, müssen die Betreiber:innen die Einspeisung dieser Daten unterbinden. Dabei ist Diskriminierung jeglicher Art vorzubeugen, nicht nur von VRU.

3.1.3 Datenschutzrechtliche Einordnung

Das Projekt EDDY befasst sich nur mit der Gestaltung der UDM, nicht direkt jedoch der Nutzung der UDM. Wie genau die UDM genutzt wird, hängt von den Anwender:innen selbst ab. Die Daten, die in der UDM verwendet werden, müssen allerdings ihrerseits rechtmäßig erhoben worden sein. In dem folgenden Abschnitt werden daher die datenschutzrechtlichen Grundlagen dargestellt und ihre Relevanz für das Projekt EDDY aufgezeigt.

3.1.3.1 Anwendbarkeit des Datenschutzrechts

Die VRU werden durch Kamera und LiDAR erfasst. Geplant ist, ihre Trajektorie in Form von Live-Standorten in der UDM zur Verfügung zu stellen. Der nächste Abschnitt zeigt auf, welche dieser Technologien in den Anwendungsbereich des Datenschutzrechts fallen.

3.1.3.1.1 Kamera

Da die Projektfahrzeuge mit Kameras ausgestattet werden sollen, müssen die Vorgaben der DS-GVO erfüllt werden, wenn es sich bei den erfassten Daten um personenbezogene Daten i.S.d. Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO)[22] handelt und diese i.S.d. Art. 4 Nr. 2 DS-GVO verarbeitet werden.

Für die Beurteilung, ob personenbezogene Daten vorliegen, kommt es darauf an, ob eine Identifizierung einer natürlichen Person nach den Umständen des Einzelfalles möglich ist. Ein Foto, welches mit

[21] BVerfG, Beschluss vom 18.07.2025 - 1 BvQ 25/15, 6.

[22] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

GPS-Daten verbunden ist, die mit den Bilddaten gespeichert werden und eine Lokalisierung ermöglichen, gelten als personenbezogene Daten.[23]

Die Kameras erfassen grundsätzlich physische, physiologische, genetische, soziale und kulturelle Merkmale. Mit Hilfe der Standortdaten ist ein Rückschluss auf eine bestimmte natürliche Person möglich. Demnach handelt es sich bei den erfassten Daten um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO.

Diese Daten werden auch i. S. d. Art. 4 Nr. 2 DS-GVO verarbeitet. Denn eine Verarbeitung im Sinne der DS-GVO ist ein mit oder ohne Hilfe automatisierter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (z. B. Speicherung, Erhebung oder Übermittlung von personenbezogenen Daten).[24] Die Verarbeitung erfolgt durch Erhebung der personenbezogenen Daten durch kontinuierliche Erfassung per Kamera, sowie der Reaktion des autonomen Fahrzeugs auf die mittels Kamera erfassten Verkehrssituation in Form verkehrserheblicher Vorgänge.

Damit findet die DS-GVO mitsamt ihren Pflichten für die Verarbeiter:innen und Rechte für die Betroffenen im Falle einer Verarbeitung der Daten i. S. d. Art. 4 Nr. 2 DS-GVO Anwendung. Die Anwendbarkeit der DS-GVO könnte nur ausgeschlossen werden, wenn die Kamera-Daten sofort durch Blurring unkenntlich und damit anonymisiert werden. So wäre keine Identifizierbarkeit der natürlichen Personen gegeben, weshalb keine personenbezogenen Daten i. S. d. Art. 4 Nr. 2 DS-GVO verarbeitet werden. Dies ist im Projekt aber nicht der Fall, da kein sofortiges Blurren stattfindet.

Etwas anderes kann gelten, wenn die Datenverarbeitungen durch eine **öffentliche Stelle** durchgeführt werden. Dies kann beispielsweise durch Ausbau der Straßeninfrastruktur mit Kameras etc. zur öffentlichen Erfassung der Verkehrssituation erfolgen. In diesem Fall kann § 4 Bundesdatenschutzgesetz (BDSG)[25] als spezielles nationales Recht hinsichtlich der Videoüberwachung öffentlich zugänglicher Räume durch öffentliche Stellen Vorrang vor der europarechtlichen DS-GVO haben. Dieser Vorrang greift vor allem ein, wenn keine personenbezogenen Daten erhoben werden und damit der Anwendungsbereich der DS-GVO nach Art. 4 DS-GVO nicht eröffnet wird.[26] Denn § 4 BDSG gilt auch für Videoüberwachungen, auf denen Personen nicht identifiziert oder identifizierbar sind.[27] Insoweit besteht ein Unterschied zwischen der Videoüberwachung durch private und öffentliche Stellen, welcher jedoch nur in seltenen Fällen relevant wird. So werden durch die mögliche Erfassung von Gesichtern bzw. Kfz-Kennzeichen Daten per Kameraaufzeichnung erfasst, welche Rückschlüsse auf eine natürliche Person und daher die Identifizierung der Personen grundsätzlich ermöglichen. Der gegenüber Art. 6 DS-GVO erweiterte Anwendungsbereich des § 4 BDSG ist damit gering.

Zudem findet § 4 BDSG keine Anwendung, wenn sensible personenbezogene Daten i. S. d. Art. 9 Abs. 1 DS-GVO erhoben werden. Nur in Einzelfällen kann auf die Landesdatenschutzgesetze zurückgegriffen werden, um eine Videoüberwachung zu rechtfertigen, z. B. § 24 Abs. 1 Nr. 1 BayDSG i. V. m. Art. 9 Abs. 2 lit. g) DS-GVO.[28] Da bei fast jeder Videoüberwachung sensible Daten erfasst werden, ist der

---

[23] *Schild* in Wolff/Brink: BeckOK Datenschutzrecht, Art. 4 DS-GVO, Rn. 14.

[24] Vgl. Art. 4 Nr. 2 DS-GVO.

[25] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 414) geändert worden ist.

[26] *Marsch*, in: Sydow/Marsch, DSGVO/BDSG, 3. Auflage 2022, § 4 BDSG Rn. 6.

[27] *Jandt*, ZRP 2018, 16 (17).

[28] *Reuter*, ZD 2018, 564 (568).

Anwendungsbereich von § 4 BDSG im Ergebnis stark eingeschränkt, sodass Art. 9 DS-GVO Vorrang genießt.[29]

3.1.3.1.2 LiDAR

Weiterhin soll das Projektfahrzeug mithilfe von LiDAR-Sensorik navigiert werden. Dafür müssten auch durch die LiDAR-Sensorik personenbezogene Daten i.S.d. Art. 4 Nr. 2 DS-GVO erhoben werden.

Das durch LiDAR erstellte Punktwolkenbild der Umwelt erfasst auch Menschen. Allerdings sind diese (Sach-)Daten für die menschliche Wahrnehmung nicht erkennbar. Auch ein eingesetzter Algorithmus ist nicht in der Lage, basierend allein auf dieser Datenlage die abgebildete Person zu identifizieren.[30] Durch die Punktwolken-Lokalisierung können damit grundsätzlich keine Bildaufnahmen von Personen erstellt werden. Eine (mittelbare) Identifizierbarkeit ist demnach anders als bei dem Einsatz von Kameras nicht gegeben. Demnach werden keine personenbezogenen Daten erhoben und die DS-GVO ist nicht anwendbar.

Sobald die per LiDAR erhobenen Daten aber nicht mehr isoliert verarbeitet werden, sondern in Bezug zu Datensätzen gesetzt werden, anhand derer eine natürliche Person identifizierbar ist, können auch diese Sachdaten rechtlich personenbezogene Daten darstellen.[31]

Unklar ist, ob LiDAR oder ähnliche Systeme § 4 BDSG unterfallen. Der Wortlaut bezieht sich zwar ausdrücklich auf Videoüberwachung. Nach der Definition des Begriffs „optisch-elektronische Einrichtung" müssten jedoch alle Verfahren erfasst sein, die Licht in elektronische Signale umwandeln.[32] Da LiDAR-Systeme Lichtstrahlen in Form von Lasern verwenden, um mittels Sensoren Umrisse und Formen ihrer Umgebung darzustellen, nutzen sie ein entsprechendes Verfahren, auch wenn keine klassischen Bilder geliefert werden. Es besteht zudem die Möglichkeit, Personen mithilfe der erstellten Daten zu identifizieren, sodass betroffene Personen ein Schutzbedürfnis gegen diese Technologie haben. Allerdings dient LiDAR im Vergleich zur Erfassung der Umgebung mit Kameras, vermehrt der räumlichen Orientierung und Objekterkennung. Daher muss aufgrund des eindeutigen Wortlauts der Vorschrift daran gezweifelt werden, dass die Gesetzgebung Lidar-Systeme mit § 4 BDSG regulieren wollte.

3.1.3.1.3 CAM

Durch CAM werden Statusinformationen der Verkehrsteilnehmenden versendet und umfassen Echtzeit-Informationen über Position, Identifikation, Zeitpunkt und Bewegungsstatus des:r Versender:in. Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Da durch CAMs, Informationen über die Position und andere relevante Daten der VRU versendet werden, ist ein derartiger Personenbezug anzunehmen.

Auch wenn die CAM der VRU eindeutig, aber pseudonym i.S.d. Art. 4 Nr. 5 DS-GVO sein sollten, wäre zumindest ein Tracking einzelner VRU möglich. Kann insoweit nicht sichergestellt werden, dass sich hieraus keine personenbezogenen Daten ableiten lassen (vgl. pseudonymes Tracking von Internetnutzern für Werbezwecke o.ä.), ist der Anwendungsbereich des Art. 4 Nr. 1 DS-GVO eröffnet.

---

[29] *Reuter*, ZD 2018, 564 (567).

[30] *Stoklas/Wendt*, Das vernetzte und autonome Fahrzeug, Gutachten im Rahmen des ABIDA Projekts, S. 18.

[31] *Stoklas/Wendt*, Das vernetzte und autonome Fahrzeug, Gutachten im Rahmen des ABIDA Projekts, S. 18.

[32] *Starnecker*, in: Gola/Heckmann, DS-GVO/BDSG, 3. Auflage 2022, § 4 BDSG Rn. 22; *Wilhelm-Robertson*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 46. Ed. Stand: 01.11.2021, § 4 BDSG Rn. 4.

Zudem werden diese Daten gem. Art. 4 Nr. 2 DSGVO verarbeitet. Diese Verarbeitung könnte im Kontext des autonomen Fahrens durch den Empfänger, ein autonomes Fahrzeug oder die Verkehrsinfrastruktur, verschiedene Formen annehmen. So empfängt das Empfangsgerät die CAM der VRU. Zudem könnten diese empfangenen CAM möglicherweise vorübergehend oder dauerhaft gespeichert werden, um eine Analyse der Daten zwecks Bewertung der Situation und potenzieller Risiken im Umfeld des Fahrzeugs durchzuführen. Weiter können die empfangenen CAM-Daten verwendet werden, um Entscheidungen zu treffen, z. B. hinsichtlich der Geschwindigkeitsanpassung oder Durchführung bestimmter Fahrmanöver, um sicher mit anderen Verkehrsteilnehmern zu interagieren.

Damit ist das Datenschutzrecht auch auf CAM anzuwenden.

3.1.3.2 Möglichkeiten zur Abwendung datenschutzrechtlicher Verpflichtungen

Wenn möglich sollten Fahrzeuge, die Datenerhebung nutzen, die Anwendbarkeit der DS-GVO umgehen, um einen effizienten Betrieb zu ermöglichen (weniger administrativer und organisatorischer Aufwand). Dies ist insbesondere bei geschlossenen Systemen oder automatischer Anonymisierung möglich. Allerdings ist die Umsetzbarkeit im Hinblick auf VRU fraglich.

3.1.3.2.1 Geschlossene Systeme

Eine technische Vorkehrung, mit der die Anwendbarkeit der DS-GVO komplett ausgeschlossen wird, ist das sog. geschlossene System (Englisch: „closed-loop-system“). Diese Systeme zeichnen sich dadurch aus, dass Daten in einer Weise verarbeitet werden, bei der sich die Auswertung darauf beschränkt, eine Person als Mensch ohne individuelle Eigenschaften zu identifizieren, um z. B. eine Notbremsung einzuleiten oder Verkehrszeichen zu erkennen.[33] Hierdurch kommt es lediglich zur Identifizierung eines Objekts als Mensch ohne weitere Spezifizierung, sodass keine Personenbezogenheit i. S. d. Art. 4 Nr. 1 DS-GVO besteht. Dafür werden die Daten innerhalb des Systems technisch gesichert und nach der Verwendung gelöscht.[34] Möglich ist nur die Aggregierung und Kategorisierung von Daten innerhalb des Systems mit einer anschließenden Weitergabe dieses Outputs zwecks unmittelbarer Reaktion und Gefahrvermeidung.

Im vorliegenden Use-Case 1 ist eine Umgehung der Anwendbarkeit der DS-GVO durch die Anwendung eines geschlossenen Systems allerdings gerade nicht möglich.

Dies liegt daran, dass die Identifizierung von VRU-Hotspots nicht nur eine Momentaufnahme erfordert, auf welche das Fahrzeug reagiert, sondern eine dauerhafte Datensammlung. Um Hotspots zu identifizieren, müssen Positionsdaten und Bewegungsmuster über einen längeren Zeitraum gesammelt und analysiert werden. Nur so können Gebiete mit vermehrtem Verkehr von VRUs identifiziert werden. Darüber hinaus geht die Verarbeitung der Daten von VRUs über die bloße Identifizierung eines Objekts als Mensch hinaus. Um die besondere Vulnerabilität dieser Personen zu erkennen und das Fahrverhalten entsprechend anzupassen, müssen zusätzliche Informationen verarbeitet werden. Dies umfasst möglicherweise sogar sensible personenbezogene Daten wie Gesundheitsinformationen, die weit über die bloße Identifizierung eines Objekts als Mensch hinausgehen. Derartige Identifikatoren könnten das Alter der Verkehrsteilnehmer:innen oder etwaige Mobilitätseinschränkungen wie die Nutzung von Rollstühlen darstellen. Diese Daten können potenziell zur Identifizierung von Personen führen und erfordern daher die Einhaltung der DS-GVO.

---

[33] *Schröder*, ZD 2021, 302 (304).

[34] Dazu am Bsp. der "Dash-Cam”: *Schröder*, ZD 2021, 302 (305).

Die einzige Situation, in der die Anwendbarkeit der DS-GVO möglicherweise ausgeschlossen werden könnte, ist, wenn die Daten ausschließlich für die unmittelbare Entscheidungsfindung des Fahrzeugs verwendet werden. Dies beschränkt sich aber auf die bloße Identifizierung eines Objekts als Verkehrsteilnehmer:in, auf welchen das Fahrzeug konkret und unmittelbar zu reagieren hat. Im Rahmen des Use-Case 1 ist dies jedoch nicht zielführend.

3.1.3.2.2 (Automatische) Anonymisierung

Daten werden automatisch anonymisiert, wenn sie unkenntlich gemacht werden, noch bevor sie den elektronischen Sensor verlassen, der die Daten erhebt, Art. 4 Nr. 5 DS-GVO.[35] Die Daten müssen insoweit unkenntlich gemacht bzw. entfernt werden, als Identifikatoren bestehen, die eine Rückverfolgbarkeit der Daten auf eine Person ermöglichen. Diese Technologie lässt den Personenbezug entfallen, wenn keine Rückgängigmachung der Anonymisierung möglich ist.[36]

Die Beurteilung, ob die Anonymisierung rückgängig gemacht werden kann, erfolgt anhand eines risikobasierten Ansatzes. So ist keine absolute Anonymisierung erforderlich, um den Anwendungsbereich der DS-GVO zu verlassen. Ein vernachlässigbares Restrisiko ist unschädlich.[37] Es ist aufgrund von ErwG 26 S. 4 DS-GVO jedoch regelmäßig zu überprüfen, ob infolge des technischen Fortschritts eine Re-Identifikation möglich geworden ist.[38] Anonymisierungsverfahren sollten daher eine „Schutzreserve" beinhalten, die zukünftigen Risiken vorbeugt.[39]

Vorliegend könnte problematisch sein, dass eine Bewertung der durch das Fahrzeug erfassten Daten insoweit erfolgen muss, um den VRU-Status der erfassten Personen zu identifizieren, bevor die Daten anonymisiert werden können. Diese Bewertung könnte potenziell personenbezogene Informationen enthalten, die besonders schützenswert sind.

Damit lässt sich die einzelne Erkennung und konkrete Reaktion auf VRU durch das Fahrzeug bei einer Anonymisierung der Daten nicht konkret umsetzen. Zudem muss die Anonymisierung der Hinderniserkennung vorgeschaltet werden, wodurch die Sensordaten verfremdet werden. Es besteht damit die Gefahr eines Eingriffs des Anonymisierungssystem in sicherheitsrelevante Prozesse.[40]

Um dennoch eine Anonymisierung der Daten zu gewährleisten ist eine Datenaggregation durchzuführen, durch welche auf lokaler Ebene Datensummen gebildet werden und lediglich die aggregierten Ergebnisse an das Fahrzeug und die UDM übermittelt werden. Sofern die Datensummen groß genug sind, ist die Zuordnung an einzelne Person zunehmend erschwert.[41]

So wird durch die Aggregation von Daten hinsichtlich VRU die Identifizierung allgemeiner Trends und Hotspots möglich, ohne dass einzelne Personen identifiziert werden können bzw. müssen. Spezifische Standorte oder individuelle Bewegungsprofile einzelner VRU werden dadurch derart anonymisiert, dass eine Identifizierung der dahinterstehenden Person nicht bzw. nur erschwert möglich wird. Dies

---

[35] *Volkmann/Feiten/Zimmermann/Sester/Wehle/Becker*, Digitale Tarnkappe: Anonymisierung in Videoaufnahmen. Informatik 2016, S.1.

[36] DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, Stand 17.7.2020, S. 5.

[37] EuG, Urteil vom 26. April 2023, T-557/20, ZD 2023, 399 (404).

[38] *Roßnagel*, ZD 2018, 243 (247); *Klabunde*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 4, Rn. 20.

[39] *Schaar*, ZD 2016, 224 (225).

[40] *Hofmann,* ZD 2023, 18 (18).

[41] *Seufert*, ZD 2023, 256 (260).

reduziert das Risiko, dass personenbezogene Daten offengelegt werden und stellt sicher, dass die gesammelten Informationen nur für statistische und analytische Zwecke im Rahmen der UDM genutzt werden.

Durch Einspeisung der aggregierten und hierdurch mitunter anonymisierten Daten wird ermöglicht, dass die UDM anhand der gesammelten Informationen wächst, ohne dass personenbezogene Daten unbefugt offengelegt werden.

3.1.3.3 Rechtmäßigkeit der Verarbeitung

Sollte eine Anwendung der obigen Systeme nicht möglich sein, ist die Verarbeitung und Speicherung der personenbezogenen Daten durch die Behörde nur aufgrund einer rechtlichen Grundlage möglich. Die Verarbeitung personenbezogener Daten ist dann nur rechtmäßig, wenn ein Rechtfertigungsgrund gem. Art. 6 DS-GVO vorliegt. Bei Wahrnehmung öffentlicher Aufgaben, findet Art. 6 UAbs. 1 lit. e DS-GVO Anwendung, jedoch handelt es sich hierbei nach Ansicht des Gesetzgebers und Teilen der Literatur nicht um einen eigenständigen Erlaubnistatbestand für die Verarbeitung von Daten, sondern um eine klarstellende Einstiegsnorm.[42] Als konkrete Grundlage für die Datenverarbeitung hat der deutsche Gesetzgeber eine sehr allgemeine Erlaubnisnorm zugunsten öffentlicher Stellen, nämlich § 3 BDSG geschaffen. Die weite Generalklausel dient nur als Rechtfertigung für Eingriffe von geringer Intensität und ist begrenzt durch das Bestimmtheits- und Verhältnismäßigkeitsgebot, insbesondere steht sie unter dem Vorbehalt der Erforderlichkeit.[43]

§ 4 BDSG ist jedoch spezieller als § 3 BDSG. So regelt § 4 BDSG spezifisch die Videoüberwachung, und wird damit im Zusammenhang mit VRU-Daten relevant, welche mithilfe der Kameras an autonomen Fahrzeugen gesammelt werden.

Private Unternehmen und andere nicht öffentliche Stellen, die von einer Behörde mit der hoheitlichen Aufgabe der öffentlichen Verwaltung betraut werden, also Beliehene, gelten im Sinne der DS-GVO, nämlich gem. § 2 Abs. 4 S. 2 BDSG, auch als öffentliche Stellen. Die öffentliche Stelle muss für die Aufgabe, für die sie Daten verarbeitet, zuständig sein und die Aufgabenerfüllung muss rechtmäßig sein.[44]

Als öffentliche Aufgabe i. S. d Art. 6 Abs. 1 S. 1 lit. e DS-GVO wird insbesondere die Auswertung und Verarbeitung personenbezogener Daten durch Polizei und Rettungsdienste angesehen, damit diese in Notfallsituationen eingreifen können. Der konkrete Use-Case 1 der Lokalisierung von VRU und VRU-Hotspots ist jedoch keine derartige Notfallsituation, welche unmittelbaren Handlungsbedarf verlangt. Allerdings kann die Verarbeitung von VRU-Daten zur Identifikation von Hotspots und damit der Verbesserung der Verkehrssicherheit als öffentliches Interesse angesehen werden. Dies wird dadurch verstärkt, dass die Maßnahmen zur Prävention von Unfällen und dem Schutz von Verkehrsteilnehmern sowie VRU dienen. Eine Aufgabenwahrnehmung innerhalb des öffentlichen Interesses bzw. öffentlicher Gewalt erfolgt damit durch öffentliche Stellen oder durch private Unternehmen, die im Rahmen hoheitlicher Aufgaben handeln.

Als weiterer möglicher Rechtfertigungsgrund für die Datenerfassung kann neben der Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DS-GVO zudem Art. 6 Abs. 1 S. 1 lit. f DS-GVO relevant werden. Nach Art. 6 Abs. 1 S.1 lit. f DS-GVO ist eine Datenverarbeitung rechtmäßig, soweit sie zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist und keine überwiegenden Interessen des

---

[42] *Schulz,* in: Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 51.

[43] *Starnecker*, in: Gola/Heckmann/Starnecker, 3. Aufl. 2022, BDSG § 3 Rn. 26.

[44] *Starnecker,* in: Gola/Heckmann/Starnecker, 3. Aufl. 2022, BDSG § 3 Rn. 20, 22.

Betroffenen, insbesondere dessen Grundrechte, entgegenstehen. Hierunter werden insbesondere Daten gefasst, die der Verbesserung der Sicherheit des Fahrzeugs dienen. Dies sind z.B. Umfelddaten in Form konkreter personenbezogener Daten anderer Verkehrsteilnehmer, wie z.B. VRU. Um jedoch den Anforderungen nach § 6b Abs. 1 BDSG gerecht zu werden, muss technisch sichergestellt werden, dass nicht das gesamte Geschehen auf und entlang der Fahrstrecke anlasslos aufgezeichnet und gespeichert wird. Diese Umfelddaten müssen vielmehr sofort überschrieben oder gelöscht werden, es sei denn, im konkreten Einzelfall besteht ein konkreter Grund für ein längeres Vorhalten.[45] Ein derartiger Grund könnte in der Sammlung von VRU-Trends liegen, um so entsprechende Hotspots in der UDM markieren zu können.

Allerdings können sich rechtliche Bedenken unter dem Gesichtspunkt der **Datenminimierung im Zusammenspiel mit den per Kamera, LiDAR und Radar erhobenen Daten** ergeben. In hochautomatisierten Fahrzeugen, die ihre Umgebung mit Kamera, LiDAR und Radar wahrnehmen, erfolgt häufig eine massive Datennutzung.[46] Zwar ist für die per LiDAR-Sensorik erhobenen Daten die DS-GVO nicht immer anwendbar, für die per Kamera erhobenen Daten in den meisten Fällen allerdings schon.

Demnach gilt für diese Daten auch der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO. Danach müssen personenbezogene Daten *dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein*. Der Grundsatz stellt eine Ausprägung des Verhältnismäßigkeitsgrundsatzes dar, wonach Daten ungeeignet und damit unerheblich sind, die zur Erreichung des erstrebten Zwecks nicht beitragen.[47] Es dürfte für die Datenerhebung kein milderes, gleich geeignetes Mittel zur Verfügung stehen. Die Kamera-Daten wären demnach unerheblich, wenn die Daten der LiDAR-Sensorik schon ausreichen, um den angestrebten Zweck zu erreichen. Der angestrebte Zweck ist hierbei die sichere und fehlerfreie Navigation des Fahrzeugs mit Hilfe der UDM.

Für die Automobil-Industrie erschwingliche Kameras erreichen nicht die Auflösung und den Dynamikumfang eines menschlichen Auges. Dynamikumfang bezeichnet die Spanne zwischen hellen und dunklen Bildbereichen, in denen zeitgleich etwas erkennbar ist. Starkes Gegenlicht und sich plötzlich verändernde Lichtverhältnisse, spiegelnde Fahrbahnen und Dunkelheit können den Kameras Probleme bereiten. LiDAR-Sensoren werden daher weit überwiegend als notwendig für Stufe 4 Autonomes Fahren entsprechend SAE J3016[48] angesehen. Kameras sind allerdings notwendig, um Verkehrsschilder, Fahrbahnmarkierungen und Fußgänger:innen zu erkennen.[49] Außerdem können die Fahrzeuge durch die per Kamera erhaltenen Daten die infrastrukturseitig erhaltenen Daten abgleichen.[50] Demnach sind die Daten, die allein durch die LiDAR-Sensorik erfasst werden, nicht ausreichend, um das Fahrzeug sicher zu navigieren. Ebenso sind die Kamera-Daten allein nicht ausreichend. Das Zusammenspiel aus beiden Datensätzen ist notwendig, um ein sicheres Navigieren zu ermöglichen. Insbesondere stehen mit dem Gesichtspunkt von Verhältnismäßigkeitserwägungen dem Gebot der Datenminimierung

---

[45] *Klink-Straub/Straub*, NJW 2018, 3201 (3204).

[46] *Borges*, Stiftung Datenschutz - Potenziale von künstlicher Intelligenz mit Blick auf das Datenschutzrecht, S. 5.

[47] Vgl. *Reimer* in Sydow/Marsch, DS-GVO BDSG, Art. 5 DS-GVO Rn. 34.

[48] SAE-Stufe 4, BT-Drucks. 19/27439, S. 16: „Die Kraftfahrzeuge können führerlos verkehren und sich notfalls selbst in den risikominimalen Zustand versetzen, wenn sie an ihre Systemgrenzen gelangen. Es verbleibt stets die Möglichkeit, die Kraftfahrzeuge mit autonomer Fahrfunktion über einen externen Zugriff (etwa aus einer Leitstelle) zu deaktivieren oder auch, sofern in der jeweiligen Entwicklung implementiert, situativ erforderliche Ausnahmefahrmanöver freizugeben. Hierfür ist die sogenannte Technische Aufsicht verantwortlich.“.

[49] *Kleinschmidt/Wagner* in Oppermann/Stender-Vorwachs, Autonomes Fahren, 3. Auflage 2024, Rn. 26.

[50] Zur Diskrepanz zwischen digitalen und analogen Lichtsignalen in Bezug auf Autonome Fahrzeuge s. *Knezevic*, Rechtsrahmen zum autonomen Fahren: Kommunikation zwischen fahrerlosen Fahrzeugen und straßenseitiger Infrastruktur, KlimaR 2022, 279.

gewichtige Güter von Verfassungsrang gegenüber, nämlich das Leben und die körperliche Unversehrtheit, vgl. Art. 2 Abs. 2 S. 1 GG, anderer Verkehrsteilnehmer. Demnach kann durch die Erhebung von Daten per Kamera und zusätzlich per LiDAR-Sensorik kein Verstoß gegen Art. 5 Abs. 1 lit. c DS-GVO festgestellt werden.

Da sich die ausgesendeten Laserimpulse im augensicheren Bereich befinden, begegnet der Einsatz der LiDAR-Sensorik auch im **Hinblick auf Art. 2 Abs. 2 S. 1 Var. 2 GG, dem Grundrecht auf körperliche Unversehrtheit,** keine Bedenken.

3.1.3.4 Hinweispflichten

Mit Anwendbarkeit der DS-GVO sind auch die Informationspflichten aus Art. 13 und Art. 14 DS-GVO zu beachten. Art. 13 DS-GVO regelt die Informationspflichten, wenn die Daten direkt bei der betroffenen Person erhoben werden (Direkterhebung), während Art. 14 DS-GVO die Erhebung nicht bei der betroffenen Person regelt (Dritterhebung). Eine Direkterhebung erfolgt, wenn der Datenverarbeitungsprozess bei der betroffenen Person beginnt und umfasst damit von der jeweiligen Person aktiv bereitgestellte sowie passiv "beobachtete" Daten. Insoweit wird zwischen offener und verdeckter Videoüberwachung differenziert. Bei einer offenen Videoüberwachung weiß die betroffene Person um ebendiese, sodass sie sich wissentlich im Blickwinkel der Videoanlage bewegen bzw. sich gegebenenfalls auch dafür entscheiden kann, den überwachten Bereich zu meiden.[51]

Aufzeichnungen durch autonome Fahrzeuge erfolgen regelmäßig ohne Kenntnis der tangierten Verkehrsteilnehmer:innen. Damit wäre grundsätzlich Art. 14 DS-GVO einschlägig, welcher verdeckte Videoüberwachungen umfasst. Allerdings ergibt sich aus einer derartigen verdeckten Videografie eine erhöhte Eingriffsintensität in die Grundrechte der gefilmten Person, welche im Rahmen des Art. 6 Abs. 1 DS-GVO gerechtfertigt sein muss. Zwar erfolgt vorliegend die Heimlichkeit der Videoerfassung als bloßer Nebeneffekt, da autonome Fahrzeuge grundsätzlich keine nach außen hin erkennbare Kamerasysteme aufweisen. Allerdings könnte durch entsprechende Hinweise auf dem Fahrzeug eine Offenheit der Videoüberwachung hergestellt werden, sodass ein milderes, gleich effektives Mittel gegeben ist. Die heimliche Videoüberwachung ist daher nicht erforderlich und somit unverhältnismäßig.

Kommt es jedoch zu einer derartigen Kennzeichnung der Videoerfassung, wenn natürliche Personen mit der Kamera des EDDY-Fahrzeugs erfasst werden, werden die Daten direkt bei der Person erhoben. Dann handelt es sich um eine Direkterhebung i. S. d. Art. 13 DS-GVO. Der Verantwortliche ist nach Art. 13 Abs. 1 DS-GVO verpflichtet, der betroffenen Person zum Zeitpunkt der Erhebung der Daten folgende Informationen mitzuteilen:

> *a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;*
>
> *b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;*
>
> *c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlagen für die Verarbeitung;*

[51] *Paal/Hennemann,* in: Paal/Pauly/Paal/Hennemann: DS-GVO BDSG, 3. Aufl. 2021, Art. 13 Rn. 11b.

d) wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Der Verantwortliche muss mit vollem Namen, ladungsfähiger Adresse und mindestens E-Mail-Adresse oder Telefonnummer angegeben werden.[52] Weiterhin sind auch die in Art. 13 Abs. 2 DS-GVO genannten Information zur Verfügung zu stellen, um eine faire und transparente Datenverarbeitung zu gewährleisten. Insbesondere ist die betroffene Person über das Recht auf Widerruf einer erteilten Einwilligung nach Art. 7 Abs. 3 DS-GVO und den Auskunftsanspruch nach Art. 15 DS-GVO zu informieren.

Die nach Art. 13 Abs. 1 und Abs. 2 DS-GVO erforderlichen Informationen müssen „zum Zeitpunkt der Erhebung" mitgeteilt werden. Art. 13 DS-GVO regelt eine proaktive Informationspflicht durch den Verpflichteten.[53] Es reicht nach vorherrschender Ansicht nicht aus, die erforderlichen Informationen passiv bereitzuhalten; dies folge aus den anderen sprachlichen Fassungen der Verordnung („*to provide*" und „*fournir*"), sowie dem Sinn und Zweck der Vorschrift, die Betroffenen umfassend über die Datenverarbeitung in Kenntnis zu setzen.[54] Es sei damit zumindest erforderlich, einen aktiven Hinweis dahingehend zu liefern, wo und wie die Informationen umfassend zur Verfügung gestellt werden.[55] So ist es möglich, ein Informationsblatt mit den in Art. 13 DS-GVO geforderten Informationen im Fahrzeug bereitzuhalten. Aufgrund der aktiven Informationsverpflichtung muss allerdings ein Hinweis auf diese Blätter am mit der Kamera ausgestatteten Fahrzeug selbst angebracht werden. Auch kann ein QR-Code auf dem Fahrzeug selbst genutzt werden.

Fraglich ist, ob „zum Zeitpunkt der Erhebung" meint, dass die Informationen schon vor Beginn der Datenerhebung zur Verfügung gestellt werden müssen. Dafür spricht, dass die Information auch dazu dient, dass die betroffene Person eine informierte Entscheidung über die Einwilligung in die Datenverarbeitung treffen kann.[56] Insbesondere die Formulierung des Art. 13 Abs. 2 lit. e DS-GVO verdeutliche, dass die Information grundsätzlich ergehen muss, bevor der Datenfluss einsetzt.[57] Nach anderer Ansicht gebe der Wortlaut keine zeitlich vorgelagerte Informationspflicht her.[58] Spätestens aber

---

[52] *Schmidt-Wudy,* in Wolff/Brink: BeckOK Datenschutzrecht, Art. 13, Rn. 39; Art. 14. Rn. 40.

[53] *Conrad,* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 34 Rn. 579.

[54] *Bäcker,* in: Kühling/Buchner, DS-GVO BDSG, Art. 13 DS-GVO Rn. 59, 56.

[55] *Bäcker,* in: Kühling/Buchner, DS-GVO BDSG, Art. 13 DS-GVO Rn. 59*; Knyrim,* in: Ehmann/Selmayr, DS-GVO, Art. 13 Rn. 22.

[56] So *Bäcker,* in: Kühling/Buchner, DS-GVO BDSG, Art. 13 DS-GVO Rn. 56*; Franck,* in: Gola/Heckmann, DS-GVO BDSG, Art. 13 DS-GVO Rn. 39*;* unentschieden *Knyrim,* in: Ehmann/Selmayr, DS-GVO, Art. 13 Rn. 11.

[57] *Franck,* in: Gola/Heckmann, DS-GVO BDSG, Art. 13 Rn. 39.

[58] *Eßer,* in: Auernhammer, DSGVO – BDSG, Art. 13 DS-GVO Rn. 17; *Kamlah,* in: Plath, DSGVO/BDSG, Art. 13 DS-GVO Rn. 8.

gleichzeitig zum Zeitpunkt der Datenerhebung müssen die Informationen übermittelt werden.[59] Das heißt, dass die Informationspflicht entweder bereits vor der Datenerhebung, jedenfalls aber simultan mit der initialen Datenverarbeitung ausgelöst wird. Daraus folgt auch, dass die Informationspflicht aus Art. 13 DS-GVO nicht durch eine nachträgliche Anonymisierung der Daten entfällt, da sie jedenfalls schon vorher entstanden ist.

Die Umsetzung dieser Hinweispflichten im fließenden Straßenverkehr stellt damit eine praktisch erhebliche Herausforderung dar. So ist es im öffentlichen Verkehrswesen technisch und logistisch so gut wie unmöglich, alle betroffenen Personen umfassend und rechtzeitig über die Erhebung ihrer Daten zu informieren und dadurch Art. 13 Abs. 1 DS-GVO gerecht zu werden. Dies gilt umso mehr, als autonome Fahrzeuge kontinuierlich Daten erfassen und verarbeiten müssen, um ihre Funktion im Straßenverkehr erfüllen zu können. Aufgrund dieser Echtzeit-Erhebung haben die betroffenen Personen in der Regel keine Möglichkeit auf die Verarbeitung zu reagieren oder sie zu verhindern.

Der Ausschlussgrund des Art. 13 Abs. 4 DS-GVO, nachdem eine Informationspflicht nicht besteht, wenn die betroffene Person bereits über die Informationen verfügt, führt vorliegend zu keiner Auflösung der Problematik.

Die Hürden ließen sich lediglich durch eine Anwendbarkeit der Ausnahmetatbestände von den Informationspflichten nach Art. 14 Abs. 5 DS-GVO überwinden. Insbesondere Art. 14 Abs. 5 lit. b DS-GVO wäre im vorliegenden Fall zielführend, da eine Bereitstellung der Information einen unverhältnismäßigen Aufwand bedeuten würde und daher ausnahmsweise nicht zu erfolgen hätte. Allerdings sind diese Ausnahmen ausdrücklich auf Art. 14 DS-GVO beschränkt und nicht auf Art. 13 DS-GVO anwendbar. Insoweit besteht mit Blick auf Art. 13 Abs. 4 DS-GVO keine planwidrige Regelungslücke, die eine Analogie rechtfertigen könnte. Zudem ist es bei Datenerhebungen, die unmittelbar bei der betroffenen Person und mit deren Kenntnis erfolgen, erforderlich, diese mit entsprechenden Informationen zu versorgen.[60]

3.1.3.5 Betroffenenrechte

Die weiteren Betroffenenrechte sind in den Art. 15 ff. DS-GVO geregelt.

Nach Art. 15 DS-GVO haben Betroffene das Recht, von den Verantwortlichen eine Bestätigung darüber zu verlangen, ob ihre personenbezogenen Daten verarbeitet werden, und wenn ja, Auskunft über diese Daten sowie über bestimmte Informationen wie die Verarbeitungszwecke, die Kategorien personenbezogener Daten und die Empfänger oder Kategorien von Empfängern zu erhalten.

Art. 16 DS-GVO gewährt Betroffenen das Recht unverzüglich die Berichtigung unrichtiger personenbezogener Daten bzw. die Vervollständigung unvollständiger Daten zu verlangen. Art. 17 DS-GVO normiert das "Recht auf Vergessenwerden", wonach betroffene Personen die Löschung ihrer personenbezogenen Daten verlangen können, sofern die Voraussetzungen des Art. 17 Abs. 1 DS-GVO erfüllt sind. Dies ist beispielsweise der Fall, wenn die Daten für die ursprünglichen Zwecke nicht mehr notwendig sind (lit. a) oder diese unrechtmäßig verarbeitet wurden (lit. d).

Betroffene können nach Art. 18 DS-GVO auch die Einschränkung der Verarbeitung ihrer personenbezogenen Daten verlangen, z. B. wenn die Richtigkeit der Daten bestritten wird, oder die Verarbeitung

[59] *Knyrim,* in: Ehmann/Selmayr, DS-GVO, Art. 13 Rn. 11.

[60] *Dix,* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 13 DS-GVO, Rn. 22.

unrechtmäßig ist. Art. 20 DS-GVO gewährt Betroffenen das Recht, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Zudem können Betroffene nach Art. 21 DS-GVO, jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen bzw. eine einmal gegebene Einwilligung in die Verarbeitung der personenbezogenen Daten nach Art. 7 Abs. 3 DS-GVO widerrufen.

Schließlich normiert Art. 77 DS-GVO die Möglichkeit eine Beschwerde bei der Aufsichtsbehörde des jeweiligen Mitgliedstaats einzulegen, sollte sie der Ansicht sein, dass die Verarbeitung der personenbezogenen Daten gegen die DS-GVO verstößt.

3.1.4 Fazit

Schon bei der technischen Entwicklung und Programmierung der UDM sowie bei dem späteren Betrieb müssen die Grundrechte aller Verkehrsteilnehmenden geachtet werden. Insbesondere müssen besondere Maßnahmen zum Schutz von VRU ergriffen werden, um eine Diskriminierung gegenüber weniger vulnerablen Verkehrsteilnehmenden zu verhindern. Die IVS-Richtlinie soll (nur) einen diskriminierungsfreien Zugang von VRU zu IVS gewährleisten. Art. 3 Abs. 1 GG geht darüber hinaus und schreibt eine diskriminierungsfreie Entwicklung und Anwendung vor. Dies beutetet allerdings nicht, dass Fahrzeuge weniger Mittel nutzen dürfen, als ihnen technisch zur Verfügung stehen, um Verkehrsteilnehmende zu schützen. Die Betreiber:innen von autonomen Fahrzeugen tragen die ethische Verantwortung, die größtmögliche Sicherheit für Verkehrsteilnehmende zu garantieren. Existieren daher Technologien, die Leben retten oder schwere Verletzungen verhindern könnten, sind diese, unabhängig vom Risikoniveau des Standorts zu nutzen. Die Reduktion der Sicherheitsvorkehrungen bei einem Fahren außerhalb eines sog. „Alarmmodi“ ist daher nicht möglich. Die Fahrzeuge müssen vielmehr jederzeit in einer Art „Alarmmodus“ fahren und darf nicht außerhalb besonders risikobehafteter Bereiche bewusst hinter den eigenen technischen Möglichkeiten zurückbleiben.

3.2 Use Case 2: Nutzbarkeit und Verbindlichkeit von Daten in der UDM

In der UDM werden viele Daten verarbeitet, genutzt und weitergegeben. Für fehlende oder fehlerhafte Daten haftet bisher niemand. Doch ohne verbindliche Haftung können sich Nutzende nicht auf die inhaltliche Richtigkeit der Daten verlassen und diese deswegen nur eingeschränkt nutzen. In diesem Abschnitt werden die zivilrechtliche Haftung und datenschutzrechtliche Regelungen genauer untersucht. Die Betreiber:innen/ Hersteller:innen der UDM haften nicht für die Fehlerhaftigkeit und inhaltliche Richtigkeit von Daten. Daten selbst werden weiterhin (rechtlich) nicht als Produkt erfasst. Der/Die Betreiber:in könnte die Haftung für die inhaltliche Richtigkeit der Daten übernehmen, um den Daten Verbindlichkeit zu geben. Ein Teil der Daten bzw. Daten einer gewissen Qualität können gegen eine Gebühr zur Verfügung gestellt werden, um den Betrieb einer UDM zu finanzieren. Wenn die UDM durch die öffentliche Hand betrieben wird, ist aber fraglich, ob eine solche Vereinbarung mit den Haushaltsgrundsätzen vereinbar ist. Jedenfalls müsste vorher eine entsprechende Rechtsgrundlage geschaffen werden, die im Moment noch nicht existiert.
Für Fehler in der Hard- und Software der UDM kann das Produkthaftungsrecht durchaus greifen. Auch daraus lässt sich jedoch keine Haftung für die inhaltliche Richtigkeit der UDM ableiten.

Datenschutzrechtlich relevant ist die Verwendung von LiDAR-Sensorik und Kameras. Bei beiden werden überwiegend personenbezogene Daten erhoben, so dass die DSG-VO beachtet werden muss. Eine Vermeidung der Anwendbarkeit der DSG-VO bspw. durch sogenannte geschlossene Systeme oder automatische Anonymisierung ist für die UDM nicht realisierbar, da es gerade auf die Datenweitergabe und -nutzung durch andere Verkehrsteilnehmer ankommt.

3.2.1 Sachverhalt

Im Kontext der Datenverlässlichkeit für autonome Fahrzeuge ist es wichtig, dass eine umfassende Datensammlung gewährleistet wird, die eine sichere und präzise Verkehrsnavigation ermöglicht. Autonome und automatisierte Fahrzeuge werden vor allem mithilfe von GNSS[61] und LiDAR-Sensorik[62] navigiert. Fahrzeuge, die keine IP- oder Mobilfunk basierte Verbindung zur UDM haben, stellen die Objektinformationen als Message-Forwarding[63] bereit. Das EDDY-Fahrzeug ist zusätzlich mit einer Kamera und weiteren unterstützenden Sensoren ausgestattet, um relevante Objekte wie Baustellen, Schilder, Schlaglöcher, Straßenbelag aufzunehmen. Ein sofortiges Blurren als Form der Unkenntlichmachung der Bilder findet nicht statt. Erst **nach Übertragung der Daten auf einen zentralen Speicher** werden die Daten anonymisiert. Die per Kamera und LiDAR detektierten Informationen sollen wiederum als abstrahierte Objektdaten in die UDM eingespeist werden. Im Falle eines GNSS-Ausfalls gewinnt die LiDAR-Sensorik und die Kamera zwecks Landmarkenerfassung an Bedeutung, um das EDDY-Fahrzeug zu navigieren. Diese Landmarken sollen ebenfalls in der UDM gespeichert werden. Damit beziehen sich diese Daten, anders als die in den Use Cases 1 und 4 gesammelten spezifischen Daten hinsichtlich Bewegungsmuster und der Identifikation einzelner Verkehrsteilnehmer:innen als VRU, auf bloß abstrahierte Objektdaten. Sie bieten allgemeine Umgebungsinformationen, die ein Verständnis der Fahrzeugumgebung fördern und bei der Entscheidungsfindung für die Fahrzeugnavigation helfen. Diese umfassende Sammlung an spezifischen und allgemeinen Datenarten ist relevant, um sicherzustellen, dass autonome Fahrzeuge sowohl den speziellen Anforderungen für die Sicherheit und Interaktion z. B. mit VRU gerecht werden als auch die allgemeine Umgebung effektiv verstehen können.

Neu im Projekt EDDY ist, dass die Datenübertragung nicht bloß von der Infrastruktur an das Fahrzeug stattfindet, sondern auch vom Fahrzeug Richtung Infrastruktur. Funktioniert diese Selbstlokalisierung und die Navigation nicht, kann es zu Unfällen kommen. Die inhaltliche Richtigkeit der Daten ist damit von hoher Bedeutung für die Navigation und Lokalisierung der Fahrzeuge.

Dies wird an **folgendem Beispiel** besonders deutlich: Ein autonomes Fahrzeug wird mithilfe der UDM navigiert. Die dort integrierten Geo-Daten sind unvollständig oder fehlerhaft, sodass das Fahrzeug

[61] Global Navigation Satellite System als Sammelbegriff für die Verwendung bestehender und künftiger globaler Satellitensysteme zur Positionsbestimmung und Navigation.

[62] Die Methode des **Light Detection and Ranging** (LiDAR) dient der Umfelderfassung. Dabei wird Licht in Form eines gepulsten Lasers ausgesendet und von den Objekten reflektiert. Das reflektierte Licht wird von dem Fahrzeug detektiert. Aus der Zeitspanne zwischen Aussendung und Rückkehr des Lichtimpulses kann das Auto den Abstand zum erfassten Objekt berechnen. Somit können Objekte erkannt und kategorisiert werden. Die eingesetzten Laserstrahlen liegen im sog. augensicheren Bereich. LiDAR-Sensoren erzeugen präzise, dreidimensionale Informationen über die Form und Oberflächeneigenschaft der umliegenden Objekte, vgl.: https://www.blickfeld.com/de/blog/was-ist-lidar/.

[63] Message Forwarding bezeichnet ein System zur Weiterleitung von Nachrichten. Das System besteht aus einer Gruppe von Funkstationen bei der Mitteilungen einer Ursprungsstation (hier: alle Fahrzeugen im System) an eine oder mehrere Zielstationen (hier: die UDM) gesendet werden. Dabei können die Nachrichten durch eine oder mehrere Weiterleitungsstationen gesendet werden.

statt auf dem rechten Fahrstreifen auf dem rechtsseitig gelegenen Bürgersteig fährt. Dies führt zu beschädigten Straßenschildern und einem verletzten Fußgänger. Eine steuernde Person, die haften könnte, gibt es in diesem Szenario nicht.

3.2.2 Haftung für fehlende und fehlerhafte Daten in der UDM

Im Folgenden wird untersucht, ob und inwiefern eine (zivilrechtliche) Haftung für zur Verfügung gestellte Daten besteht.

Die UDM kann für eine Vielzahl von Anwendungszwecken genutzt werden, weshalb auch eine Vielzahl von Haftungsfragen auftreten können. Im Kern kommt es jedoch darauf an, wer für fehlende oder fehlerhafte Daten der UDM haftet.

Durch das vorsätzliche Einspeisen falscher oder fehlerhafter Daten kommt grundsätzlich auch eine strafrechtliche Haftung in Betracht, insbesondere wenn autonome Fahrzeuge nur mit Hilfe der UDM navigiert würden.[64] Im Folgenden wird aber nur die zivilrechtliche Haftung behandelt.

3.2.2.1 Produkthaftungsrecht der Europäischen Union für Daten

Das Produkthaftungsrecht wird maßgeblich von der Richtlinie 85/374/EWG (sog. Produkthaftungsrichtlinie)[65] aus dem Jahr 1985 reguliert, welche mit dem Produkthaftungsgesetz (ProdHaftG)[66] 1989 in nationales Recht umgesetzt wurde. Die Richtlinie dient dem Verbraucherschutz[67] und ist daher nur in „Business-to-Consumer"-Beziehungen (B2C) anwendbar.

Bisher umfasst das Produkthaftungsrecht der Europäischen Union (EU) **nicht explizit Sicherheitsrisiken, die aus fehlerhaften oder fehlenden Daten** folgen. Die Produkthaftungsrichtlinie soll nun jedoch grundlegend erneuert werden. Mit der Überarbeitung soll unter anderem sichergestellt werden, dass die Haftungsvorschriften der Beschaffenheit von Produkten im digitalen Zeitalter und den damit zusammenhängenden Risiken, Rechnung tragen.[68] Der Produkthaftungsrichtlinienvorschlag gilt nur für materielle Verluste aufgrund von Tod, Körperverletzung, Sachschäden, Datenverlust und -verfälschungen.[69] Der Anwendungsbereich der Richtlinie umfasst damit künftig auch den Verlust oder die Verfälschung von Daten, so sollen z.B. aus einer Festplatte gelöschte Inhalte entschädigt werden, einschließlich der Kosten für die Rettung oder Wiederherstellung der Daten.[70] Schaden i. S. d. Vorschlags bezeichnet damit wesentliche Verluste, die sich aus dem Verlust oder der Verfälschung von Daten, die nicht ausschließlich für berufliche Zwecke verwendet werden, ergeben, vgl. Art. 4 Abs. 6 lit. c) der COM (2022), 495 final.

---

[64] Z.B.: § 315b As. 1 Nr. 3 StGB (Gefährlicher Eingriff in den Straßenverkehr); § 268 Abs. 1 StGB (Fälschung technischer Aufzeichnungen); §§ 303a, 303b StGB (Datenveränderung, Computersabotage); eventuell sogar §§ 211, 212 StGB (Mord, Totschlag).

[65] Richtlinie des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten über die Haftung für fehlerhafte Produkte (Produkthaftungsrichtline).

[66] Produkthaftungsgesetz vom 15. Dezember 1989 (BGBl. I S. 2198), das zuletzt durch Artikel 5 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2421) geändert worden ist.

[67] Vgl. Erwägungsgründe zur Produkthaftungsrichtlinie v. 1985.

[68] Vgl. Vorschlag der Europäischen Kommission vom 28. September 2022 für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte, COM(2022) 495 final, 2022/0302 (COD), S. 2.

[69] COM(2022) 495 final, S. 3.

[70] COM(2022) 495 final, Erwägungsgrund 16.

Mit dem Vorschlag erneuert die Kommission das Produkthaftungsregime grundlegend. Der Vorschlag erkennt **Daten als vermögenswerte Position** und damit als ersatzfähigen Schadensposten an.[71] Die Kommission geht jedoch nicht darauf ein, ob auch Vermögensschäden umfasst sind, die **aufgrund** von fehlerhaften oder fehlenden Daten entstanden sind. **Dafür müssten Daten selbst als Produkt gelten**.

Wenn Daten als Produkte i. S. d. § 2 ProdHaftG angesehen werden und aufgrund der Fehlerhaftigkeit dieses Produkts an anderen Rechtsgütern ein ersatzfähiger Schaden entstanden ist, fiele der Sachverhalt unter den Anwendungsbereich des ProdHaftG.

Nach dem Vorschlag der Kommission bezeichnet „Produkt“ *alle beweglichen Sachen, auch wenn diese in eine andere bewegliche oder unbewegliche Sache integriert sind. Dazu zählen auch Elektrizität, digitale Bauunterlagen und Software.*[72] Datenträger (z.B. Buch, CD, USB-Stick) sind ohne weiteres als bewegliche Sachen und damit als Produkt einzuordnen. Wenn der schadensauslösende Fehler in der körperlichen Beschaffenheit liegt, gelangt man zu einer Haftung des Herstellers im Sinne des Produkthaftungsrechts.[73] Wenn aber die gespeicherte Information selbst aufgrund ihres Inhalts den Schaden ausgelöst hat, ist unklar, ob eine Haftung nach § 1 ProdHaftG greift. Für eine Haftung müssten die in den Daten gespeicherten Informationen als „Produkt“ gelten. Ob Produkthaftung auch für **geistige Leistungen** greift, wird seit Mitte der 1990er in der rechtswissenschaftlichen Literatur diskutiert. Die Bandbreite möglicher Anwendungsfälle ist groß. Folgende Beispiele sollen dies veranschaulichen:

- In einer Orientierungskarte für die Instrument-Flugnavigation ist ein Berg nicht eingezeichnet, infolgedessen kommt es zu einem Flugzeugabsturz;
- ein Fehler in einer statistischen Berechnung, die dem Bau eines Krans zugrundgelegt wird, führt zu Beschädigungen der Maschine, die ihrerseits Personen- und Sachschäden zur Folge haben;
- aufgrund eines Kommafehlers in einem medizinischen Anleitungswerk infundiert ein Arzt bei der Durchführung eines Diabetes-Tests statt einer 2,5%igen eine 25%ige Kochsalzlösung, worauf der Patient verstirbt.[74]

Daten i. S. d. Vorschlags der Kommission bezeichnen *jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild-, oder audiovisuellen Material*.[75]

Daten als digitale Darstellung von Informationen, deren inhaltliche (Un-)Richtigkeit schwerwiegende Folgen haben kann, fügen sich in die obigen Beispielfälle ein. Insbesondere das Anwendungsbeispiel des autonomen Autos, welches mit Hilfe der UDM navigiert, weist erhebliche inhaltliche Nähe zu dem Fall der fehlerhaften Karte für die Instrumentenflugnavigation auf. Die Frage, ob eine inhaltliche Richtigkeit von Informationen unter das ProdHaftG fällt, ist demnach eine Grundsatzfrage, die durch die Digitalisierung in einem neuen Gewand erscheint.

---

[71] COM (2022) 495 final, S. 4, 14, S. 18.

[72] COM (2022) 495 final, Art. 2 Abs. 1.

[73] *Förster,* in Hau/Poseck: BeckOK BGB, § 2 ProdHaftG Rn. 18.

[74] Siehe diese und weitere Beispiele: *Cahn*, Produkthaftung für verkörperte Leistungen, NJW 1996, 2899 (2899).

[75] Vgl. COM (2022) 495 final, Art. 4 Abs. 7 i.V.m. Art. 2 Abs. 1 der Verordnung (EU) Nr. 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt).

Insofern hat die Kommission versäumt, in ihrem Vorschlag grundlegende Fragen zu beantworten. Die Kommission hätte auch für Klarheit sorgen können, indem sie feststellt, dass die inhaltliche Fehlerhaftigkeit von Daten nicht unter den Regelungsgehalt des Produkthaftungsrechts fällt.

Die Gefährlichkeit von „sicherheitsrelevanten Falschinformationen" ist unbestreitbar. Fraglich ist, ob das ProdHaftG die richtige Stelle ist, um diese Fragen zu lösen.[76]

§ 1 ProdHaftG ist nur dazu berufen, eine Haftung für fehlerhafte Produkte zu begründen, nicht jedoch für fehlerhafte Dienstleistungen. Wenn digitale Dienste so in ein Produkt integriert oder mit ihm verbunden werden, dass das Produkt ohne die kontinuierliche Bereitstellung der Daten in seiner Funktion eingeschränkt ist, wird die verschuldensunabhängige Haftung des erneuerten Produkthaftungsrechts auch auf diese Dienstleistungen erweitert, z. B. kontinuierliche Bereitstellung von Verkehrsdaten in einem Navigationssystem.[77] Die Bereitstellung der Daten wird als „integrierter Dienst" in einem Produkt vom Haftungsregime des Produkthaftungsrechts erfasst. **Nicht erfasst werden danach die bereitgestellten Daten selbst.**

Auch Software ist als Produkt erfasst.[78] Software bezeichnet Programme, die auf einem Computer ausgeführt werden können und jegliche Daten, die damit erzeugt werden können. Für diese Art von erzeugten Daten soll das Produkthaftungsrecht damit in Zukunft sehr wohl gelten. Der Quellcode von Software stellt nach den Vorstellungen des Richtliniengebers allerdings kein Produkt im Sinne der Richtlinie dar, da es sich um reine Informationen handele.[79] Auch aus diesem Grund scheint es dem Willen der Kommission zu entsprechen den **Inhalt von Daten als digitalisierte Information nicht als Produkt anzusehen.** Eine solche ablehnende Haltung zu dieser Frage hätte die Kommission in den Erwägungsgründen des Vorschlags klarstellen können.

Nun bleibt abzuwarten, ob der deutsche Gesetzgeber sich dieser Fragen im Rahmen der Umsetzung der neuen Produkthaftungsrichtlinie annimmt. Insbesondere, da die EU die Mitgliedsstaaten verpflichtet hat, Haftungsfragen in Bezug auf die Einführung und Nutzung von IVS-Anwendungen und -Diensten im Einklang mit dem Unionsrecht, insbesondere den erlassenen Spezifikationen und dem Produkthaftungsrecht, zu regeln (vgl. Art. 11 IVS-Richtlinie). Die Haftung für IVS sind derzeit weder explizit im ProdHaftG, im IVSG oder im nationalen IVS-Aktionsplan „Straße"[80] angesprochen. Der nationale Gesetzgeber hat damit bei der Umsetzung der erneuerten Produkthaftungsrichtlinie die Chance, seiner Verpflichtung aus Art. 11 IVS-Richtlinie nachzukommen.

Ob Daten per se als Produkt unter das Produkthaftungsrecht fallen, ist damit ungeklärt. Eine Auslegung des Vorschlags für das neue Produkthaftungsrecht spricht dagegen. Es besteht nach wie vor Forschungs- und Klärungsbedarf, um ein Haftungsregime für die Richtigkeit von sicherheitsrelevanten Daten zu entwickeln. Ein Haftungsrecht für Daten zu entwickeln, wäre aber der nächste Schritt in

---

[76] Vgl. *Förster* in BeckOK BGB Hau/Poseck, § 2 ProdHaftG Rn. 19.

[77] COM (2022) 495 final, Erwägungsgrund 15.

[78] Vgl. Art. 1 Abs. 1 S. 2 COM (2022) 495 final.

[79] Vgl. COM (2022) 495 final, Erwägungsgründe 12, 13.

[80] Der nationale IVS-Aktionsplan „Straße" dient der koordinierten Weiterentwicklung bestehender und der beschleunigten Einführung neuer Intelligenter Verkehrssysteme in Deutschland bis 2020 und wurde in Umsetzung der IVS-Richtlinie im September 2012 erlassen.

vielen sicherheitsrelevanten Bereichen, um diese im „europäischen Binnenmarkt für Daten“[81] vollständig nutzbar zu machen.

Wenn für die Daten nicht verbindlich Haftung übernommen wird, können sich die Nutzenden der Datensätze nicht auf die inhaltliche Richtigkeit der Daten verlassen. Sie sind demnach nur sehr eingeschränkt nutzbar. Ohne eine Haftung für die konkreten Daten kann ein autonomes Fahrzeug nicht ausschließlich aufgrund dieser Daten navigiert werden. Die UDM kann zwar bei sicherheitsunkritischen Fahrfunktionen (z. B. Navigation) von autonomen Fahrzeugen unterstützend beitragen, die Betreiber:innen haften jedoch nicht für die inhaltliche Richtigkeit der Daten. Als mögliche Anwendungsmöglichkeiten der UDM für autonome und automatisierte Fahrzeuge verbleiben daher z. B.:

- Ableitung von Empfehlungen für Fahrspur, Geschwindigkeit oder Abstand unter Berücksichtigung des Verkehrsgeschehens sowie der Umgebungsbedingungen wie das Wetter;
- optimiertes Routing von Fahrzeugen zur besseren Auslastung des Verkehrsnetzes;
- Verwendung tages- bis stundenaktueller Daten zu Baustellen, Staus, etc.;
- Identifikation und Kommunikation von Konfliktschwerpunkten zur Empfehlung einer vorsichtigeren Fahrweise in dem betreffenden Bereich.

3.2.2.2 Produktsicherheitsrecht für Daten

Eine weitere Möglichkeit, Verbindlichkeit für Daten herzustellen, bietet das Produktsicherheitsrecht. Dieses könnte den Hersteller eines individuellen Systems in die Pflicht nehmen, indem der Gesetzgeber **Regulierungen der Sicherheitsanforderungen an sicherheitsrelevante Daten** aufgreift.

Durch eine **Zertifizierungspflicht bestimmter sicherheitsrelevanter Daten** könnte ein Markt für Daten geschaffen werden, die im Wege der externen Vernetzung zwischen verschiedenen Systemen zirkulieren können. Sicherheitsrelevante Daten können z. B. solche sein, die in einen Trainingsdatensatz eines KI-Systems einfließen, der sicherheitsrelevante Optimierungen ermöglicht. Den Herstellern bzw. Verwendern dieser Systeme wird durch die Zertifizierungspflicht die ausführliche Prüfung der Datenqualität abgenommen, die Prüfung kann sich auf eine Prüfung des Zertifikates beschränken. Ein solcher Ansatz besteht bereits im Verhältnis Hersteller:in und Arbeitgeber:innen: Der/Die Arbeitgeber:in kann sich grundsätzlich auf das CE-Kennzeichen und die Angaben in der Konformitätserklärung verlassen.

Dieser Ansatz könnte durch ein neu zu schaffendes „**Produktsicherheitsrecht für Daten**“ aufgegriffen werden. Für bestimmte sicherheitsrelevante Datenprodukte können gesetzlich vorgeschriebene und von anerkannten Prüfstellen ausgestellte Zertifikate deren Verkehrsfähigkeit erhöhen und damit eine umfangreiche sicherheitsrelevante externe Vernetzung von Systemen ermöglichen.

Die **Cybersecurity-Verordnung**[82] sieht **Zertifizierungsschemata** vor, die eine solche Zertifizierung ermöglichen. Allerdings ist die Cybersecurity-VO für die UDM nicht direkt anwendbar (siehe 5.1.1 unten). Außerdem sind Daten nach dem Willen des europäischen Gesetzgebers kein Produkt (siehe 3.2.2.1 oben). Die Idee einer Zertifizierung kann grundsätzlich weiterentwickelt werden, sodass sicherheitsrelevante Daten verbindlicher werden. Im Moment bietet aber auch das

[81] Vgl. Europäische Datenstrategie der EU-Kommission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (zuletzt aufgerufen am 31. Juli 2024).

[82] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit – Cybersecurity-VO), ABl. L 151 vom 7.6.2019, S. 15.

Produktsicherheitsrecht keine Lösung, um Daten für die verbindliche Navigation von Fahrzeugen durch die UDM nutzbar zu machen.

3.2.3 Produkthaftungsrecht der Europäischen Union für die UDM

Wie in 3.2.2.1 oben ausgeführt, erscheint es nicht dem Willen der EU-Kommission zu entsprechen, dass das Produkthaftungsrecht nach der (erneuerten) Produkthaftungsrichtlinie und dem ProdHaftG die Haftung für inhaltliche Richtigkeit von Daten miteinschließt. Allerdings könnten die Regelungen für Produkthaftung für die UDM im Allgemeinen gelten. Dafür muss die **UDM als „Produkt" i. S. d. erneuerten Produkthaftungsrichtlinie** angesehen werden. Die erneuerte Produkthaftungsrichtlinie gilt nicht für Dienstleistungen als solche, trotzdem ist es notwendig die verschuldensunabhängige Haftung auf manche digitalen Dienste auszuweiten.[83] Als Beispiel für solche integrierten digitalen Dienste in einem Produkt, ohne welche das Produkt seine Funktionen nicht erfüllen kann, nennt der Vorschlag der Kommission „*die kontinuierliche Bereitstellung von Verkehrsdaten in einem Navigationssystem*". Die digitalen Dienste seien für die Sicherheit des Produkts genauso grundlegend wie physische oder digitale Komponenten, sodass die verbundenen Dienstleistungen als Komponenten des Produkts betrachtet werden sollten, wenn sie der Kontrolle des Herstellers des Produkts unterliegen.[84] Die UDM kann demnach als Produkt angesehen werden, die in ihr bereitgestellten Verkehrsdaten sind ein integrierter digitaler Dienst, ohne den die UDM seine Funktion nicht erfüllen kann. Wie in 3.2.2.1 oben beschrieben ergibt sich allerdings auch aus der (neuen) Produkthaftungsrichtlinie keine Haftung für die inhaltliche Richtigkeit der Informationen. Eine Haftung für die UDM ergibt sich nur bei Schäden, die auf der Fehlerhaftigkeit der UDM und ihrer Software als solcher beruhen. Software wird als Produkt im Rahmen des Vorschlags der neuen Produkthaftungsrichtlinie angesehen, vgl. Art. 4 Abs. 1 S. 2 COM (2022) 495 final. Nicht nur die Hardware-Hersteller:innen, sondern auch die Software-Hersteller:innen und Bereitsteller:innen von digitalen Diensten sollen damit haftbar gemacht werden. Das Produkt gilt auch dann als fehlerhaft, wenn Produktsicherheits-Anforderungen, inklusive sicherheitsrelevante Cyber-Security-Standards nicht eingehalten werden. [85] Allerdings soll das erneuerte Produkthaftungsrecht nicht für freie und quelloffene Software gelten, die ohne jegliche Gegenleistung frei zur Verfügung gestellt wird und deren Quellcode veränderbar und weiterverteilbar ist. Als Gegenleistung gilt auch das Teilen von personenbezogenen Daten.[86] Wenn die UDM nur genutzt werden kann, wenn die nutzende Person selbst ihre personenbezogenen Daten teilt, fällt sie demnach nicht unter diese Ausnahme.

Auch wenn die Betreiber:innen der UDM damit nicht für die inhaltliche Richtigkeit der Informationen haften, müssen trotzdem gewisse Standards bei dem Betrieb der UDM eingehalten werden. So können sich aus dem Betrieb der UDM dennoch Haftungsfragen ergeben, zum Beispiel wenn für die verwendete Software erforderliche Cyber-Security-Standards nicht eingehalten werden.

3.2.4 Finanzierung der UDM durch Haftungsübernahme und Monetarisierung von Daten

Eine abschließende Klärung, wie man die Daten für Technik und Entwicklung nutzbar macht, würde über den Rahmen dieses Gutachtens hinausgehen. Einige (nicht abschließende) Lösungsansätze sollen dennoch in diesem Teil dargestellt werden.

---

[83] COM (2022) 495 final, Erwägungsgrund 15.

[84] COM (2022) 495 final, Erwägungsgrund 15, S. 6.

[85] COM (2022) 495 final, S. 5.

[86] COM (2022) 495 final, Erwägungsgrund 13.

Wie der (breite und flächendeckende) Aufbau einer UDM finanziert werden soll, ist nicht abschließend geklärt. Ziel des Projekts ist es gerade die Daten in der UDM der Öffentlichkeit als Gemeingut zur Verfügung zu stellen. Dass für den Zugriff auf die UDM jedenfalls eine Gebühr gezahlt werden soll, würde diesem Ziel diametral zuwiderlaufen.

Ein mögliches Konzept ist jedoch, dass ein „Grundstock" an Daten kostenfrei zur Verfügung gestellt wird. Diese könnten entweder weniger genau sein, jedenfalls aber ohne Haftungsübernahme zur Verfügung gestellt werden. Wer allerdings einen bestimmten Betrag bezahlt, kann Zugriff auf die genauen Daten erhalten. Im Gegenzug für diesen Betrag kann der/die Nutzende zum einen Zugriff auf akkuratere Daten bekommen, zum anderen können die Betreiber:innen vereinbaren, dass für diese Daten auch die Haftung für deren (inhaltliche) Richtigkeit übernommen wird. So könnten verschiedene Stakeholder sich verlässliche Daten beschaffen, welche sie tatsächlich für die Weiterentwicklung ihrer digitalisierten Produkte verwerten können. Diese Daten wären dann nicht mehr nur eine interessante Zusatzinformation, sondern eine verlässliche Informationsquelle. Mithilfe dieser Finanzierung können die Betreiber:innen auch eine Versicherung für Schäden aufgrund von fehlerhaften Daten abschließen. Ein Teil der Versicherungsraten kann durch die Gebühren gezahlt werden.

Wenn die Betreiber:innen der UDM staatlich bzw. öffentlich sind, ergeben sich eine Reihe von Herausforderungen. Insbesondere muss der Staat die finanziellen Mittel für die übernommenen Verpflichtungen bereitstellen können, da insoweit eine Versicherung der öffentlichen Hand nicht möglich ist. So müssen öffentliche Haushalte effizient und verantwortungsvoll mit den zur Verfügung stehenden Mitteln umgehen. Eine Versicherungslösung würde das Risiko und die Kosten auf den Steuerzahler übertragen, was nicht den Prinzipien des Haushaltsrechts, insbesondere den Prinzipen der Wirtschaftlichkeit und Sparsamkeit sowie der Haushaltswahrheit, entspricht. Die Grundsätze der Wirtschaftlichkeit und Sparsamkeit sind beispielsweise in § 6 HGRG und § 7 LHO Hamburg[87] verankert. Das Sparsamkeitsgebot fordert, dass ein bestimmtes Ergebnis mit dem geringstmöglichen Mitteleinsatz erreicht wird, während das Prinzip der Wirtschaftlichkeit verlangt, dass mit einem bestimmten Mitteleinsatz das bestmögliche Ergebnis erzielt wird.[88]

Daher stellt sich die Frage, ob der Aufbau einer (zuverlässigen) UDM nicht auch mit geringeren Mitteln zu erreichen wäre und ob eine Versicherung von privaten Betreiber:innen tatsächlich das bestmögliche Ergebnis liefert. Insbesondere ist das vorliegende Risiko im Vorfeld schwer abzuschätzen und die Haftung des Staates für die inhaltliche Richtigkeit der Daten schwer kalkulierbar. Dies kann zu unvorhersehbaren Belastungen im Haushalt führen. Der Grundsatz der Haushaltswahrheit verpflichtet jedoch den öffentlichen Sektor zur genauen und transparenten Angabe von Einnahmen und Ausgaben.[89] Zwar können die Einnahmen (z.B. Gebühren zur Haftungsübernahme) präzise beziffert werden. Da die Kosten und Risiken einer Haftungsübernahme schwer vorhersehbar sind, würde dies zu Unsicherheiten und potenziellen Verstößen gegen diesen Grundsatz führen würde.[90]

Eine Finanzierung der UDM über Steuergelder und damit eine Haftungsübernahme wäre daher nur denkbar, wenn der Aufbau einer UDM samt verlässlichen, nutzbaren Daten im öffentlichen Gemeininteresse stünde (ob der Aufbau und Betrieb einer UDM verpflichtend für Kommunen sein kann, wird der Betrieb einer UDM zur öffentlich-rechtlichen Daseinsvorsorge?" behandelt.). Jedenfalls bedarf die

---

[87] Haushaltsordnung der Freien und Hansestadt Hamburg (Landeshaushaltsordnung - LHO); vom 17. Dezember 2013 (HmbGVBl S. 503), zuletzt geändert am 27. April 2021 (HmbGVBl. S. 283, 284).

[88] *Kilian* in: Schulte/Kloos, Handbuch Öffentliches Wirtschaftsrecht, § 4 Das Recht der Haushalte, Rn. 66.

[89] *Kilian* in: Schulte/Kloos, Handbuch Öffentliches Wirtschaftsrecht, § 4 Das Recht der Haushalte, Rn. 66.

[90] *Kilian* in: Schulte/Kloos, Handbuch Öffentliches Wirtschaftsrecht, § 4 Das Recht der Haushalte, Rn. 66.

Übernahme von Haftungsrisiken durch den Staat einer klaren gesetzlichen Regelung, die derzeit nicht existiert. Die Übernahme eines derart großen wirtschaftlichen Risikos stellt eine wesentliche Entscheidung dar, die der Gesetzgeber selbst zu treffen hat und nicht der Verwaltung überlassen darf. [91] Insoweit müsste der Gesetzgeber erst eine entsprechende Rechtsgrundlage in Form eines parlamentarischen Gesetzes schaffen, was einen längeren legislativen Prozess erfordert.[92] Bis eine solche Rechtsgrundlage vorhanden ist, bleibt eine Versicherungslösung nicht umsetzbar.

3.2.5 Datenschutzrechtliche Einordnung

Auch Use Case 2 erfordert eine sorgfältige datenschutzrechtliche Bewertung und der Implementierung umfassender technischer und organisatorischer Maßnahmen, um den Anforderungen der DS-GVO gerecht zu werden.

3.2.5.1 Anwendbarkeit des Datenschutzrechts

Vorliegend werden durch die autonomen Fahrzeuge insbesondere Kameraaufnahmen der Umgebung zu Zwecken der Navigation genutzt. Hierbei können personenbezogene Daten i. S. d. Art. 4 Nr. 1 DS-GVO erfasst werden, soweit andere Verkehrsteilnehmer:innen oder auch Kfz-Kennzeichen aufgenommen werden. Ein Blurren (Unkenntlichmachen) der Bilder soll erst nach Übertragung auf einen zentralen Speicher erfolgen, sodass personenbezogene Daten i. S. d. Art. 4 Nr. 1 DS-GVO bis zu diesem Zeitpunkt nach Art. 4 Nr. 2 DS-GVO verarbeitet werden. Da somit keine Sofortanonymisierung erfolgt, ist die DS-GVO grundsätzlich anwendbar.

Auch könnten unter Umständen bei der Speicherung und Verarbeitung von Landmarken Rückschlüsse auf Personen oder private Grundstücke gezogen werden, die datenschutzrechtlich i. S. d. Art. 4 Nr. 1 DS-GVO relevant werden könnten. Anders ist dies bezüglich allgemeiner Objektdaten, wie Baustellen oder Straßenschildern, welche in der Regel keinen Personenbezug aufweisen und daher nicht unter den Schutzbereich der DS-GVO fallen.

3.2.5.2 Möglichkeiten zur Abwendung datenschutzrechtlicher Verpflichtungen

Damit erfordert auch die Umsetzung des Use Case 2 mit der Erfassung und Verwendung möglicherweise personenbezogener Objektdaten zur effizienten Navigation autonomer Fahrzeuge innerhalb einer UDM, Strategien zur Umgehung der Anwendbarkeit von Datenschutzregelungen wie der DS-GVO. Allerdings wäre derzeit die Umsetzung von geschlossenen Systemen oder automatischer Anonymisierungen als effektive Werkzeuge einer derartigen Umgehung im geplanten UDM wohl nicht möglich.

3.2.5.2.1 Geschlossene Systeme

Eine Umgehung der DS-GVO-Vorschriften durch Implementierung eines geschlossenen Systems, erfordert mehrere technische und organisatorische Maßnahmen, die wohl im vorliegenden Use Case nicht umgesetzt werden können.

Um ein solches geschlossenes System zu gestalten, müssten Sensoren und Kameras, welche die Umgebungsdaten erfassen, diese sofort abstrahieren. Beispielsweise könnten Fußgänger:innen als einfache geometrische Formen oder als “Objekt A” dargestellt werden. Dadurch wird sichergestellt, dass keine

[92] BVerfGE 49, 89 (126 f.); BVerfGE 57, 295 (327); BVerfGE 83, 130 (142), BVerfGE 101, 1 (34).

Personenbezogenheit der Daten i. S. d. Art. 4 Nr. 1 DS-GVO besteht. Die innerhalb des Systems verarbeiteten Daten werden technisch gesichert und nach ihrer Verwendung gelöscht. Es erfolgt lediglich eine Aggregierung und Kategorisierung der Daten, wobei der Output nur zur unmittelbaren Reaktion und Gefahrvermeidung weitergegeben wird.

Zudem hat die gesamte Verarbeitung der Objektdaten innerhalb dieses geschlossenen Systems stattzufinden. Dies bedeutet, dass keine Daten an externe Server oder Cloud-Dienste gesendet werden dürfen. Alle Verarbeitungsschritte haben innerhalb des Systems zu erfolgen, sodass eine vollständige Kontrolle und Sicherung der Daten gewährleistet wird.

Im vorliegenden Use Case sollen die Daten jedoch sowohl durch die einzelnen Fahrzeuge als auch durch die Verkehrsinfrastruktur gesammelt und in der UDM zusammengeführt werden. Dies erfordert eine zunehmenden Datensammlung und -analyse der konkreten Verkehrsdaten, welche auch personenbezogene Daten umfassen. Dadurch soll die UDM anhand abstrahierter Objektdaten eine sichere und zuverlässige Navigation des Fahrzeugs durch den öffentlichen Straßenverkehr gewährleisten. Damit widerspricht das derzeitige Projekt den Voraussetzungen der strikten Datenisolierung und –abstraktion eines geschlossenen Systems, sodass insofern die Anwendbarkeit der DS-GVO nicht ausgeschlossen werden kann.

3.2.5.2.2 (Automatische) Anonymisierung

Ein weiteres Werkzeug zur Abwendung der Anwendbarkeit der DS-GVO wäre auch im Use Case 2 die automatische Anonymisierung der Daten, sodass der Personenbezug i.S.d. Art. 4 Nr. 1 DS-GVO nicht mehr besteht und auch nicht mehr wiederherstellbar wäre, vgl. Erwägungsgrund Nr. 26 zur DS-GVO.

Die in Echtzeit erfassten Daten werden bereits im Fahrzeug anonymisiert , bevor sie an die UDM übertragen werden. Diese Anonymisierung im Fahrzeug könnte durch eine Pixelierung oder ein Blurring der Bilder im Hinblick auf personenidentifizierbare Merkmale, wie Gesichter oder Kfz-Kennzeichen umgesetzt werden. Zudem könnten Objekte als abstrakte Klassen dargestellt werden, wie beispielsweise “bewegliches Hindernis” statt eines spezifischen Verkehrsteilnehmenden. Dies senkt das Risiko, dass identifizierbare Informationen offengelegt werden könnten und ermöglicht, dass nur anonymisierte Daten in die UDM integriert werden, die keine Rückschlüsse auf einzelne Personen zulassen.

Trotz der Reduktion der datenschutzrechtlichen Implikationen durch die Anonymisierung im Fahrzeug ist es wichtig zu differenzieren, ob die Fahrzeuge durch die Betreiber:innen der UDM oder durch Dritte betrieben werden. Falls die Fahrzeuge durch die Betreiber:in der UDM betrieben werden, trägt diese:r weiterhin die Verantwortung dafür, dass die anonymisierten Daten gemäß den Bestimmungen der DS-GVO verarbeitet und genutzt werden. Auch wenn “saubere”, also anonymisierte Daten, in die UDM eingespeist werden, verbleibt die Pflicht der Betreiber:innen, sicherzustellen, dass diese Daten im Einklang mit den Anforderungen der DS-GVO behandelt werden. Dies beinhaltet den Schutz der Daten während ihrer Speicherung und Verarbeitung in der UDM, um zu verhindern, dass die Anonymisierung umgangen oder die Informationen re-identifiziert werden können.

So könnten Daten, selbst wenn Gesichter und Kfz-Kennzeichen in den Bilddaten unkenntlich gemacht wurden, durch den Abgleich mit anderen Informationen, wie etwa den zeitlichen und räumlichen Kontexten oder durch die Aggregation mit anderen öffentlich zugänglichen Datenquellen, möglicherweise re-identifiziert werden. So könnte z.B. ein bestimmtes Fahrzeug an einer bekannten Position zu einer bestimmten Zeit erkannt werden, was unter Umständen auf die Identität des:r Fahrer:in schließen lässt. Ein weiterer Ansatz zur Anonymisierung wäre die Datenaggregation. Durch das Zusammenfassen von Daten zu größeren Einheiten könnten individuelle Informationen verwischt werden, sodass kein direkter Personenbezug mehr erkennbar ist. Allerdings ist dies lediglich hinsichtlich der Analyse

von Bewegungsmustern von Personen zur Darstellung allgemeiner Verkehrstrends bzw. VRU-Hotspots sinnvoll, wie in Use Cases 1 und 4 ausgeführt wird.

Im vorliegenden Use Case 2 sind hingegen punktuelle Objekt- und Personendaten entscheidend, um die Navigation des Fahrzeugs im Straßenverkehr zu gewährleisten und insbesondere mögliche Unfälle zu vermeiden. Eine Aggregation der Daten mehrerer Verkehrsteilnehmenden zur Darstellung von Verkehrstrends ist in diesem Fall nicht praktikabel, da sie nicht die detaillierten und kurzfristigen Informationen liefert, die für kurzfristig erforderliche Ausweichmanöver notwendig sind.

Die geplante Vorgehensweise der Anonymisierung der Daten im Fahrzeug vor Übermittlung an die UDM kann das Risiko im Hinblick auf die Anwendbarkeit der DS-GVO in diesem Kontext des EDDY-Projekts reduzieren, aber nicht vollständig ausschließen. Die Verantwortung für den rechtmäßigen Umgang mit den Daten nach der DS-GVO bleibt bestehen und muss durch geeignete Maßnahmen gewährleistet werden.

3.2.5.3 Rechtmäßigkeit der Verarbeitung

Da die Anwendung der oben beschriebenen Systeme im derzeitigen Stand des Projekts nicht möglich ist, ist die Verarbeitung und Speicherung der personenbezogenen Daten durch die öffentliche Stelle i.S.d. § 2 Abs. 4 S. 2 BDSG nur aufgrund einer rechtlichen Grundlage möglich. Auch hierfür wird ein Rechtfertigungsgrund gemäß Art. 6 DS-GVO erforderlich.

Eine mögliche Rechtfertigung könnte gem. Art. 6 Abs. 1 lit. e DS-GVO erfolgen, wonach die Verarbeitung personenbezogener Daten durch öffentliche Stellen dann zulässig ist, wenn diese zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich ist. Die Erfassung und Verarbeitung abstrahierter Objektdaten, welche unter Umständen Personenbezug haben und der Verbesserung der Verkehrssicherheit und Navigation im öffentlichen Straßenverkehr dienen, stellt eine derartige öffentliche Aufgabe dar. Insoweit ist die Datenverarbeitung auch verhältnismäßig, da die Kamera- und Sensorikdaten im EDDY-Projekt nur kurzzeitig in die UDM eingespeist wird, um potenzielle Kollisionen mit anderen Verkehrsteilnehmer:innen zu vermeiden. Dies geschieht in Echtzeit, ohne dass durch einen vorherigen Prozess die Daten anonymisiert werden. Anschließend erfolgt eine sofortige und automatische Löschung der Daten aus dem System.

Eine Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DS-GVO als Rechtfertigungsgrund ist insoweit nicht praxistauglich. Eine solche Einwilligung müsste explizit eingeholt werden. Eine konkludente bzw. hypothetische Einwilligung, wie sie bei einer Datenverarbeitung zur Kollisionsvermeidung wohl jederzeit von Verkehrsteilnehmenden abgegeben werden würde, ist in der DS-GVO nicht geregelt. Aufgrund der kurzen Reaktionszeit des Fahrzeugs ist daher die Einholung einer derartigen Einwilligung damit praktisch nicht umsetzbar.

Allerdings wird Art. 6 Abs. 1 lit. f DS-GVO als Rechtfertigungsgrund einschlägig sein, der die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des Verantwortlichen erlaubt, sofern nicht die Interessen oder Grundrechte der betroffenen Personen überwiegen. Dies trifft insbesondere zu, wenn die Verarbeitung der Daten dazu dient, die Sicherheit und Effizienz der Fahrzeuge zu verbessern, ohne dabei übermäßig in die Rechte der betroffenen Personen einzugreifen. Die Datenerhebung erfolgt hier konkret zum Zwecke der Sicherung der Grundrechte der betroffenen Person, insbesondere des Art. 2 Abs. 1 GG, da diese zur Kollisionsvermeidung erfolgt und verarbeitet wird.

Insgesamt ist jedoch entscheidend, die Datenschutzrechte der betroffenen Personen zu wahren und gleichzeitig das öffentliche Interesse an Sicherheit und effizienten Verkehrsmanagement optimal zu

gewährleisten. Insoweit sind die Hinweispflichten nach Art. 13 Abs. 1 DS-GVO und die Betroffenenrechte der DS-GVO wie in 3.1.3.4. bzw. 3.1.3.5. beschrieben zu berücksichtigen.

3.2.6 Fazit

Es besteht (noch) kein Haftungsregime für die inhaltliche Richtigkeit von Daten. Solange die in den Daten enthaltenen Informationen rechtlich nicht verbindlich oder verlässlich sind, sind diese für die technische Nutzung und Entwicklung uninteressant. Durch die fehlende Verlässlichkeit werden Entwicklungs- und Digitalisierungsprozesse im Verkehr gebremst. Ohne ein Haftungsregime für die Daten bleiben diese und ihr Potential weitgehend ungenutzt. Deshalb besteht hier EU-weit Forschungs- und Handlungsbedarf. Die Entwicklung eines Europäischen Haftungsrahmens für Daten ist an dieser Stelle nicht möglich. Dieses Ergebnis ist vor allem vor dem Hintergrund unbefriedigend, dass viele Hersteller in der Verkehrs-Industrie Daten brauchen, um ihre „smarten" Produkte zu betreiben. Große Player, wie z.B. Google Maps haften auch nicht für die von Ihnen bereitgestellten Daten.

Haftungsfragen aus produkthaftungsrechtlicher Sicht können sich bei dem Betrieb der UDM trotzdem ergeben.

Grundsätzlich könnte ein Teil der Daten bzw. Daten einer gewissen Qualität auch gegen eine Gebühr zur Verfügung gestellt werden, um den Betrieb einer UDM zu finanzieren. Um den Daten eine gewisse Verbindlichkeit zu geben, müsste der/die Betreiber:in Haftung für die inhaltliche Richtigkeit der Daten übernehmen. Wenn die UDM durch die öffentliche Hand betrieben wird, ist fraglich, ob eine solche Vereinbarung mit den Haushaltsgrundsätzen vereinbar ist, jedenfalls müsste aber eine entsprechende Rechtsgrundlage geschaffen werden.

Sowohl bei dem Einsatz von Kameras als auch von LiDAR werden meist personenbezogene Daten erfasst, sodass die DS-GVO beachtet werden muss. Die Anwendbarkeit der DS-GVO kann umgangen werden durch eine sog. automatische Anonymisierung oder durch die Verwendung von geschlossenen Systemen. Für die UDM ist aber beides wohl nicht realisierbar.

3.3 Use Case 3: Dynamische Zusatzinfos – weitere Daten und Datenweitergabe

Verkehrsteilnehmende können Daten auch selbst mit der UDM teilen. Dafür müssen sie in die Verarbeitung ihrer personenbezogenen Daten einwilligen. Diese Einwilligung muss freiwillig erfolgen und setzt eine informierte aktive Entscheidung der Nutzer:innen voraus. Die Beweislast für die grundsätzlich formfreie Einwilligung zur Datenverarbeitung liegt bei den Betreiber:innen, was bedeutet, dass diese im Zweifelsfall nachweisen müssen, dass der/die Nutzer:in eingewilligt hat. Für die Betreiber:innen ist es somit nützlich die Einwilligung in irgendeiner Form zu speichern. Die Einwilligung zur Datenverarbeitung bezieht sich auf einen bestimmten Zweck, für welchen die Daten genutzt werden. Bei Änderung des Zweckes ist eine neue Einwilligung erforderlich. Wird die Einwilligung widerrufen oder sind die genutzten Daten für den ursprünglichen Zweck nicht mehr notwendig, so müssen die Daten gelöscht werden. Werden Daten nur in anonymisierter Form erfasst und verarbeitet, ist aufgrund der fehlenden Identifizierbarkeit der Person die DS-GVO nicht anwendbar und damit keine Einwilligung erforderlich.

Die Nutzung von Scootern von Voi kann zur weiteren Datensammlung beitragen. Es ist zu beachten, dass es sich bei Standortdaten, selbst bei Aggregation von Datensätzen, meistens (höchstens) um eine Pseudonymisierung und nicht um eine Anonymisierung handelt, so dass eine Einwilligung in die Verarbeitung erforderlich bleibt. Wann immer natürliche Personen anhand der Daten noch re-identifizierbar sind, auch in Verbindung mit weiteren Informationen, sind die Daten höchstens pseudonymisiert. Die Frage, ob natürliche Personen re-identifizierbar sind, sollten sich die Betreiber:innen der UDM immer zur Kontrolle stellen, ob die DS-GVO beachtet werden muss.

Der stationslose Rollerverleih gehört in Hamburg zum öffentlichen Gemeingebrauch und benötigt demnach keine Genehmigung von öffentlicher Seite. Dass Voi Daten mit der Stadt teilen muss, kann demnach nicht von einer Sondernutzungserlaubnis für den Rollerverleih abhängig gemacht werden.

3.3.1 Sachverhalt

Wie bereits in den anderen Use Cases beschrieben wurde, werden die Daten aus vielfältigen Quellen in die UDM eingespeist. Zum einen **erfasst das EDDY-Fahrzeug** selbst Objektdaten, kartiert diese und sendet sie an die UDM.

Weiterhin detektieren auch **andere Verkehrsteilnehmende** Daten **über die Umgebung** und leiten diese direkt an die UDM weiter. Die Infrastruktur und/oder die Fahrzeuge sammeln V2X-Daten (Vehicle to Everything) und die UDM stellt sodann daraus aggregierte Live-Informationen bereit. Aufgrund der Echtzeit-Daten kann das Fahrzeug sein Fahrverhalten anpassen und so besser, sicherer und ökologischer fahren.

Verkehrsteilnehmende können Daten **über sich selbst** teilen und der UDM als Objektinformation zur Verfügung stellen, zum Beispiel per App (Was für ein Road-user/Fahrzeugtyp, Weg, Geschwindigkeit). Diese Daten werden in der UDM aufbereitet und bereitgestellt. So könnte beispielsweise ein Fußgänger seinen Weg und seinen Standort teilen, sodass er auf der UDM als 3D-Objekt mitsamt Trajektorie dargestellt wird.

Auch E-Scooter sollen zur Ausgestaltung der UDM eingesetzt werden können. Die Scooter der Firma „Voi“ werden dazu mit Messboxen von ConsiderIT ausgestattet, die verschiedene Messwerte erfassen. Die Scooter können damit eine statistische Aufbereitung ihrer Nutzung der UDM zur Verfügung stellen, indem sie alle Daten mit ihr teilen. Diese werden an die UDM übermittelt. Bei Messung dieser Daten soll der/die Scooter-Nutzer:in, der/die das Fahrzeug per App gemietet hat, „anonymisiert“ werden. Die Scooter sollen im normalen Betrieb fahren.

3.3.2 Datenschutzrechtliche Einordnung

Anders als in den vorherigen Use Cases, bei denen es um die (persönlichen) Daten geht, die per Sensorik **passiv** erhoben werden, behandelt dieser Use Case Daten, welche aktiv von Verkehrsteilnehmenden mit der UDM geteilt werden. Insofern werden hier Themen wie die Form und Reichweite der Einwilligung zur Datenverarbeitung und einer Löschung der personenbezogenen Daten relevant.

In Bezug auf den Einsatz von E-Scootern zur Datenerhebung ist insbesondere interessant, ob es ausreicht, wenn der oder die Fahrer:in während des Vorgangs der Datenteilung „anonym" ist, oder ob weitere rechtliche Maßnahmen notwendig sind.

Wenn anhand der (Mobilitäts-)Daten Personen identifiziert werden können, sind diese persönliche Daten im Sinne der Datenschutz-Grundverordnung (DS-GVO)[93]. Insbesondere bei Fahrzeugdaten handelt es sich meist um personenbezogene Daten, sodass der Anwendungsbereich der DS-GVO eröffnet ist und die Datenverarbeitung rechtmäßig sein muss.[94]

3.3.2.1 Möglichkeiten zur Abwendung datenschutzrechtlicher Pflichten

Anonymisieren meint das Verändern personenbezogener Daten, so dass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht, respektive nicht mehr identifiziert werden kann.[95] Für anonymisierte Datensätze findet mangels der möglichen Identifizierbarkeit die DS-GVO keine Anwendung.[96]

Auch wenn der EDDY-Server keine Anbindung an die Infrastruktur von Voi hat, heißt dies nicht automatisch, dass die Daten der Scooter-Nutzer:innen anonym sind. Zwar wird in der UDM nicht der Name der Person angezeigt, die den Scooter bewegt, obwohl diese Person sich vorher bei Voi mit ihrem Namen und dem Nachweis der Fahrerlaubnis in der Voi-App einloggte.
Wenn die Nutzer:innen der Scooter wie andere Verkehrsteilnehmende in der UDM angezeigt werden, sind diese aufgrund ihrer Standorte identifizierbar.

Bei der Frage nach der Identifizierbarkeit einer Person, sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person wahrscheinlich genutzt werden. Es sind die zum Zeitpunkt der Verarbeitung verfügbaren Technologien und technologischen Entwicklungen zu berücksichtigen.[97] Aufgrund der zunehmenden Möglichkeiten mit technischen Mitteln scheinbar anonyme Daten dennoch den Betroffenen zuzuordnen, kann ohnehin weit seltener von anonymen Daten gesprochen werden.[98] Der Name der Scooter-Fahrer:in wird zwar nicht in der UDM angezeigt, allerdings kann aufgrund der live geteilten Standortdaten eine Person identifiziert werden.[99] Die Daten der Scooter-Fahrer:innen sind damit als personenbezogen zu qualifizieren und nicht anonym. Damit findet die DS-GVO Anwendung, mitsamt der für die UDM-nutzenden Verkehrsteilnehmenden skizzierten Rechte. Dies ist anders zu qualifizieren, wenn die Nutzer:innen der Scooter nicht als Verkehrsteilnehmende in der UDM angezeigt werden, sondern nur andere per Scooter erhobene Daten eingespeist werden.

Durch Aggregierung von Datensätzen, also die Zusammenführung mehrerer personenbezogener Datensätze zu einem Gruppendatensatz, aus dem heraus nicht mehr festgestellt werden kann, wem

---

[93] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[94] *Steege*, MMR 2019, 508 (511).

[95] *Ernst* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO Rn. 48.

[96] Erwägungsgrund 26, S. 5 zur DS-GVO.

[97] Erwägungsgrund 26, S. 3, 4 zur DS-GVO.

[98] *Ernst* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO Rn. 50.

[99] Hierzu ein Beispiel: Auf der UDM wird angezeigt, dass an einer Kreuzung nur ein Scooter-Nutzer an einer roten Ampel steht. Wenn ein:e Autofahrer:in, der oder die ebenfalls die UDM nutzt, an derselben Kreuzung steht, kann er mit einem Blick den oder die in der UDM angezeigten Nutzer:in dem oder der Scooter-Fahrer:in an der Kreuzung zuordnen.

innerhalb dieses Datenkonglomerats welche Einzeldatensätze zuzuordnen sind, ist eine Anonymisierung möglich.[100]

Aggregierte Mobilitätsdatensätze, bei denen Daten nicht „vereinzelt" („singling-out") werden können, und historische Daten gelten als anonymisiert, wenn die natürliche Person nicht aufgrund der Daten re-identifizierbar ist. Allerdings ist eine Anonymisierung nicht immer möglich, wenn noch ein nutzbares Datenset bestehen bleiben soll. In manchen Fällen kann die Gefahr einer möglichen Re-Identifizierung nicht weit genug abgesenkt werden, damit das Datenset als anonym gilt. Dies ist zum Beispiel der Fall, wenn die Gesamtanzahl der natürlichen Personen in dem Set zu gering ist, wenn das Datenset viele demographische Attribute oder ggf. Standortdaten beinhaltet.[101] Auch die Veröffentlichung von aggregierten Mobilitätsdaten kann zur Verletzung der Privatsphäre führen, da es möglich ist, aus den aggregierten Mobilitätsdaten (ohne Vorkenntnisse) die Trajektorien von Einzelpersonen zu ermitteln. Eine Generalisierung oder Beeinflussung der Datensätze kann erforderlich sein, um Anonymität zu gewährleisten.[102] Wann immer Standortdaten in der UDM angezeigt werden, muss den Betreiber:innen klar sein, ob natürliche Personen unter Berücksichtigung aller Mittel, die (vernünftigerweise) von dem für die Verarbeitung Verantwortlichen oder einer dritten Person verwendet werden können, re-identifiziert werden können. Zur Beantwortung dieser Frage kann die folgende Grafik zur Selbstkontrolle genutzt werden.

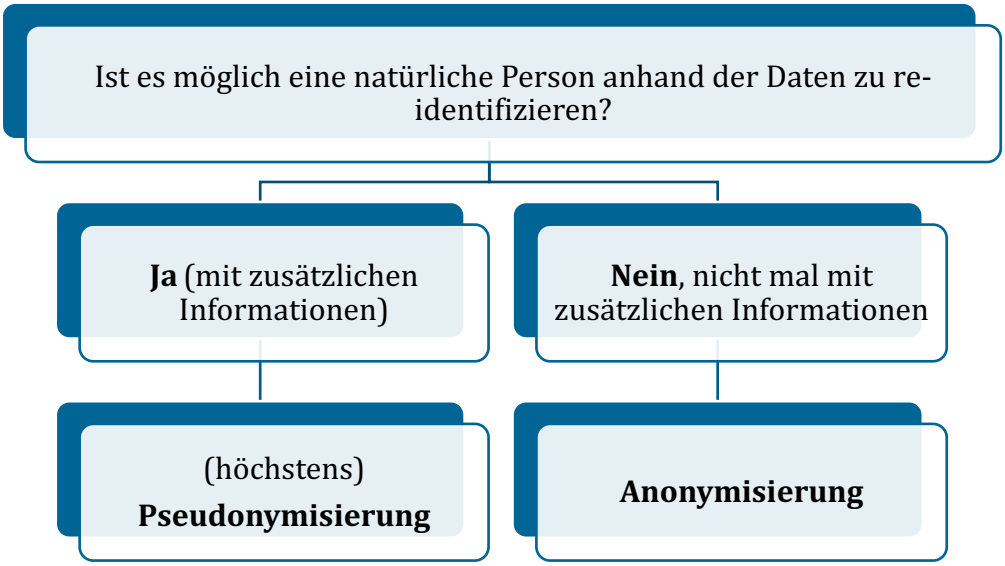

Abbildung 2: Kontrollfrage: Pseudonymisierung oder Anonymisierung?[103]

Wenn die Daten der Scooter nur genutzt werden, um Gefahrenbereiche anzuzeigen, weil hierdurch ein „**Hotspot**" an Scootern und das Fahrverhalten der Scooter-Nutzer:innen (viel Stop-and-Go, viel Bremsen etc.) ein erhöhtes Verkehrsaufkommen festgestellt wird, wären diese Datensätze (wohl)

[100] *Ernst* in: Paal/Pauly, DS-GVO BDSG, Art. 4 DS-GVO Rn. 49.

[101] *Xu/Tu/Li/Zhang/Fu/Jin*, Trajectory Recovery From Ash: User Privacy is NOT Preserved in Aggregated Mobility Data, April 2017 (in the proceedings of the 26th international conference on world wide web pp. 1241-1250), p. 1241, https://dl.acm.org/doi/abs/10.1145/3038912.3052620.

[102] Xu/Tu/Li/Zhang/Jin, p. 1249 https://dl.acm.org/doi/abs/10.1145/3038912.3052620.

[103] Eigene Darstellung des IKEM 2024.

anonymisiert. Aus der Tatsache, dass in der UDM ein Gefahrenbereich/Hotspot angezeigt wird, lassen sich einzelne Scooter-Fahrer:innen nicht identifizieren.

Im Ergebnis bedeutet dies, dass wenn die Scooter-Fahrer:innen als Verkehrsteilnehmende in der UDM angezeigt werden, eine Anonymisierung nicht gegeben ist. Eine Anonymisierung lässt sich nur herstellen, wenn die Scooter-Nutzer:innen nicht als Verkehrsteilnehmende in der UDM angezeigt werden. Demnach sind für eine Anonymisierung der Daten UDM-interne Schritte notwendig. Es ist zu beachten, dass Datensätze nicht vorschnell als anonym qualifiziert werden sollten.

Die DS-GVO ist daher auch bei der Darstellung der Scooter-Fahrer:innen in der UDM anwendbar und muss eingehalten werden. Wenn die betroffenen Scooter-Fahrer:innen wirksam in die Datenverarbeitung einwilligen, können so jedoch die datenschutzrechtlichen Vorgaben der DS-GVO eingehalten werden. Es müssen die gleichen allgemeinen Vorgaben für die Einwilligung eingehalten werden, wie sie oben dargestellt wurden, vgl. Kapitel 3.2.5.3.

3.3.2.2 Rechtmäßigkeit der Verarbeitung

3.3.2.2.1 Einwilligung (Allgemeine Anforderungen)

Wenn eine Person Daten über sich selbst mit der UDM teilt, muss sie in diese Datenverarbeitung einwilligen. Die Einwilligung muss in der angemessenen Form erfolgen und die Reichweite der Einwilligung muss die tatsächliche Datenverarbeitung abdecken. Außerdem müssen weitere Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden, unter anderem das Gebot der Zweckbindung. Eine Darstellung aller Grundsätze zur Datenverarbeitung würde den Rahmen dieses Gutachtens übersteigen.

Die Einwilligung im Sinne der DS-GVO bezeichnet nach Art. 4 Nr. 11 DS-GVO von „*der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.*“ Art. 7 DS-GVO regelt die Bedingungen für eine wirksame Einwilligung.

3.3.2.2.1.1 Form und Reichweite

Die DS-GVO sieht für die Erteilung der Einwilligung **kein (Schrift-)Formerfordernis** vor. Die Formfreiheit bedeutet gleichzeitig, dass es zu Einbußen an Rechtsicherheit hinsichtlich des Bestehens einer Einwilligung als Zulässigkeitstatbestand für die Verarbeitung der Daten kommen kann.[104] Die Einwilligung kann auch elektronisch erklärt werden, sodass der Erklärungswille digital dokumentiert wird. Dies kann durch Anklicken eines Kästchens bei Nutzung einer Anwendung erfolgen oder durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen mangels einer bestätigenden **Handlung** keine wirksame Form der Einwilligung dar.[105] Bei einer Aufforderung zur Einwilligung in elektronischer Form, muss die Aufforderung selbst in klarer, knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.[106]

---

[104] *Buchner/Kühling* in: Kühling/Buchner, DS-GVO BDSG, Art. 7 DS-GVO Rn. 27.

[105] Vgl. Erwägungsgrund 32 S.2, 3 zur DS-GVO, Hervorhebung wurde durch die Autorin hinzugefügt.

[106] Erwägungsgrund 32, S.6 zur DS-GVO.

Insbesondere für den Verarbeiter der Daten ist es sinnvoll die Einwilligung ausdrücklich einzuholen und zu dokumentieren. Die datenverarbeitende Stelle nach Art. 7 Abs. 1 DS-GVO trägt die Beweislast dafür, dass die betroffene Person in die Datenverarbeitung eingewilligt hat.[107] Beweislast heißt, dass die beweisbelastete Partei das tatsächliche Vorliegen eines Umstands beweisen muss. Die verarbeitenden Stellen, die die Beweislast tragen, sind die Betreiber:innen der UDM.

Auch im Datenschutzrecht, wie im Allgemeinen Zivilrecht, wird die Einwilligung als vorherige Zustimmung verstanden. Sie muss **vor der tatsächlichen Datenverarbeitung** erteilt werden.[108] Ein „Verfallsdatum" für die Einwilligung gibt es nicht. Eine „Erneuerung" der Einwilligung nach bestimmten Fristen ist damit nicht notwendig, kann jedoch in Einzelfällen zu empfehlen sein.[109] Hier spielt wieder eine Rolle, dass die Betreiber:innen der UDM als datenverarbeitende Stellen die Beweislast tragen. Damit müssen die Betreiber:innen im Zweifel beweisen können, dass eine ältere Einwilligung den aktuellen Datenverarbeitungsvorgang noch abdeckt.

In Bezug auf zeitliche Grenzen sollte außerdem das sog. „Recht auf Vergessen(werden)"[110] beachtet werden, welches in Art 17 Abs. 1 a) DS-GVO umgesetzt wurde. Danach hat die betroffene Person das Recht, dass ihre Daten, wenn diese für den Zweck nicht mehr benötigt werden, gelöscht werden. Da die Aspekte der Reichweite der Einwilligung, der Zweckbindung und der Löschung eng miteinander verknüpft sind, wird im Folgenden genauer auf die Zweckbindung der Datenverarbeitung und die Löschungsrechte eingegangen.

3.3.2.2.1.2 Zweckbindung

Laut Art. 4 Nr. 11 DS-GVO muss die Einwilligung für einen bestimmten Fall erteilt werden. Die Einwilligung muss sich auf alle zu demselben Zweck vorgenommenen Verarbeitungen beziehen. Wenn die Verarbeitung mehreren Zwecken dient, müssen für alle Verarbeitungszwecke Einwilligungen gegeben werden.[111] Pauschal- und Blankoeinwilligungen sind unzulässig.[112] Eine Zweckänderung ist nach Art. 5 Abs. 1 b) DS-GVO grundsätzlich unzulässig. Personenbezogene Daten dürfen nur für diejenigen Zwecke weiterverarbeitet werden, für die sie erhoben worden sind; Ausnahmen sind jedoch möglich, vgl. Art. 6 Abs. 4 DS-GVO.[113] Für den Betreiber der UDM ist es daher wichtig, den Zweck oder die Zwecke der Datenverarbeitung genau und eindeutig anzugeben. Insbesondere wenn die Daten von anderen Verkehrsplanenden genutzt werden sollen, muss auch dieser Zweck und natürlich die Weitergabe von der Einwilligung der betroffenen Personen umfasst sein. Der Zweck der Datenverarbeitung darf nicht nachträglich verändert werden. Wenn sich die Verwendung zu einem anderen Zweck als bisher geplant abzeichnet, bleibt dem Verwender der UDM die Möglichkeit, eine erneute, diesen Zweck umfassende Einwilligung abzugeben. Dieser muss dann wieder klar und eindeutig angegeben werden, da Blanko- und Pauschaleinwilligungen unzulässig sind.

---

[107] *Buchner/Kühling* in: Kühling/Buchner, DS-GVO BDSG, Art. 7 DS-GVO Rn. 27.

[108] *Buchner/Kühling* in Kühling/Buchner, DS-GVO BDSG, Art. 7 DS-GVO Rn. 30.

[109] *Stemmer* in Wolff/Brink: BeckOK Datenschutzrecht, Art. 7 DS-GVO, Rn. 88.

[110] Grundrechtsgestützt entwarf der EuGH ein „Recht auf Vergessenwerden" gegen einen Internetsuchmaschienenbetreiber (vgl. EuGH, Urteil vom 08.04.2014 – C-293/12, C-594/12); dieses wurde nach dem genannten Grundsatzurteil in Art. 17 DS-GVO im Sekundärrecht der EU umgesetzt, vgl. *Kühling*, NJW 2020, 275 (275).

[111] Vgl. Erwägungsgrund 25 zur DS-GVO.

[112] *Stemmer* in: BeckOK Datenschutzrecht, Wolff/Brink, Art. 7 DS-GVO, Rn. 78.

[113] *Pötters* in: Gola/Heckmann, DS-GVO BDSG, Art. 5 DS-GVO, Rn. 19.

3.3.2.2.2 Ausgestaltung der Einwilligung bei Scooter-Nutzung

Nicht personenbezogene oder anonymisierte Daten kann Voi an die Stadt als Betreiberin der UDM ohne die Einwilligung der Person, bei der sie erhoben wurden, weitergeben.

In Bezug auf personenbezogene Daten muss bei der Weitergabe der Daten an die UDM die DS-GVO beachtet werden, insbesondere muss eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllt sein, damit die Verarbeitung rechtmäßig ist.

Neben der Einwilligung ist die Datenverarbeitung regelmäßig auch dann rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrages dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen (**Art. 6 Abs. 1 lit. b) DS-GVO).** Die Weitergabe der Daten der Nutzenden wird regelmäßig nicht für die Erfüllung des Mietvertrags des Rollers erforderlich sein. Es ist auch nicht ersichtlich, dass das Interesse von Voi als Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO die Interessen der betroffenen Personen am Schutz ihrer Daten i.S.d. **Art. 6 Abs. 1 lit. f) DS-GVO** überwiegt. Zwar hat Voi in der Regel ein starkes wirtschaftliches Interesse die Daten der Nutzenden nicht nur an die UDM weiterzugeben. Diese Interessen werden aber nicht das Interesse der Betroffenen am Schutz ihrer Daten überwiegen.

Da die anderen Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO regelmäßig nicht vorliegen werden, kommt es auf eine wirksame Einwilligung der betroffenen Person zur Weitergabe der Daten an. Grundsätzlich muss die Einwilligung nach **Art. 6 Abs. 1 a) DS-GVO** derjenigen Person gegenüber erfolgen, welche die Daten verarbeitet. Wenn jedoch Nutzende den Scooter bei Voi per App mieten, haben sie keinen direkten Kontakt zu den Betreiber:innen der UDM.

Die Einwilligung zur Weitergabe der Daten an und die Nutzung dieser durch die Betreiber:innen der UDM muss demnach schon **im Vertrag zwischen dem Transportdienstleister Voi und den Nutzenden** erfolgen. Wie oben dargestellt, muss diese Weitergabe und die Nutzung sowie deren Zwecke klar und verständlich dargestellt werden, damit die Einwilligung wirksam ist. Durch die Vorgaben der DS-GVO muss der Verkehrsdienstleister die Einwilligung der Betroffenen vor Weitergabe einholen.

Außerdem muss die Einwilligung der Betroffenen freiwillig erfolgen, **vgl. Art. 7 Abs. 4 DS-GVO**. Eine Kopplung von Vertragsschluss und Einwilligung ist nicht zulässig (**sog. Kopplungsverbot**).[114] Die Einwilligung gilt dann als „freiwillig", wenn sie frei erfolgt ist und eine echte oder freie Wahl bestand und die betroffene Person in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.[115] Der Abschluss des Mietvertrages des Scooters zwischen Voi und den Nutzenden darf somit **nicht davon abhängig gemacht werden, ob die Einwilligung zur Weiterleitung der Daten an die UDM erteilt wird.**

Verschiedenen Verleihern von E-Rollern wurde in der Vergangenheit eine Reihe von Datenschutzverstößen vorgeworfen.[116] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit warnte 2019, dass die Nutzenden von E-Scootern die Anonymität verlören, mit der sie sich durch den

---

[114] *Schulz* in: Gola/Heckmann, DS-GVO BDSG, Art. 7 DS-GVO, Rn. 22.

[115] Vgl. Erwägungsgrund 42, S.5 zur DS-GVO.

[116] Vgl. z.B.: Artikel von heise.online vom 16. September 2019, https://www.heise.de/news/Datenschuetzer-Nutzer-von-E-Scootern-hinterlassen-lueckenlose-Bewegungsprofile-4525462.html (zuletzt aufgerufen am 31. Juli 2024); Artikel von Netzpolitik.org vom 24. November 2021, https://netzpolitik.org/2021/datenschutzverstoesse-e-roller-apps-sollen-persoenliche-daten-an-dritte-weitergeben/ (zuletzt aufgerufen am 31. Juli 2024); Artikel von Mobilsicher vom 24. November 2021, https://mobilsicher.de/ratgeber/apps-gecheckt-daten-die-vom-e-roller-fallen (zuletzt aufgerufen am 31. Juli 2024).

öffentlichen Raum bewegten. Viele E-Scooter-Verleiher vereinbarten schon in den Nutzungsverträgen, dass die Nutzerdaten, regelmäßig inklusive Kontakt-, Konto- und Standortdaten, an nicht näher eingegrenzte dritte Stellen weitergegeben würden, ohne dass dies für den Vertragsschluss notwendig sei.[117]

Die Betreiber:innen der UDM müssen daher sichergehen, dass die Rechte der Betroffenen eingehalten werden, wenn sie mit einem Transportdienstleister vereinbaren, dass dieser die Daten der Nutzenden an die UDM übermittelt. Es müssen alle oben genannten Voraussetzungen an die Einwilligung eingehalten werden. Ansonsten laufen die Betreiber:innen der UDM Gefahr, Daten zu erhalten, die nicht rechtmäßig erhoben und/oder weitergeleitet wurden. Diese dürften dann nicht für den Aufbau und Betrieb der UDM verwendet werden. Es besteht demnach ein erhebliches Interesse auf Seiten der Betreiber:innen, dass die Daten rechtmäßig verarbeitet werden.

3.3.2.3 Betroffenenrechte

Wie oben unter 3.3.2.2.1.1. angesprochen, müssen die personenbezogenen Daten der betroffenen Personen auf deren Verlangen unter bestimmten Voraussetzungen gelöscht werden. Dieses Recht auf Löschung regelt Art. 17 DS-GVO. Die Umstände, die eine Pflicht zur Löschung nach Aufforderung durch die betroffene Person begründen, sind in Art. 17 Abs. 1 lit. a) bis f) geregelt. Diese Umstände sind zum Beispiel der Widerruf der Einwilligung, lit. b), oder ein Widerspruch gegen die Datenverarbeitung durch die betroffene Person, lit. c).

Außerdem sind aufgrund des Rechts einer Person „Vergessen zu werden" die personenbezogenen Daten auf Verlangen der Person zu löschen, wenn die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, vgl. Art. 17 Abs. 1 a) DS-GVO. Das Recht auf Vergessenwerden soll den Verantwortlichen, der die personenbezogenen Daten veröffentlicht hat, auch verpflichten, den Verantwortlichen, die die personenbezogenen Daten verarbeiten, das Löschungsverlangen mitzuteilen, und zu veranlassen, dass alle Links zu diesen Daten, Kopien und Replikation der personenbezogenen Daten gelöscht werden, vgl. Art. 17 Abs. 2 DS-GVO.[118] Dieses Recht ist bedeutsam, wenn die personenbezogenen Daten veröffentlicht wurden. Das Recht auf Vergessenwerden wird relevant, wenn der oder die (identifizierbare) Nutzer:in in der UDM als Verkehrsteilnehmende angezeigt wird und verschiedene historische Versionen der UDM mitsamt der Verkehrslage in diesem Zeitpunkt gespeichert werden und öffentlich einsehbar bleiben. Über Art. 17 Abs. 1 a) DS-GVO können so zeitliche Grenzen für die Einwilligung gelten, vgl. Seite 42.

Im Anschluss regelt Art. 17 Abs. 3 DS-GVO Ausnahmetatbestände, wann trotz Vorliegen der Voraussetzungen des Art. 17 Abs. 1 und Abs. 2, die Daten auf Verlangen trotzdem nicht gelöscht werden müssen. Regelmäßig dürfte in Bezug auf den Betrieb einer UDM jedoch keiner dieser Ausnahmetatbestände in Betracht kommen, sodass die Daten der betroffenen Person auf Verlangen regelmäßig durch die Betreiber:innen der UDM gelöscht werden müssen.

3.3.3 Anreiz zur Datenteilung durch Sondernutzungsvertrag

Die Betreiberin der UDM, die Stadt Hamburg, hat Interesse daran, dass das Transportunternehmen, hier Voi, die von der an den Scootern angebrachten Sensorbox der Firma ConsiderIT erfassten Umfelddaten, wie Straßenzustand, Luftqualität und andere Umgebungsinformationen, an die UDM

[117] Pressemitteilung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (Johannes Casper): „E-Scooter – Die Daten Fahren mit" vom 13. September 2019, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2019/2019-09-13_E-Scooter.PDF (zuletzt aufgerufen am 31. Juli 2024).

[118] Siehe dazu auch: Erwägungsgrund 66 zur DS-GVO.

weiterleitet. Voi stellt in diesem Zusammenhang lediglich die Scooter als Träger der Sensorboxen zur Verfügung und ist somit nur indirekt in die Datenerfassung eingebunden, hat jedoch Interesse daran, den öffentlichen Straßenraum durch Abstellen und Parken der Scooter zu nutzen. Insoweit besteht die rechtliche Unsicherheit, ob das stationslose gewerbliche Anbieten von Leihtretrollern als erlaubnispflichtige Sondernutzung des öffentlichen Straßenraums oder als erlaubnisfreier Gemeingebrauch zu bewerten ist. Der jeweilige Landesgesetzgeber kann in den Straßen- und Wegegesetzen stationslose Leihroller ausdrücklich als Sondernutzung deklarieren.[119] In Hamburg ist dies bislang allerdings nicht geschehen. Der Landesgesetzgeber hält damit weiter an einem Urteil des OVG Hamburg aus dem Jahre 2009 fest.[120] In Hamburg benötigt die Firma Voi demnach keine Sondernutzungserlaubnis, um den stationslosen E-Roller-Verleih zu betreiben.

Die Stadt Hamburg als Betreiberin der UDM hat damit derzeit keine Möglichkeit, in einem Vertrag mit Voi die Erteilung einer Sondernutzungsgenehmigung an die Pflicht zur Bereitstellung der von der Sensorbox von ConsiderIT erfassten Umfelddaten zu knüpfen. Diese Möglichkeit würde sich erst dann ergeben, wenn die Stadt Hamburg ihr Straßen- und Wegerecht, insbesondere § 19 HWG ändern würde oder eine entsprechende Satzung auf Grundlage von § 19 Abs. 7 HWG erlässt.

Daher bleibt der Stadt Hamburg im Moment nur die Möglichkeit Anreize zu setzen, damit ConsiderIT die von den Sensorboxen an den Voi-Scootern erfassten Umfelddaten mit ihr teilt. Die Gegenleistung, die die Stadt anbieten kann, ist die Nutzung der UDM. Allerdings ist es gerade das Ziel, dass die UDM allen Nutzenden kostenlos zur Verfügung gestellt werden soll. Dies wäre anders, wenn für den stationslosen Rollerverleih eine Sondernutzungserlaubnis für den öffentlichen Straßenraum erforderlich wäre. Dann könnte die Stadt in einem Sondernutzungsvertrag die Erteilung der Sondernutzungserlaubnis an die Pflicht zum Datenteilen knüpfen, vgl. Erwägungsgrund Nr. 6 der DA (EU) 2022/670.

3.3.4 Exkurs: Integration von ODD in die UDM

Eine „ODD“ (Operational Design Domain, bzw. zulässige Betriebsdomäne) ist sowohl aus technischer als auch rechtlicher Perspektive zu betrachten. Diese differenzierte Betrachtung ist erforderlich, um die unterschiedlichen Anforderungen, die sowohl die technische Implementierung als auch die rechtlichen Vorgaben betreffen, vollständig zu verstehen und die Auswirkungen auf die Integration autonomer Fahrzeuge in den Straßenverkehr präzise einschätzen zu können.

Die ODD beschreibt den Betriebsrahmen für ein automatisiertes Fahrsystem und legt fest, unter welchen spezifischen Betriebsbedingungen ein autonomes Fahrzeug sicher agieren kann. Zu diesen Bedingungen gehören umweltbedingte, geographische und tageszeitliche Einschränkungen sowie das (Nicht-)Vorhandensein bestimmter Verkehrs- oder Fahrbahnmerkmale.[121] Diese technischen Parameter sind nicht isoliert zu betrachten, sondern stehen in direkter Wechselwirkung mit den rechtlichen Anforderungen, die die Sicherheit und die Genehmigungsfähigkeit des Betriebs autonomer Fahrzeuge regeln.

---

[119] *Johannisbauer*, NJW 2019, 3614 (3617).

[120] Vgl. OVG Hamburg, Beschluss vom 19.06.2009 – 2 Bs 82/09.

[121] vgl. ISO/TR 4804:2020(E): Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation, S. 6 Definition Nr. 3.37.

Rechtlich betrachtet stellt eine ODD eine Genehmigungsvoraussetzung nach § 8 Abs. 1 Nr. 1 AFGBV[122] für den Betrieb autonomer Fahrzeuge dar. Die ODD legt den spezifischen Betriebsbereich fest, der kartographisch präzise eingegrenzt ist und die geographischen sowie verkehrlichen Anforderungen erfüllt. Sie definiert die Bedingungen, unter denen ein automatisiertes Fahrsystem sicher betrieben werden kann, einschließlich Umweltfaktoren, geografischen Gegebenheiten, Verkehrsbedingungen und zeitlichen Einschränkungen.[123] Um eine Typengenehmigung für den Betrieb eines autonomen Fahrzeugs zu erhalten, ist eine präzise Festlegung der ODD durch die Hersteller:innen erforderlich. Dies erfordert eine Abstimmung des nach § 7 Abs. 2 AFGBV festgelegten Betriebsbereichs, welchen das autonome Fahrzeug selbständig bewältigen kann und der Betriebserlaubnis, Betriebshandbuch und Sicherheitskonzepten, vgl. § 12 AFGBV.

Die Einschätzung der Hersteller:innen bzw. Betreiber:innen werden durch die zuständige Behörde nach den in § 9 Abs. 2 AFGBV beschriebenen Verfahrensschritten überprüft. Geprüft wird i. S. d. § 1 e Abs. 2 Nr. 2 StVG, ob das Fahrzeug im gesamten Betriebsbereich selbständig den an die Fahrzeugführung gerichteten Verkehrsvorschriften entsprechen kann. Zudem muss sichergestellt werden, dass beim Betrieb "weder die Sicherheit und Leichtigkeit des Straßenverkehrs beeinträchtigt noch Leib und Leben von Personen über das allgemeine Risiko einer Beeinträchtigung durch den für den beantragten Betriebsbereich ortsüblichen Straßenverkehr hinaus erheblich gefährdet" wird, § 9 Abs. 2 Nr. 3 AFGBV. Dadurch setzt die Genehmigung voraus, dass das Fahrzeug unter den definierten Bedingungen sicher betrieben werden kann.

Die ODD spielt somit eine entscheidende Rolle bei der Festlegung der Grenzen, innerhalb derer ein autonomes Fahrzeug sicher agieren kann. Diese Informationen sind für die zuständigen Behörden von großer Bedeutung, da sie sicherstellen müssen, dass alle relevanten Sicherheitsstandards eingehalten werden.

Nach der behördlichen Prüfung wird die ODD starr und unveränderlich festgelegt. Allerdings ist nicht erforderlich, dass auch das daraus resultierende Betriebsgebiet starr ist. So könnten Hersteller:innen einen größeren Betriebsbereich festlegen, der dynamisch agieren kann. In einem Flächensystem könnte die UDM dann eine konkrete Gebietsfestlegung anhand der genehmigten ODD vornehmen. Die Verwaltung der ODD innerhalb einer UDM ermöglicht es, Veränderungen in der Straßeninfrastruktur, wie z.B. den Ausfall von Straßenbeleuchtungen, effektiv und zuverlässig zu erfassen und den Halter:innen autonomer Fahrzeuge mitzuteilen. Dies würde ermöglichen, dass das Fahrzeug flexibel auf Veränderungen in der Umgebung reagiert, während die grundlegenden ODD-Anforderungen weiterhin erfüllt bleiben. Im Beispiel der ausgefallenen Straßenbeleuchtung könnte die UDM Informationen darüber enthalten, welche Straßenlaternen aktuell funktionieren. Fällt in einem Straßenzug die Beleuchtung aus, könnte und dürfte das Fahrzeug diesen Bereich während des Ausfalls nicht befahren. Durch den Abruf der UDM-Daten wird das Fahrzeug über diesen Umstand informiert und kann die Navigation entsprechend anpassen.

Um einen solchen "dynamischen" Betriebsbereich zu realisieren, müsste sich die Behörde auf die Flexibilität eines solchen Systems einlassen und den eigenen Entscheidungsspielraum nutzen. Sie muss hierbei sorgfältig abwägen, wie sie sowohl den rechtlichen Vorgaben als auch den technischen

---

[122] Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV) vom 24. Juni 2022 (BGBl I S. 986), geändert durch Art. 10 der Verordnung vom 20. Juli 2023 (BGBl. 2023 I Nr. 199).

[123] Art. 2 Nr. 16 DVO (EU) 2022/1426, ABl. 2022 L 221, 1; vgl. SAE International: Surface vehicle recommended practice J 3016, Juni 2018, S. 14.

Möglichkeiten gerecht werden könnte. Der Ermessensspielraum der Behörde aus § 9 AFGBV bezieht sich hierbei darauf, dass der Betriebsbereich großflächiger angelegt werden kann, um eine höhere Flexibilität und Anpassungsfähigkeit für den Betrieb autonomer Fahrzeuge zu gewährleisten und dennoch die Einhaltung der ODD sicherzustellen.

Allerdings kann diese Empfehlung aufgrund möglicher europarechtlicher Implikationen wie Marktzugangshemmnissen durch die Festlegung dynamischer Betriebsbereiche bzw. Betriebsbereiche allgemein bei grenzüberschreitendem Fahren, noch nicht abschließend ausgesprochen werden. Insbesondere könnte die Schaffung dynamischer Betriebsbereiche in einem nationalen Kontext Schwierigkeiten mit sich bringen, wenn diese Regelungen nicht mit den Vorgaben anderer europäischer Staaten harmonisiert sind. Unterschiedliche nationale Vorschriften könnten dazu führen, dass autonome Fahrzeuge, die in einem Land problemlos operieren dürfen, in einem anderen nicht fahren können.

Insgesamt erfordert eine dynamische Handhabung des Betriebsbereichs eine klare und starre Definition der ODD als Rechtsrahmen, um so die Integrität und Sicherheit des Straßenverkehrs zu gewährleisten. Damit stellt sich neben den rechtlichen Herausforderungen auch die Frage der praktischen Umsetzung, welche auf eine kontinuierliche Abstimmung zwischen technischem Fortschritt und behördlicher Aufsicht angewiesen ist.

Hier zeigt sich erneut die Wechselwirkung zwischen rechtlichen und technischen Aspekten: Während die technische Flexibilität des Systems ein hohes Maß an Anpassungsfähigkeit ermöglicht, erfordert die rechtliche Rahmung eine klare und stabile Grundlage, um die Integrität und Sicherheit des Straßenverkehrs zu gewährleisten.

So zeigt sich, dass eine dynamische Handhabung des Betriebsbereichs nicht nur eine rechtliche Herausforderung darstellt, sondern auch eine Frage der praktischen Umsetzung, die auf den kontinuierlichen Dialog zwischen technischer Innovation und behördlicher Aufsicht angewiesen ist.

3.3.5 Fazit

Wenn Nutzer:innen Daten mit der UDM teilen, müssen die Voraussetzungen der DS-GVO eingehalten werden. Eine Einwilligung kann formfrei erfolgen, auch elektronisch. Da die Betreiber:innen der UDM beweisen müssen, dass die Einwilligung vor Verarbeitung erteilt wurde, empfiehlt sich, diese digital zu dokumentieren. Die Einwilligung ist streng zweckgebunden, die Daten können ohne Anpassung der Einwilligung nicht für andere Zwecke verwendet werden. Die Darstellung von Scooter-Nutzenden in der UDM ist nicht anonym, deswegen müssen auch hier die Regeln der DS-GVO beachtet werden. Nur wenn die Scooter-Nutzenden nicht mit ihrem Standort in der UDM angezeigt werden, ist eine Anonymisierung möglich.

In Hamburg ist für den stationslosen Verleih von E-Rollern im Moment keine Sondernutzungserlaubnis notwendig; dieser unterfällt den Gemeingebrauch an öffentlichen Straßen. Die Stadt Hamburg kann daher eine Pflicht zum Datenteilen durch Voi nicht von der Gegenleistung abhängig machen, eine Sondernutzungsgenehmigung zu erteilen. Für den Vertragsschluss zwischen Voi und den Betreiber:innen der UDM müssen daher andere Anreize gesetzt werden.

Da die Scooter-Nutzenden keinen direkten Kontakt zu den Betreiber:innen der UDM haben, muss die Einwilligung zur Weiternutzung und -gabe an die UDM schon im Vertrag zwischen dem Transportdienstleister Voi und den Nutzenden erfolgen. Der Vertragsschluss darf aber nicht von der Erteilung der Einwilligung abhängig gemacht werden. Wenn die Einwilligung zur Weitergabe nicht wirksam war, dürfen die Betreiber:innen der UDM die Daten der Nutzenden nicht für seine angegebenen Zwecke verwenden. Die Stadt Hamburg muss als Betreiberin der UDM prüfen, ob die Klauseln im Vertrag

zwischen Voi und den Verkehrsteilnehmenden wirksam sind, um sicherzugehen, die Daten nutzen zu dürfen.

3.4 Use Case 4: Zählung der Trajektorien

Für die Planung der eigenen Navigation ist die Prädiktion des Verhaltens der umgebenden Verkehrsteilnehmer:innen unerlässlich. Insbesondere das Verhalten menschlicher Autofahrer:innen, welches im Vergleich zu autonomen Fahrzeugen häufig willkürlich und emotionsgesteuert ist, stellt eine besondere Herausforderung dar. Um diese komplexen Verhaltensweisen abzubilden, werden zumeist wahrscheinlichkeitsbasierte Modelle verwendet, welche Trajektorien berechnen und analysieren. Trajektorien sind Pfade, die von beweglichen Objekten wie Fahrzeugen oder Fußgänger:innen über einen bestimmten Zeitraum hinweg zurückgelegt werden. In diesen Modellen werden umfangreiche Datensammlungen zu Verkehrsverhalten und -routen analysiert, um Präferenzen zu identifizieren und die Navigation des autonomen Fahrzeugs an diese anzupassen.

3.4.1 Sachverhalt

Der vierte Use Case kombiniert Elemente der Use Cases 1 und 2. Durch Echtzeit-Analyse und das Management von Fahrzeugtrajektorien sollen sowohl der Verkehrsfluss optimiert als auch die Verkehrssicherheit verbessert werden. Die Erfassung der Trajektorien erfolgt durch Sensoren und Kameras der autonomen Fahrzeuge, die kontinuierlich Verkehrs- und Bewegungsdaten erfassen. Diese Trajektorien werden zur **Visualisierung** aufbereitet. Neben dieser Visualisierung werden Zählungen durchgeführt, um zu erfassen, wie viele Fahrzeuge welche Kombination von Kreuzungseinfahrten und -ausfahrten nutzen. Da die Visualisierung an sich entbehrlich ist und vor allem der Demonstration dient, während die Zusammenfassung der Trajektorien für die Zählung der Fahrten unerlässlich ist, werden lediglich die **aggregierten Zählerstände** an die UDM weitergegeben. Die visualisierten Trajektorien selbst werden nicht an die UDM weitergegeben.

Zudem könnte es im Datenerhebungsprozess selbst erforderlich sein, den **ID-Wechsel im Kreuzungsbereich nachzuvollziehen**. Ansonsten besteht die Gefahr, dass unvollständige Trajektorien gezählt werden (z. B. Linksabbieger mit kurzen Freigabezeiten und langer Verweildauer in der Kreuzung). Mögliches Resultat wären fehlerhafte Zählungen.

Durch die Trajektorienanalyse sollen Verhaltens- und Bewegungsmuster wie Stoßzeiten, typische Routen und Fußgängerzonen identifiziert und Gefahrenmuster wie häufige Bremsmanöver oder Rückstau durch viele Linksabbieger an bestimmten Kreuzungen erfasst und analysiert werden. Auf Basis dieser Analyse kann durch Verkehrsmanagement die Verkehrssteuerung optimiert werden, indem z.B. Ampelschaltungen angepasst, Geschwindigkeitsbegrenzungen eingeführt oder der Verkehr umgeleitet werden. Zudem dient die Trajektorienanalyse der Unfallprävention. Durch Erkennung möglicher sich kreuzender Trajektorien durch die UDM kann das Fahrzeug mit diversen präventiven Maßnahmen, wie die Versendung einer CAM oder ein automatisches Abbremsen reagieren.

3.4.2 Datenschutzrechtliche Einordnung

3.4.2.1 Anwendbarkeit des Datenschutzrechts

Die erfassten Trajektoriedaten, also Daten über die Bewegung und die geplante Route des autonomen Fahrzeugs sowie anderer Verkehrsteilnehmer:innen, können nach Art. 4 Nr. 1 DS-GVO personenbezogen sein, wenn andere Verkehrsteilnehmer:innen erfasst und identifizierbar sind. Dies erfolgt bei

Erfassung von Kfz-Kennzeichen oder spezifischen Merkmalen von Fußgänger:innen, welche erforderlich sind, um ID-Wechsel innerhalb der Kreuzung zu identifizieren.

Hiervon sind jedoch die aggregierten Zähldaten der jeweiligen Trajektorien abzugrenzen. Diese Daten zeigen lediglich zählerisch auf, wie viele Verkehrsteilnehmer:innen wie, wo und wann über die Kreuzung gefahren sind. Personenidentifizierbare Merkmale lassen sich hieraus gerade nicht mehr erschließen.

Damit ist lediglich die Zählung der Trajektorien mit Personenbezug an Kreuzungen relevanter Aspekt der Datenverarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO. Diese Datenverarbeitung umfasst das Erheben, Erfassen und Speichern der Trajektorien, die Rückschlüsse auf individuelle Verkehrsteilnehmer:innen zulassen könnten. Zudem ist die Verarbeitung der Daten erforderlich, um einen ID-Wechsel nachvollziehen zu können und so unvollständige bzw. verfälschte Trajektorien zu vermeiden. Hierfür wird unter Umständen eine temporäre Speicherung der personenbezogenen (bzw. personendifferenzierenden) Daten erforderlich.

3.4.2.2 Möglichkeiten zur Abwendung datenschutzrechtlicher Verpflichtungen

Somit erfordert auch die Umsetzung des Use Case 4 mit der Erfassung und Aggregierung von Trajektorien insbesondere im Hinblick auf die erforderliche temporäre Speicherung von ID-Daten zur Identifizierung eines ID-Wechsels innerhalb eines Kreuzungssystems, Strategien zur Umgehung der Anwendbarkeit von Datenschutzregelungen wie der DS-GVO.

Hinsichtlich der allgemeinen Erfassung von Trajektorien könnte die Anwendbarkeit der DS-GVO durch die Umsetzung von geschlossenen Systemen und automatischen Anonymisierungen effektive Werkzeuge darstellen. Dies wäre jedoch zumindest hinsichtlich der ID-Wechsel-Erkennung schwierig.

3.4.2.2.1 Geschlossenes System

Für den Use Case könnte ein geschlossenes System in der Weise eingesetzt werden, dass Trajektorien gesammelt und innerhalb des Kreuzungssystems kategorisiert werden, um einen Datenfluss allgemein zu beobachten.[124] Das System könnte sodann beispielsweise die Kategorie „20 oder mehr Fahrzeuge sind in einem Zeitraum von wenigen Sekunden aus der A-Straße über die Kreuzung in die B-Straße gefahren“ an den AMQP-Broker weitergeben. Wichtig ist, dass die Daten vor der Übertragung an den AMQP-Broker kategorisiert und damit anonymisiert werden. Eine Übertragung von dem Kreuzungssystem an den Broker würde das geschlossene System „öffnen“ und zur Anwendung der DS-GVO führen.

Ähnlich wie bei den VRU-Hotspots des Use Case 1 handelt es sich bei einer Trajektoriensammlung und -analyse um eine dauerhafte Datensammlung. Diese geht über eine einfache Momentaufnahme hinaus, da mit Trajektorien Positionsdaten und Bewegungsmuster aufgezeichnet werden. Allerdings werden lediglich aggregierte Zähldaten und nicht die visualisierten Bewegungsmuster, welche unter Umständen Personenbezug aufweisen, weitergegeben. Damit wird anders als bei der Identifizierung von VRU-Hotspots grundsätzlich keine derartige kontinuierliche personenbezogene Datensammlung durchgeführt.

Anders zu beurteilen ist jedoch die Einspeisung von Erkenntnissen über ID-Wechsel innerhalb der Kreuzung. Um einen ID-Wechsel zu identifizieren, muss jedes konkrete Fahrzeug bzw. jede:r

[124] Für die Definition des Begriffs „geschlossenes System“ siehe 3.1.3.2.1.

Verkehrsteilnehmer:in erfasst und deren Verweildauer innerhalb der Kreuzung analysiert werden. Hierbei kann ein geschlossenes System nicht zu einem Ausschluss der Anwendbarkeit der DS-GVO führen. Vielmehr ist eine sofortige Anonymisierung der personenbezogenen Daten erforderlich, sowie eine sofortige Löschung der personenbezogenen Daten nach Ausfahrt aus der Kreuzung und damit eine Vollziehung des ID-Wechsels.

3.4.2.2.2 (Automatische) Anonymisierung

Wenn die Anonymisierung erst nach der Speicherung der Daten erfolgt, bleibt der Personenbezug während der Speicherung bestehen. Die DS-GVO bleibt sodann anwendbar.

Wie bereits in Use Case 2 ausgeführt, soll im vorliegenden EDDY-Projekt die Anonymisierung bereits im Fahrzeug aber nach Datenverarbeitung durch dieses erfolgen. Insofern ist wiederum die Behandlung der Analyse eines ID-Wechsels problematisch. Die Identifizierung eines ID-Wechsels erfordert die Analyse der Bewegungsmuster und Verweildauer jedes konkreten Fahrzeugs bzw. Verkehrsteilnehmenden. Hierbei werden alle gesammelten Daten erfasst und verarbeitet, solange der ID-Wechsel vollzogen wird. Während dieses Zeitraums bleibt die DS-GVO anwendbar, da die personenbezogenen Daten zu Zwecken der Unterscheidung der Verkehrsteilnehmenden innerhalb der Kreuzung weiter vorliegen.

Um den Grundsätzen der DS-GVO gerecht zu werden, müssen alle gesammelten Daten durch das Fahrzeug, soweit sie nicht mehr benötigt werden, unverzüglich anonymisiert werden. Dies ist im Falle des ID-Wechsels erst nach dessen Vollzug und damit nach vollständiger Erfassung und Analyse möglich. Sodann sollten die personenbezogenen Daten nach der Ausfahrt des jeweiligen Verkehrsteilnehmenden aus der Kreuzung sofort gelöscht werden, um die Datenspeicherung nach Art. 5 Abs. 1 lit. c) DS-GVO auf das notwendige Minimum zu beschränken.

Nach Weiterleitung dieser nunmehr anonymisierten Daten an die UDM muss diese jedoch auch mit diesen vermeintlich “sauberen” Daten, datenschutzkonform weiterarbeiten. Insbesondere kann durch die Aggregation der Zähldaten der Trajektorien eine Weitergabe und damit Verarbeitung möglicherweise verbleibender personenbezogener Daten i.S.d. Art. 4 Nr. 1 und 2 DS-GVO ausgeschlossen werden. Diesbezüglich ist unerheblich, ob die Daten bereits vor oder nach Speicherung anonymisiert werden, da durch die Aggregation, also Vermengung der Daten zu einem einheitlichen Datensatz, keine Auftrennung in Daten über einzelne Personen mehr zulässt.

Die Weitergabe von aggregierten Daten reduziert das Risiko eines Personenbezugs und entspricht den Grundsätzen der Datenminimierung und Zweckbindung nach Art. 5 Abs. 1 lit. b) und c) DS-GVO.

Problematisch wird es im obigen Beispielsfall der Kreuzungssituation, wenn nur ein einzelnes Fahrzeug von der A-Straße über die Kreuzung in die B-Straße fährt. Dieses Datum könnte nicht kategorisiert werden und eine Anonymisierung unmöglich machen. Als Lösung für dieses Problem könnte das System so programmiert werden, dass nur die Kategorie „wenig Verkehrsaufkommen“ herausgegeben wird, wenn zwei oder weniger Fahrzeuge einen Kreuzungsverlauf passieren. Alternativ könnten in solchen Fällen keine Informationen geteilt werden. Sowohl keine Information zu teilen als auch die Kategorie „wenig Verkehrsaufkommen“ lassen keinen Rückschluss auf die Zahl der passierenden Fahrzeuge zu und eröffnen dadurch auch kaum Möglichkeiten der Re-Identifikation.

Damit erscheint auch insoweit eine vollständige Abwendung datenschutzrechtlicher Verpflichtungen nicht möglich.

3.4.2.3 Rechtmäßigkeit der Verarbeitung

Die obigen Systeme können daher nicht vollständig die Anwendung datenschutzrechtlicher Regelungen, insbesondere der DS-GVO, abwenden. Die Verarbeitung personenbezogener Daten, im Rahmen der Identifizierung eines ID-Wechsels innerhalb einer Kreuzung bedarf damit einer Rechtsgrundlage. Eine solche ergibt sich auch im Use Case 4 aus Art. 6 DS-GVO.

Allerdings ist auch insoweit eine Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO, wie bereits im Use Case 2 dargelegt (siehe 3.2.5.3.), nicht praxistauglich.

Als Rechtsgrundlage könnte Art. 6 Abs. 1 lit. e DS-GVO in Betracht kommen, sofern die öffentliche Stelle die Datenverarbeitung zur Wahrung einer Aufgabe im öffentlichen Interesse vornimmt. Die vorliegende Verarbeitung personenbezogener Daten zu Zwecken der Identifizierung eines ID-Wechsels innerhalb einer Kreuzung, um eine korrekte Zählung der passierenden Verkehrsteilnehmer:innen vorzunehmen, kann dem Verkehrsmanagement und der Verkehrssicherheit dienen. Die aggregierten Daten ermöglichen Rückschlüsse auf die Effektivität des jeweiligen Kreuzungssystems und liefern Informationen, wie das Verkehrsmanagement durch die öffentliche Stelle optimiert werden könnte. Insbesondere können potenzielle Gefahrenstellen frühzeitig identifiziert werden, auf welche die öffentliche Verwaltung durch gezielten Ausbau der Verkehrsinfrastruktur reagieren kann. Beispielsweise können Kreuzungen, an denen regelmäßig hohe Verkehrsaufkommen und lange Wartezeiten beobachtet werden, durch bauliche Maßnahmen oder optimierte Ampelschaltungen entlastet werden.

Insoweit ist die Datenverarbeitung verhältnismäßig, da die Kamera- und Sensorikdaten des EDDY-Projekts nur für eine kurze Zeit in der UDM eingespeist werden, bis der ID-Wechsel vollzogen ist. Dies geschieht in Echtzeit, ohne dass durch einen vorherigen Prozess die Daten anonymisiert werden. Erst im Anschluss erfolgt die sofortige und automatische Löschung der Daten aus dem System. Damit wird eine klar definierte Zweckbindung der Erhebung und Verarbeitung der Daten sichergestellt.

Auch Art. 6 Abs. 1 lit. f DS-GVO kann als Rechtsgrundlage angeführt werden. Insoweit ist die Verarbeitung personenbezogener Daten zulässig, wenn diese der Wahrung berechtigter Interessen des Verantwortlichen dient und nicht die Interessen oder Grundrechte der betroffenen Personen überwiegen. Als berechtigtes Interesse der Betreiber:innen könnte die Verkehrssicherheit und das effiziente Verkehrsmanagement gesehen werden. Insoweit könnte jedoch Art. 3 Abs. 1 GG relevant werden, wenn eine Ungleichbehandlung i. S. d. Art. 3 Abs. 1 GG zu Lasten der Personen angenommen wird, die aufgrund der konkreten Verkehrssituation länger in der Kreuzung verweilen müssen. Deren Daten werden für eine längere Zeit im System gespeichert, um den ID-Wechsel nachvollziehen zu können, sodass sie einem schlechteren Datenschutzstandard als Verkehrsteilnehmer:innen, welche schnell die Kreuzung passieren, ausgesetzt sind.

Art. 3 Abs. 1 GG verlangt, dass der Gesetzgeber und die Verwaltung wesentlich gleiche Sachverhalte gleich und wesentlich ungleiche Sachverhalte ungleich behandeln. Eine Ungleichbehandlung ist dann gerechtfertigt, wenn sachliche Gründe vorliegen, welche die unterschiedliche Behandlung rechtfertigen.

Eine Ungleichbehandlung könnte sich gerade aus dieser längeren Datenspeicherung aufgrund der unterschiedlichen Verweildauer des Verkehrsteilnehmenden innerhalb des Kreuzungssystems ergeben. Durch diese längere Speicherung der personenbezogenen Daten, genießen Personen, die verkehrsbedingt länger innerhalb einer Kreuzung stehen, einen geringeren Datenschutzstandard als Personen die schnell die Kreuzung passieren können.

Allerdings spricht gegen eine solche Ungleichbehandlung, dass die Daten der Verkehrsteilnehmer:innen jeweils nur für die Dauer des Verweilens innerhalb der Kreuzung gespeichert werden. Die längere

Verweil- und damit Speicherdauer führt jedoch nicht dazu, dass ein wesentlich unterschiedlicher Sachverhalt begründet wird, welcher gleichbehandelt wird.

Jedenfalls würde diese unterschiedliche Verweildauer selbst als sachlicher Grund für die längere Speicherung und damit differenzierte Datenverarbeitung dienen. Es wäre jedoch notwendig, sicherzustellen, dass die längere Datenspeicherung für die betroffenen Personen, verhältnismäßig und durch das legitime Ziel der Verkehrssicherheit und des Verkehrsmanagements gerechtfertigt ist.

3.4.3 Fazit

Durch Kombination der Elemente der Use Cases 1 und 2 mit der Echtzeit-Analyse von Fahrzeugtrajektorien zielt der vorliegende Use Case darauf ab, den Verkehrsfluss und die Verkehrssicherheit durch gezieltes Verkehrsmanagement zu optimieren. Die Sensoren und Kameras der autonomen Fahrzeuge erfassen kontinuierlich Verkehrs- und Bewegungsdaten, die als aggregierte Zähldaten an die UDM weitergegeben werden. Diese werden in einem wahrscheinlichkeitsbasierten Modell zur Berechnung zukünftiger Trajektorien verarbeitet. Hierdurch wird ein "vorausschauendes" Fahren ermöglicht, bei dem das autonome Fahrzeug sein Fahrverhalten an die identifizierten Verkehrsverhaltensmuster wie Stoßzeiten oder typische Routen anpasst. Auch können auf Basis der Erkenntnisse durch die zuständigen Straßenverkehrsbehörden Maßnahmen, wie beispielsweise die Anpassung der Ampelschaltung oder eine Umleitung des Verkehrs ergriffen werden, um den Verkehrsfluss zu verbessern und die Sicherheit für die Verkehrsteilnehmer:innen zu erhöhen.

Datenschutzrechtlich sind jedoch insbesondere die Anforderungen der DS-GVO zu berücksichtigen. Die Verarbeitung der personenbezogenen Daten wäre dann verhältnismäßig, wenn sichergestellt wird, dass die Speicherung der personenbezogenen Daten nur so lange erfolgt, wie es zur Verhinderung unvollständiger oder verfälschter Trajektorien notwendig ist. Auch sind diese Daten unverzüglich nach Abschluss der erforderlichen Analysen zu anonymisieren und löschen. Durch diese Maßnahmen wird die Einhaltung der datenschutzrechtlichen Vorgaben der DS-GVO gewährleistet und die Verkehrsteilnehmer:innn werden vor einer unverhältnismäßigen Verarbeitung ihrer personenbezogenen Daten geschützt.

Bei der Erfassung und Speicherung personenbezogener Daten, die für die Nachvollziehbarkeit eines ID-Wechsels innerhalb eines Kreuzungssystems erforderlich sind, müssen insbesondere die Hinweispflichten nach Art. 13 DS-GVO eingehalten werden. Die praktische und logistische Umsetzung der Wahrnehmung dieser Hinweispflichten ist, wie bereits in 3.1.3.4. betrachtet, derzeit sehr schwierig bis unmöglich.

4 Die UDM als Teil eines Intelligenten Verkehrssystem

Eine UDM kann Teil eines sog. „Intelligenten Verkehrssystems" (IVS) sein. Die UDM ist kein eigenständiges IVS; kann aber in ein solches eingebettet werden. IVS sind auf nationaler und europäischer Ebene nur wenig reguliert. Es besteht (noch) keine Pflicht der Mitgliedstaaten IVS einzuführen. Der europäische Rechtsrahmen sieht jedoch vor, dass gewisse (Verkehrs-)Daten in einem Nationalen Zugangspunkt geteilt werden müssen. Von diesen Datensätzen können die Hersteller:innen und Betreiber:innen der UDM profitieren. Der Rechtsrahmen für IVS stellt nur wenige Anforderungen an die UDM: z. B. sollen Daten, die Endnutzer zur Verfügung stellen, pseudonymisiert werden und etwaige falsche Daten der zur Verfügung stellenden Stelle gemeldet werden.

4.1 Was sind Intelligente Verkehrssysteme?

IVS sind Systeme, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an den Schnittstellen zu anderen Verkehrsträgern eingesetzt werden. Sie werden durch die europäische IVS-Richtlinie, auf dieser basierenden europäischen Spezifikationen und das nationale „Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern" (IVSG) reguliert.

Die Digitalisierung des Verkehrssektors ist für die Nachhaltigkeit, Effizienz und Sicherheit im Verkehr von zentraler Bedeutung. Der Einsatz von Intelligenten Verkehrssystemen (IVS) wird als zentraler Faktor im europäischen Verkehrssystemen für die Erreichung dieser Ziele angesehen.[125] IVS werden hauptsächlich durch die europäische IVS-Richtlinie[126] und das nationale Umsetzungsgesetz, das IVS-Gesetz (IVSG)[127], reguliert. Zusätzlich hat die EU in delegierten Rechtsakten, die auf der IVS-Richtlinie basieren, weitere Spezifikationen erlassen, die Anforderungen an IVS stellen.

Nach Art. 4 Abs. 2 g) AEUV[128] teilt die Union ihre **Zuständigkeit** mit den Mitgliedsstaaten im Bereich Verkehr. Geteilte Zuständigkeit bedeutet, dass sowohl die Union als auch die Mitgliedsstaaten in

[125] Pressemitteilung der Europäischen Kommission „Fragen und Antworten: Intelligente Verkehrssysteme" vom 14. Dezember 2021; https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_6727 (zuletzt aufgerufen am 31. Juli 2024).

[126] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung Intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

[127] Intelligente Verkehrssysteme Gesetz vom 11. Juni 2013 (BGBl. I S. 1553), zuletzt durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2640) geändert

[128] Fassung aufgrund des am 1.12.2009 in Kraft getretenen Vertrages von Lissabon (Konsolidierte Fassung bekanntgemacht im ABl. EG Nr. C 115 vom 9.5.2008, S. 47) zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) m.W.v. 1.7.2013.

diesem Bereich gesetzgeberisch tätig werden und verbindliche Rechtsakte erlassen dürfen; dabei nehmen die Mitgliedsstaaten ihre Zuständigkeiten nur wahr, sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat, vgl. Art. 2 Abs. 2 AEUV. Diese Zuständigkeit im Bereich Verkehr wird in Titel VI „Der Verkehr" konkretisiert, vgl. Art. 90-100 AEUV. Die IVS-Richtlinie wurde gestützt auf Art. 91 AEUV erlassen, da die Gewährleistung einer unionsweiten koordinierten und kohärenten Einführung von IVS auf Ebene der Mitgliedstaaten und/oder der Privatwirtschaft nicht ausreichend verwirklicht werden kann. Daher sind, im Einklang mit dem Subsidiaritätsprinzip aus Art. 5 EUV, aufgrund von Umfang und Wirkung, die Maßnahmen besser auf Unionsebene zu verwirklichen.[129] Die delegierten Rechtsakte (DA), werden sodann aufgrund von Art. 290 AEUV erlassen.

§ 2 Nr. 1 IVSG beschreibt Intelligente Verkehrssysteme als *Systeme, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an den Schnittstellen zu anderen Verkehrsträgern eingesetzt werden*. Art. 4 Nr. 1 der IVS-Richtlinie ergänzt, dass der Straßenverkehr dabei auch seine Infrastrukturen, Fahrzeuge und Nutzer umfasst und dass auch Systeme erfasst sind, die beim Verkehrs- und Mobilitätsmanagement eingesetzt werden.

4.2 Verhältnis UDM und Intelligente Verkehrssysteme

Eine UDM ist als digitale Karte nicht selbst ein IVS. Sie kann aber in einem IVS-System eingebettet sein. In den europäischen delegierten Rechtsakten werden die Hersteller:innen von digitalen Karten insbesondere als Nutzer von IVS und den dazugehörigen Daten adressiert.

Eine UDM ist ähnlich konzipiert wie eine Local Dynamic Map (LDM). Der ETSI TR 102 863 Report definiert eine Local Dynamic Map (LDM) als konzeptionellen Datenspeicher, der in eine IVS-Station eingebettet ist. Die LDM enthält topografische, Positions- und Statusinformationen in Bezug auf IVS-Stationen innerhalb eines geografischen Gebiets.[130]

Auch in die UDM werden Informationen eingespeist und zur Darstellung von Objekten verwendet. Damit ist die UDM ein System, das zwar funktionell einer LDM ähnelt, aber durch die Integration von Informations- und Kommunikationstechnologien erweitert wird. Diese zusätzliche technische Ausstattung ermöglicht es, dass die UDM nicht nur statische Daten speichert, sondern auch mit anderen Verkehrsteilnehmer:innen kommuniziert. Daher könnte argumentiert werden, dass die EDDY-UDM als eigene IVS i. S. d. § 2 Nr. 1 IVSG anzusehen sei, da diese die Datenverarbeitung in Echtzeit und eine dynamische Interaktion mit anderen Verkehrsteilnehmer:innen ermöglicht.

Allerdings reicht dies gerade nicht aus, um die UDM als vollständiges IVS zu klassifizieren. Ein IVS muss gemäß Art. 4 Nr. 1 der IVS-Richtlinie auch zu dem Zweck des Verkehrs- und Mobilitätsmanagement und damit der Steuerung und Optimierung des Verkehrs verwendet werden können. Nach Erwägungsgrund 4 der IVS-RL sollen durch das IVS, Verkehrssysteme geplant, konzipiert, betrieben, gewartet und gesteuert werden. Im Gegensatz dazu bleibt die UDM in ihrer Funktion auf die Bereitstellung von Informationen beschränkt, ohne selbständig in die Verkehrssteuerung einzugreifen. Zwar unterstützt die UDM die Kommunikation in Form von V2X, jedoch führt dies nicht zu einem direkten Eingriff in die Verkehrsinfrastruktur. Nur durch eine nachträgliche Auswertung der kommunizierten Daten könnten

[129] Vgl. Erwägungsgründe 1, 23 IVS-Richtlinie.

[130] ETSI Technical Report 102 863 (V1.1.1 2011-06) Intelligent Transport Systems (ITS); Vehicular Communications; basic Set of Applications; Local Dynamic Map (LDM); Rationale for guidance on standardization, Abschnitt 3.1.

durch Maßnahmen des Verkehrsmanagements entsprechende Anpassungen innerhalb der Infrastruktur vorgenommen werden.

Die UDM kann daher als Teil eines IVS i. S. d. § 2 Nr. 1 IVSG angesehen werden, ist jedoch nicht selbst ein vollständiges IVS. Sie sammelt und stellt Daten bereit, die in einem umfassenderen IVS integriert und verwendet werden, um Verkehrssysteme zu steuern und zu optimieren. Wenn die UDM jedoch in ein IVS eingebettet ist, können für sie auch die Regelungen für IVS, wie das IVSG und die entsprechenden Richtlinien, relevant werden. Zum Teil werden in den delegierten Rechtsakten zur IVS-Richtlinie die Hersteller von digitalen Karten direkt angesprochen.[131] Hersteller:innen von digitalen Karten werden in den Rechtsakten als Nutzer von IVS adressiert.

4.2.1 Hersteller:innen und Betreiber:innen von Digitalen Karten

In den delegierten Rechtsakten, sind zwar nur die Hersteller:innen der digitalen Karten angesprochen, nicht auch die Betreiber:innen der Karten. Im Projekt EDDY sind Hersteller:in und Betreiber:in der digitalen Karte, der UDM, identisch. Anforderungen, die die Spezifikationen des EU-Rechts an die Hersteller:innen von digitalen Karten stellen, müssen auch im weiteren Betrieb beachtet werden (z.B. sollten geeignete technische Maßnahmen ergriffen werden, um sicherzustellen, dass die von den Endnutzern übermittelten Daten pseudonymisiert werden[132]). Die durch die Hersteller:innen geschaffenen technischen Möglichkeiten (z. B. zur Pseudonymisierung) müssen auch von dem/der Betreiber:in genutzt werden, um die Vorschriften nicht zu unterlaufen.

4.3 Anforderungen an ein Intelligentes Verkehrssystem (IVS)

An die Ausgestaltung der IVS werden einige Anforderungen gestellt, die vor allem die Interoperabilität verschiedener Systeme innerhalb der EU gewährleisten sollen. Auch die UDM soll diese Interoperabilität mit verschiedenen IVS wahren.

Für Intelligente Verkehrssysteme hat die EU eine Reihe von sogenannten Spezifikationen erlassen, welche bei der Zulassung von diesen Systemen eingehalten werden müssen. Diese Spezifikation ergeben sich aus der IVS-Richtlinie, die seit Erlass 2010, sowohl 2017 als auch im November 2023 aktualisiert wurde.[133] Die IVS-Richtlinie wurde 2013 durch das IVSG in nationales Recht umgesetzt. Im Zuge der Umsetzung der Richtlinie in deutsches Recht wurde unter Federführung des Bundesministeriums für Digitales und Verkehr (BMDV) (ehemals: Bundesministerium für Verkehr, Bau und Stadtentwicklung (BVBS)) auch ein nationaler IVS-Aktionsplan „Straße“ erlassen. Dieser definiert die Vorgehensweise bei der koordinierten Weiterentwicklung bestehender und beschleunigter Einführung neuer IVS

[131] Vgl. DA 2022/670 und DA 2017/1926.

[132] Vgl. Delegierte Verordnung (EU) 2017/1926 der Kommission vom 31. Mai 2017 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienst, Erwägungsgrund 6.

[133] Vgl. Richtlinie (EU) 2017/2380 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 zur Änderung der Richtlinie 2010/40/EU hinsichtlich des Zeitraums für den Erlass delegierter Rechtsakte (IVS-Richtlinie); Richtlinie (EU) 2023/2661 des Europäischen Parlaments und des Rates vom 22. November 2023 zur Änderung der Richtlinie 2010/40/EU zum Rahmen für die Einführung Intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

zur Erhöhung der Verkehrssicherheit, Verbesserung der Verkehrseffizienz und Verringerung der negativen Auswirkungen des Verkehrs auf die Umwelt.[134]

Bei der Einführung von IVS-Anwendungen und Diensten müssen die Behörden die Spezifikationen der Europäischen Kommission basierend auf der IVS-Richtlinie beachten.[135] Zwar richten sich diese Leitprinzipien zuerst an die Behörden, wenn diese Maßnahmen zu den Einführungen von IVS treffen. Manche dieser Maßnahmen betreffen jedoch die Entwicklung und Umsetzung der UDM direkt, sodass diese Grundsätze auch von den Betreiber:innen und den Entwickler:innen der UDM beachtet werden sollten. Art. 6 Abs. 1 IVS-Richtlinie i. V. m. Anhang II[136] der IVS-Richtlinie nennt die geforderten Spezifikationen für die Einführung von IVS. Die für die Betreiber:innen und Entwickler:innen insbesondere relevanten Punkte sind unter anderem die Folgenden:

Die Maßnahmen zur Einführung von IVS, müssen unter Anderem laut Anhang II IVS-Richtlinie:

- **f) die Rückwärtskompatibilität wahren**, d.h. sicherstellen, dass IVS, soweit angemessen, zusammen mit bestehenden Systemen betrieben werden können, die einem gemeinsamen Zweck dienen, ohne dass die Entwicklung neuer Technologien dadurch behindert wird (Anhang II f) IVS-Richtlinie);
- **h) den gleichberechtigten Zugang fördern**, d.h. sie dürfen den Zugang besonders gefährdeter Verkehrsteilnehmer zu IVS-Anwendungen und -Diensten nicht behindern oder sich diesbezüglich diskriminierend auswirken (Anhang II h) IVS-Richtlinie);
- **j) die technische Reife belegen**, d.h. nach einer angemessenen Risikobewertung die Zuverlässigkeit innovativer IVS anhand ausreichender technischer Entwicklung und betrieblicher Nutzung nachweisen (Anhang II j) IVS-Richtlinie);
- **l) die Kohärenz wahren**, d.h. den derzeitigen Vorschriften, Strategien und Maßnahmen der Union, die für IVS relevant sind, Rechnung tragen, was insbesondere für den Bereich der Normung gilt (Anhang II h) IVS-Richtlinie.

In Bezug auf die Rückwärtskompatibilität und die Kohärenz bedeutet dies aus rechtlicher Sicht, dass die derzeitigen Standards vor Inbetriebnahme der UDM evaluiert und bei der Entwicklung berücksichtigt und dem Betrieb eingehalten werden müssen.

4.4 Nationale Zugangspunkte und die Spezifikation im Einzelnen

Gewisse Daten müssen in sog. Nationalen Zugangspunkten bereitgestellt werden. Hersteller:innen (und Betreiber:innen) gehören nicht zu dem Kreis der Datenlieferpflichtigen. Allerdings müssen die Hersteller:innen von digitalen Karten, wie der UDM, eine Eigenerklärung gegenüber der Nationalen Stelle für Verkehrsdaten abgeben, dass sie sich an die Anforderungen der EU-Spezifikationen halten. Sie müssen insbesondere sicherstellen, dass Daten,

[134] Vgl. Artikel des BMDV vom 15. Juli 2020, „Intelligente Verkehrssysteme“, https://bmdv.bund.de/DE/Themen/Digitales/Intelligente-Verkehrssysteme/intelligente-verkehrssysteme.html.

[135] Vgl. dynamische Verweisung auf die IVS-Richtlinie in § 3 S. 1 IVSG.

[136] Anhang II zur IVS-Richtlinie: Grundsätze für die Spezifikation und die Einführung von IVS (gemäß den Artikeln 5, 6, und 8 der Richtlinie).

die von Endnutzenden zur Verfügung gestellt werden, pseudonymisiert werden und dass fehlerhafte Daten der zur Verfügung stellenden Stelle gemeldet werden.

Die EU hat weitere Spezifikationen erlassen, insbesondere folgende vorrangige Maßnahmen, die sich auf

- die harmonisierte Bereitstellung einer interoperablen EU-weiten eCall-Anwendung[137];
- die Bereitstellung von Informations- und Reservierungsdiensten für sichere Parkplätze von Lastkraftwagen (LKW) und anderen gewerblichen Fahrzeugen[138]
- Daten und Verfahren, um Straßennutzenden sicherheitsrelevante Verkehrsmeldungen unentgeltlich anzubieten[139];
- die Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste[140] und
- die Bereitstellung EU-weiter multimodaler Reiseinformationsdienste[141]

konzentrieren. Die Mitgliedstaaten müssen sicherstellen, dass bei der Einführung von IVS diese Spezifikationen beachtet werden. Im Folgenden werden kurz die Delegierten Rechtsverordnungen vorgestellt, die für die UDM am relevantesten sind. Genannt werden die (Hersteller) digitale(r) Karten in den DA zu EU-weiten Echtzeit-Verkehrsinformationsdiensten (2022/670) und Informationsdienste für multimodales Reisen (2017/1926). Die IVS-Richtlinie legt Anforderungen fest, die erfüllt sein müssen, um die Richtigkeit von Straßen-, Verkehrs-, und Reisedaten zu gewährleisten, die für digitale Karten verwendet werden. Diese Anforderungen werden in den DA zu EU-weiter Echtzeit-Verkehrsinformationsdienste und zu multimodaler Reiseinformationsdiensten konkretisiert. Sie treffen Regelungen zu:

- Verfügbarkeit der für digitale Karten verwendeten vorhandenen Straßen- und Verkehrsdaten für Hersteller digitaler Karten und Diensteanbieter
- Erleichterung des elektronischen Datenaustauschs zwischen den zuständigen Behörden und Akteuren und den privaten Herstellern digitaler Karten und Diensteanbietern;

[137] Vgl. Delegierte Verordnung (EU) Nr. 305/2013 der Kommission vom 26. November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes.

[138] Vgl. Delegierte Verordnung (EU) Nr. 885/2013 der Kommission vom 15. Mai 2013 zur Ergänzung der IVS-Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lastkraftwagen und andere gewerbliche Fahrzeuge.

[139] Vgl. Delegierte Verordnung (EU) Nr. 886/2013 der Kommission vom 15. Mai 2013 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf Daten und Verfahren für die möglichst unentgeltliche Bereitstellung eines Mindestniveaus allgemeiner für die Straßenverkehrssicherheit relevanter Verkehrsinformationen für die Nutzer.

[140] Vgl. Delegierte Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste; welche am 1. Januar 2025 durch die Delegierte Verordnung (EU) 2022/670 der Kommission vom 2. Februar 2022 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste ersetzt wird.

[141] Vgl. Delegierte Verordnung (EU) 2017/1926 der Kommission vom 31. Mai 2017 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienst.

- zeitnahe Aktualisierung der digitalen Karten durch die Hersteller digitaler Karten und die Diensteanbieter[142]

und werden im Folgenden näher vorgestellt.

4.4.1 Datenlieferungspflicht für Nationale Zugangspunkte

Viele der delegierten Rechtsakte haben gemeinsam, dass sie die Mitgliedsstaaten dazu verpflichten für einen verbesserten Datenzugang und -austausch sogenannte **Nationale Zugangspunkte** (National Access Points, NAPs) einzurichten.[143] Diese sollen als zentrale Anlaufstelle dienen, um den Nutzern den Zugang zu Reise- und Verkehrsdaten zu ermöglichen.

In Deutschland dient die „Mobilithek" (ehemals „Mobilitätsdaten-Marktplatz" und „mCloud") als NAP.

Die Nationale Stelle für Verkehrsdaten stellt klar, wer aufgrund der IVS-Richtlinie und der delegierten Rechtsakte eine sog. **Datenlieferpflicht** für den Nationalen Zugangspunkt hat: Datenlieferpflichtig ist, wer mindestens eine Datenart in digitaler Form vorliegen hat, die in einer der delegierten Verordnungen zur IVS-Richtlinie genannt wird. Wer unter die Datenlieferpflicht fällt, muss eine sog. Eigenerklärung bei der nationalen Stelle abgeben und die Daten im NAP verfügbar machen.

Zusätzlich gibt es die Verpflichtung, eine Eigenerklärung bei der Nationalen Stelle abzugeben, auch **ohne Daten an den nationalen Zugangspunkt liefern (zu müssen).** Dies ist zum Beispiel der Fall bei **Herstellern digitaler Karten oder anderen Dienstanbietern**, die von Straßenverkehrsbehörden oder Straßenbetreibern bereitgestellte Straßendaten verwenden, die in der delegierten Verordnung zu Echtzeit-Verkehrsinformationen aufgezählt sind.[144] In der Eigenerklärung versichern die Datenlieferanten gegenüber der Nationalen Stelle für Verkehrsdaten, die Anforderungen der Spezifikationen, insbesondere in Bezug auf Ermittlung, Zugänglichkeit, Verfügbarkeit, Austausch, Weiterverwendung, Aktualisierung, Format der Daten, Qualitätsmanagement und Inhalt einzuhalten.[145]

Digitale Karten stellen demnach – nach der Auslegung der Nationalen Stelle für Verkehrsdaten im Einklang mit der europäischen und nationalen Gesetzeslage – selbst keine IVS dar, müssen also insofern keine Daten an den Nationalen Zugangspunkt liefern. Trotzdem müssen die Hersteller:innen von digitalen Karten eine **Eigenerklärung** an die Nationale Stelle für Verkehrsdaten abgeben. Die Echtzeit- und multimodalen Reiseinformationen sollen vielmehr **für den Austausch und die Weiterverwendung durch Hersteller:innen digitaler Karten** zur Verfügung gestellt werden. Insofern sind die Hersteller:innen von digitalen Karten in erster Linie Nutzer:innen von IVS. Die UDM ist damit weder ein IVS, noch sind Betreiber:innen der UDM verpflichtet, Daten in den NAP einzuspeisen.

---

[142] Vgl. IVS-Richtlinie, Anhang I, Punkt 1.3.2.

[143] Vgl. Art. 3 Delegierte Verordnung (EU) 2015/962; Art. 3 Delegierte Verordnung (EU) 2017/1926.

[144] Vgl. Auslegung der IVS-Richtlinie und der DA durch die Nationale Stelle für Verkehrsdaten, „Muss ich Daten liefern?", https://nationalestelleverkehr.de/nast/DE/Daten/Lieferung/Daten_node.html, zuletzt aufgerufen am 15. März 2024; Siehe auch § 2 Nr. 12 ISVG: „**Datenlieferant**" **sind** öffentliche oder private Stellen, die Daten dem nationalen Zugangspunkt zur Verfügung stellen, insbesondere Straßenverkehrsbehörden, Straßenbetreiber, **Hersteller digitaler Karten** und Dienstanbieter nach Maßgabe der Delegierten Verordnung (EU) 2015/962, öffentliche und private Straßenbetreiber, Dienstleister, im Bereich der Verkehrsinformationen tätige Rundfunkanbieter nach Maßgabe der Delegierten Verordnung (EU) Nr. 886/2013 sowie Dienstanbieter, Parkplatzbetreiber und Straßenbetreiber nach Maßgabe der Delegierten Verordnung (EU) Nr. 885/2013. Für den Fall, dass auch Daten mit Personenbezug verarbeitet werden, sollten diese anonymisiert werden. Die Daten sind im Einklang mit dem Unionsrecht und dem nationalen Recht zu verarbeiten.".

[145] Vgl. § 6 Abs. 1 Satz 1 IVSG.

4.4.2 DA 2022/670 Bereitstellung EU-weiter Echtzeit-Verkehrsinformations-dienste

Der delegierte Rechtsakt (EU) 2022/670 hebt EU 2015/962 auf und gilt ab dem 1. Januar 2025[146]. Die Spezifikationen in dieser Verordnung sollen die Zugänglichkeit, den Austausch, die Weiterverwendung und die Aktualisierung von Straßen- und Verkehrsdaten durch die Straßenverkehrsbehörden, Straßenbetreiber und Dienstanbieter für EU-weite Echtzeit-Verkehrsinformationsdienste gewährleisten (Art. 1 Abs. 1). Die Echtzeitdaten sollen von den genannten Akteuren erhoben werden und **für** andere Straßenbetreiber, Verkehrsbehörden etc. und **Hersteller digitaler Karten in den** NAPs zur Verfügung gestellt werden (EW 14). Allerdings sollen die Spezifikationen nicht so ausgelegt werden, als würden sie verpflichten, neue Daten zu erheben, die bislang nicht erhoben wurden (vgl. EW 16). Außerdem sollen Dienstanbieter:innen nicht verpflichtet werden, ihre Daten anderen Dienstanbieter:innen zur Verfügung zu stellen (EW 17).

Die Echtzeit-Verkehrsinformationen werden **für** den Austausch und die Weiterverwendung durch **Hersteller:innen digitaler Karten** oder durch Dienstanbieter:innen in der Union diskriminierungsfrei, innerhalb eines Zeitraumes, der die rechtzeitige Bereitstellung des Echtzeit-Verkehrsinformationsdienstes ermöglicht, in dem NAP zur Verfügung gestellt (Art. 4 Abs. 2). Hersteller:innen digitaler Karten arbeiten mit den anderen Datennutzer:innen und Dateninhaber:innen zusammen, damit etwaige Ungenauigkeiten in Bezug auf die Daten den Dateninhaber:innen unverzüglich gemeldet werden (Art. 4 Abs. 3).

Gegenüber der alten Fassung (DA 2015/962) hat sich vor allem geändert, dass nun auch die Metadaten für Datennutzer:innen über die NAPs bereitgestellt werden sollen (vgl. Art. 3 Abs. 4 DA 2022/670); dass Mindestqualitätsanforderungen an die Daten gestellt werden und diese nicht mehr nur „rechtzeitig", sondern „*innerhalb eines Zeitrahmens, der eine zuverlässige und wirksame Verwendung der Daten zur Erstellung von Echtzeit-Verkehrsinformationen ermöglicht*" (vgl. Art. 4 Abs. 2 lit. b, c DA 2022/670) bereitgestellt werden sollen. Damit ist der Zeitrahmen gegenüber der alten Fassung wesentlich eingeschränkt. Allerdings ist die Formulierung noch immer vage. Eine genaue Bereitstellungsfrist lässt sich daraus nicht ableiten. Trotzdem darf aufgrund der Neufassung erwartet werden, dass mehr aktuelle und Echtzeit-Daten geteilt werden, da ansonsten die Erstellung von Echtzeit-Verkehrsinformationen nicht möglich wäre.[147]

Art. 7 Abs. 3 der DA 2022/670 sieht vor, dass Straßenverkehrsbehörden und Straßenbetreiber:innen von Inhaber:innen im Fahrzeug erzeugter Daten und von Diensteanbieter:innen verlangen können, die Arten von Daten über die Echtzeit-Benutzung des Netzes zur Verfügung stellen, die sie gemäß Art. 11 der DA erheben und aktualisieren. Die Daten über die Echtzeit-Benutzung des Netzes bezeichnet nach Art. 2 Nr. 28 der DA solche Daten, die die derzeitige Benutzung des Straßennetzes und die Benutzungsmöglichkeiten im Straßennetz beschreiben. Damit kann unter Umständen das Teilen von Daten zu Baustellen, Stauentwicklungen und anderweitigen Verkehrshindernissen erforderlich werden. Diese Daten sollten unter den sog. FRAND-Bedingungen (fair, angemessen und diskriminierungsfrei) i. S. d. Art. 2 Nr. 32 der DA zur Verfügung gestellt werden und im Format DATEX II oder einem von den Mitgliedstaaten digitalen maschinenlesbaren Format bereitgestellt werden. Damit werden die Anforderungen der DS-GVO spezifiziert. Hierdurch soll sichergestellt werden, dass die Daten fair und

[146] Bis auf die Berichterstattungspflicht durch die Mitgliedstaaten, welche schon ab 2023 gilt, vgl. Art. 13 DA EU 2022/670.

[147] Hinweis: EW 12 DA 2022/670 stellt klar, dass alle personenbezogenen Daten, die anfallen, im Einklang mit der DSGVO und Datenschutzrichtlinie für elektronische Kommunikation verarbeitet werden.

diskriminierungsfrei und in einer einheitlichen Form verfügbar gemacht werden, sodass die bereitgestellten Informationen zuverlässig in Echtzeit-Verkehrsmanagement umgesetzt werden können.

Um diesen Anforderungen gerecht zu werden, muss die UDM so konzipiert werden, dass sie die relevanten Echtzeitdaten über die Nutzung des Verkehrsnetzes erfasst und bereitstellt. Die Erfassung erfolgt bereits nach der derzeitigen Planungsphase innerhalb von EDDY. Lediglich die Bereitstellung der Erkenntnisse zu möglichen Echtzeit-Einschränkungen innerhalb des Netzes im Rahmen der Ermessensausübung durch die zuständige Stelle, wurde noch nicht implementiert. Dies wird jedoch erst bei Ermessensausübung durch die zuständige Straßenverkehrsbehörde relevant. Bisher ist eine solche Ermessensausübung noch nicht erfolgt. Angesichts der gesellschaftlichen Sensibilität hinsichtlich möglicher Datenteilungspflichten an öffentliche Stellen sowie der oben angeführten weniger invasiven Alternativen ist dies auch zukünftig nicht absehbar. Dennoch könnten die Mechanismen bereits geschaffen werden, um auf ein mögliches Informationsverlangen der zuständigen Behörden reagieren zu können. Damit müssen die bereits innerhalb der vorliegenden UDM erfassten Daten relevanten Informationen über das Straßenverkehrsgeschehen extrahiert werden, nachdem die diesen zugrundeliegenden personenbezogenen Daten gelöscht wurden. So wird sowohl den Anforderungen der DA (EU) 2022/670 als auch den Datenschutzanforderungen der DS-GVO hinsichtlich der Datenminimierung genügt. Zudem wird sichergestellt, dass für die Zwecke des Verkehrsmanagements die Echtzeit-Verkehrsinformationen verfügbar gemacht werden.

4.4.3 DA 2017/1926 - Informationsdienste für multimodales Reisen

Diese Verordnung richtet sich an alle Verkehrsträger in der Union[148] und soll die Richtigkeit und grenzüberschreitende Verfügbarkeit von EU-weiten multimodalen Reiseinformationsdiensten für IVS-Nutzer:innen gewährleisten (Art. 1). **Verkehrsbehörden, Verkehrsbetreiber:innen, Infrastrukturbetreiber:innen oder Anbieter:innen von nachfrageorientierten Verkehrsangeboten gewährleisten**, dass geeignete Metadaten zur Verfügung stehen, die es den Nutzer:innen erlauben, die über den NAP bereitgestellten Datensätze zu finden und zu nutzen (Art. 3 Abs. 4).

Hersteller:innen digitaler Karten sollen außerdem geeignete technische Maßnahmen ergreifen, um sicherzustellen, dass die von den Endnutzer:innen übermittelten Daten pseudonymisiert werden, wenn sie für einen Informationsdienst für multimodales Reisen erhoben werden. Dies beinhaltet auch Standortdaten.[149] Hier richtet sich die delegierte Verordnung direkt an die Hersteller:innen von digitalen Karten und nimmt sie in die Pflicht.

4.4.4 Ausblick für die Spezifikationen

Nach der bisherigen IVS-Richtlinie (Stand der Richtlinie von 2017) müssen die Mitgliedstaaten die erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass die Spezifikationen für IVS-Anwendungen und -dienste eingehalten werden, wenn und soweit IVS in dem jeweiligen Mitgliedsstaat genutzt werden. Das Recht der Staaten, über die Einführung solcher IVS in ihrem Hoheitsgebiet zu entscheiden, bleibt davon unberührt. Wenn jedoch IVS eingeführt werden, müssen die Vorgaben der IVS-Richtlinie bzw. des IVSG und der Spezifikationen eingehalten werden. Durch die neuesten Änderungen der IVS-Richtlinie von 2023 wird die Bereitstellung von Daten für IVS-Anwendungen teilweise obligatorisch. Allerdings nur, wenn die zugrundeliegenden Informationen bereits vorhanden sind. Daher enthält die "neue" IVS-Richtlinie teilweise die Verpflichtung, bestimmte Daten aus bestimmten geographischen

[148] Vgl. Erwägungsgrund 8 DA (EU) 2017/1926.

[149] Vgl. Erwägungsgrund 6 DA (EU) 2017/1926.

Gebieten zur Verfügung zu stellen, wie in Anhang III der Richtlinie dargelegt. Jedoch enthält sie nicht die Verpflichtung, IVS-Dienste und -Anwendungen einzuführen. Mit dieser Neuerung der IVS-Richtlinie zeigt die EU, dass es künftig mehr Verbindlichkeiten und Verpflichtungen in Bezug auf das Teilen und Erheben von Mobilitätsdaten geben soll. Wenn mehr IVS zur Verfügung stehen, können davon auch Hersteller:innen und Betreiber:innen digitaler Karten profitieren. Eine erneute Revision der IVS-Richtlinie ist allerdings erst für 2028 geplant.

4.5 Schlussfolgerungen zur IVS-Richtlinie

Insgesamt bleiben viele der Spezifikationen wenig konkret und machen keine genauen Vorgaben für die (technische) Ausgestaltung von IVS. Dies liegt vor allem daran, dass die IVS-Richtlinie in erster Linie darauf abzielt, innereuropäische Kompatibilität zwischen IVS zu gewährleisten und nicht auf eine technische Regulierung von IVS selbst.[150] Insofern handelt es sich bei IVS bisher noch um ein relativ grobes Konzept. Sowohl der EU-Rechtsrahmen als auch die deutsche Gesetzgebung sind nicht ausreichend, um ein klares Bild von IVS und den Anforderungen an diese zu zeichnen.[151] Digitale Karten gelten selbst nicht als IVS, können aber in ein solches System eingebettet sein. In den DA sind digitale Karten vor allem als Nutzer:innen von IVS und den dazugehörigen Daten angesprochen, weniger als Einspeiser von Daten oder Verpflichtete. Hersteller:innen von digitalen Karten sollen allerdings sicherstellen, dass sie falsche Verkehrsinformationen melden und Daten, die von Endnutzer:innen bereitgestellt werden, pseudonymisieren.

Die Positionierungsunterstützung ist kein Thema der DAs, auch wenn Echtzeitverkehrsinformationen durch entsprechende Dienste gefördert werden. Die Navigation und Steuerung einzelner Fahrzeuge ist weniger Thema als vielmehr das allgemeine Verkehrsmanagement vieler Fahrzeuge. In neuen Spezifikationen der Kommission könnte sich das allerdings ändern. Die Betreiber:innen der UDM müssen sich daher regelmäßig informieren, ob die Kommission neue Spezifikationen erlassen hat.

[150] Vgl. Erwägungsgrund 7, 19 zur IVS-Richtlinie.

[151] Vgl. *Jochum*, ZD 2020, 497 (501).

5 Datenökonomie

In diesem Kapitel werden Fragen zur Datenökonomie, das heißt insbesondere zu Datenweitergabepflichten, Informationspflichten und -ansprüchen behandelt. Die UDM ist keine kritische Infrastruktur. Die Cybersecurity-Anforderungen für kritische Infrastrukturen gelten damit nicht für die UDM. Trotzdem sollten alle Möglichkeiten ausgeschöpft werden, um die UDM so sicher zu betreiben wie möglich.
Wenn die UDM durch eine öffentliche Stelle betrieben wird, können sich Informationsauskunftsansprüche aus den Informationsfreiheitsgesetzen (des Bundes und der Länder), sowie aus dem Datennutzungsgesetz ergeben. Nach der jetzigen Rechtslage gehört der Aufbau und Betrieb einer UDM nicht zu den Pflichten der öffentlichen Hand, da es nicht Teil der öffentlichen Daseinsvorsorge ist. Da keine Haftung für die (inhaltliche) Richtigkeit der Daten der UDM übernommen wird, sind die Anwendungsfälle begrenzt. Trotzdem bietet der Betrieb einer UDM eine Reihe von Vorteilen für die öffentliche Hand: z.B. für verwaltungsinterne Anwendungen („IT-Legal-Enforcement-Support") und Unterstützung von allgemeinem Verkehrsmanagement.

5.1 Schutz vor Missbrauch durch Gestaltung der UDM

Die UDM gehört nicht zur sog. „kritischen Infrastruktur" und unterliegt damit nicht den strengen rechtlichen Anforderungen der Regelungen zu kritischer Infrastruktur. Nichtsdestotrotz, müssen grundlegende (Cyber-)Sicherheitsstandards beachtet werden, z.B. die ISO-Norm ISO 18750:2018, die für Intelligente Verkehrssysteme gilt.

5.1.1 Cybersecurity

Bei der technischen Entwicklung und dem Betrieb muss die UDM so gut wie möglich gegen Missbrauch geschützt werden. Dabei spielt auch die Einhaltung von Cybersecurity-Vorschriften eine Rolle.

Welche Sicherheitsstandards für Systeme wie eine UDM eingehalten werden müssen, hängt davon ab, ob es sich dabei um kritische Infrastruktur handelt. Für kritische Infrastruktur gelten im Hinblick auf die Cybersecurity strengere Maßstäbe als für andere Systeme, die nicht-kritische Infrastruktur sind.

Es ist somit zu untersuchen, ob eine UDM als kritische Infrastruktur im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)[152] angesehen werden kann. Nach § 8 Abs. 3 BSI-KritisV sind Kritische Infrastrukturen im Sektor Transport und Verkehr, Anlagen, oder Teile von Anlagen, die den in Anhang 7 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und in der entsprechenden Spalte D den genannten Grenzwert überschreiten. In Frage kommt hier die Einordnung einer UDM entweder als Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr gemäß Anlage 7 Teil 3 1.4.1 BSI-KritisV. Dazu müsste die Anzahl der Einwohner:innen der

[152] BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 23. Februar 2023 (BGBl. 2023 I Nr. 53) geändert worden ist.

versorgten Stadt beziehungsweise die Anzahl der angeschlossenen Nutzer:innen oder durchschnittlich im Versorgungsgebiet versorgten Nutzer:innen 500.000 Personen übersteigen.

Die Richtlinie 2008/114/EG[153] beschreibt in ihrem Art. 2a) Kritische Infrastruktur als *die in einem Mitgliedsstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrecht erhalten werden könnten*. Im Moment sind die Daten in einer UDM nicht verlässlich genug, als dass autonome Fahrzeuge nur mit Hilfe der UDM navigiert werden könnten, vgl. „3.2 Use Case 2: Nutzbarkeit und Verbindlichkeit von Daten in der UDM". Außerdem ist das autonome Fahren in Deutschland noch nicht so etabliert, als dass der Verkehrssektor zusammenbrechen würde, falls die UDM ausfiele und die autonomen Fahrzeuge nicht mehr navigieren könnten. Die UDM ist damit kein Teil eines Systems, das von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen ist. Die UDM ist damit nicht als kritische Infrastruktur zu qualifizieren. Demnach müssen auch nicht die erhöhten Cybersecurity-Standards für KRITIS eingehalten werden.

Für autonome Fahrzeuge gelten noch eine Reihe weiterer (Cyber-)Sicherheitsvorschriften, welche aber nicht direkt die UMD betreffen, sondern nur die Anwendung der UDM durch den Fahrzeughersteller (z. B. wenn dieser die UDM in sein Navigationssystem integriert). Solche Sicherheitsregelungen finden sich z.B. in Nr. 155 und 156 der UN/ECE-Vorschriften.

5.1.2 Weitere Maßnahmen, um Missbrauch der UDM zu verhindern

Die Betreiber:innen einer UDM sollten alle möglichen Mittel nutzen, um die Einspeisung von fehlerhaften Daten von außen in die UDM zu verhindern. Ansonsten kann die UDM für die oben genannten Vergehen und Verbrechen instrumentalisiert werden. Auch wenn es besonders schwer ist, Daten auf deren inhaltliche Richtigkeit zu überprüfen, sollte hierauf bei Programmierung und Entwicklung der UDM geachtet werden. Soweit möglich sollte eine Validierung der Datensätze vorgenommen werden. Jedenfalls aber sollten „technisch fehlerhafte" Daten vor Einspeisung in die UDM herausgefiltert werden.

Für LDMs muss außerdem der **ISO-Standard ISO 18750:2018**[154] beachtet werden. Das Dokument enthält unter anderem Standards für einen sicheren Zugang zum Hinzufügen, Aktualisieren und Löschen für IVS-Anwendungsprozesse, sichere Benachrichtigen nach Anmeldungen an IVS, Mittel zur Aufrechterhaltung des Inhalts und der Integrität des Datenspeichers der LDM. Diese ISO-Standards müssen auch bei dem Betrieb einer UDM eingehalten werden.

5.1.3 Fazit

Die UDM ist keine kritische Infrastruktur. Die Cybersecurity-Anforderungen der KRITIS-VO gelten nicht für die UDM. Trotzdem sollten alle Möglichkeiten ausgeschöpft werden, um die UDM so sicher zu betreiben wie möglich. Mindestens technisch fehlerhafte Daten sollten im Rahmen einer

[153] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

[154] Vgl. ISO 18750:2018 Intelligent transport systems – Co-operative ITS – local dynamic Map, https://www.iso.org/standard/69433.html.

Datenvalidierung aussortiert werden. Außerdem müssen die für LDMs geltenden ISO-Standards berücksichtigt werden.

5.2 Datenökonomie

Aus den Informationsfreiheitsgesetzen der Länder und des Bundes und dem Datennutzungsgesetz des Bundes können sich Auskunftsansprüche gegenüber einer:s öffentlichen Betreiber:in ergeben. Diese:r muss dann die Informationen an Dritte zur Verfügung stellen. Aus den Regulierungen zu IVS folgt keine Datenlieferpflicht (nur eine sog. Kontrollpflicht). Auch aus dem Personenbeförderungsgesetz, dem Data Act und dem Data Governance Act folgen keine Auskunftsverpflichtungen für die Betreiber:innen der UDM. Der Nationale Zugangspunkt (NAP) für Verkehrsdaten in Deutschland ist die „Mobilithek". Auch wenn keine Daten im NAP zur Verfügung gestellt werden müssen, ist eine freiwillige Bereitstellung möglich. Die Daten aus dem NAP können für den Aufbau der UDM genutzt werden. Auch der noch im Aufbau befindliche European Mobility Data Space (EMDS) kann zu diesem Zweck für die UDM genutzt werden. So wird gleichzeitig ein Beitrag zur verbesserten Datennutzung in der EU und für einen besseren Datenaustausches im Mobilitätssektor geleistet.

In Systemen, in denen eine Vielzahl von Daten gesammelt werden, stellt sich zwangsläufig die Frage, wem diese Daten in welcher Form zur Verfügung gestellt werden müssen. Diese Frage ist insbesondere interessant, wenn es sich bei den Betreiber:innen des Systems um staatliche Akteure handelt, wie dies z.B. bei EDDY der Fall ist. Hier ist die Stadt Hamburg die Betreiberin.

Zunächst ist allerdings zu klären, was genau unter **Mobilitätsdaten** verstanden wird und welcher Natur diese sind. Eine klare Definition, was genau unter Mobilitätsdaten zu verstehen ist, gibt es nicht. Auch in den ersten Sondierungspapieren der EU zum gemeinsamen Europäischen Mobilitätsdatenraum (EMDS) findet sich keine Definition von Mobilitätsdaten. Hier wird lediglich von Daten aus verschiedenen Quellen gesprochen.[155] Im Personenbeförderungsgesetz (PBefG)[156] wird der Begriff verwendet, um Daten über die Angebote des öffentlichen Personennahverkehrs zu bezeichnen, vgl. § 3a Abs. 1 PBefG. Diese Daten gehören mehrheitlich zu den nicht-personenbezogenen Daten. Zu Mobilitätsdaten gehören aber weitaus mehr als im PBefG angelegt. Dazu gehören auch Daten über die Verkehrsinfrastruktur, Echtzeitdaten zur Verkehrslage und Fahrgastströme.[157] Bei den von der UDM genutzten Daten, wie Verkehrs- und Positionsdaten, Fahrplandaten, Auslastungsdaten sowie Daten für geplante Routen und Wege handelt es sich aber zum Teil um personenbezogene Daten.[158] Nach Art. 4 Abs. 1 DS-GVO handelt es sich bei personenbezogenen Daten, um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird dabei eine Person angesehen, wenn sie direkt oder indirekt mittels Zuordnung zu einer Kennung (z.B. einem Namen)

[155] Mitteilung der EU-Kommission „Verkehrsdaten – Schaffung eines gemeinsamen europäischen Mobilitätsdatenraums", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Verkehrsdaten-Schaffung-eines-gemeinsamen-europaischen-Mobilitatsdatenraums-Mitteilung- de (zuletzt aufgerufen am 31. Juli 2024).

[156] Personenbeförderungsgesetz in der Fassung der Bekanntmachung vom 8. August 1990 (BGBl. I S. 1690), das zuletzt durch Artikel 23 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert wo

[157] Mitteilung der EU-Kommission „Verkehrsdaten – Schaffung eines gemeinsamen europäischen Mobilitätsdatenraums", https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Verkehrsdaten-Schaffung-eines-gemeinsamen-europaischen-Mobilitatsdatenraums-Mitteilung- de (zuletzt aufgerufen am 31. Juli 2024).

[158] Vgl. *Steege*, MMR 2019, 508 (511).

unter anderem zu Standorten zugeordnet werden kann. Wenn also mittels des Standorts Rückschlüsse auf die Identität der Person gezogen werden können, handelt es sich bei den Mobilitätsdaten um personenbezogene Daten im Sinne des Art. 4 Abs. 1 DS-GVO. Damit können Mobilitätsdaten personenbezogen sein, müssen sie aber nicht.

Datenweitergabepflichten können sich aus verschiedenen rechtlichen Grundlagen ergeben (siehe hierzu insbesondere 4.4.2.). Insbesondere aus der Zurverfügungstellung von Mobilitätsdaten an bestimmte Akteure, können auch Pflichten erwachsen, die Daten an weitere Stellen weitergeben zu müssen. Dabei bewegen sich diese Rechte für Zugang zu Informationen immer in einem Spannungsverhältnis zwischen (demokratischer) Transparenz und Datenschutz.

5.2.1 Aus den Informationsfreiheitsgesetzen

Wenn es sich bei den Mobilitätsdaten um amtliche Informationen handelt, können Zugangsansprüche aus dem **Informationsfreiheitsgesetz (IFG)**[159] **des Bundes** erwachsen. § 1 IFG legt fest, dass jeder nach Maßgabe dieses Gesetzes gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen hat. In Bezug auf eine UDM wäre das IFG demnach nur anwendbar, wenn die UDM durch eine Bundesbehörde betrieben wird. § 2 Nr. 1 IFG besagt, dass amtliche Informationen jegliche amtlichen Zwecken dienende Aufzeichnungen, unabhängig von der Art ihrer Speicherung, sind. Die Bezeichnung der Informationen als amtlich dient hauptsächlich der Abgrenzung zu privaten Informationen.[160] Die in einer UDM gespeicherten Daten einer Bundesbehörde können damit als amtliche Information i. S. d. IFG angesehen werden.
Zu beachten ist, dass § 7 Abs. 1 IFG einen Antrag vorsieht. Somit erwächst allein aus der Sammlung und Verarbeitung von Mobilitätsdaten für die Bundesbehörden noch nicht die Pflicht, diese den Bürger:innen zur Verfügung zu stellen. Insofern handelt es sich auch bei dem IFG nicht um einen gänzlich voraussetzungslosen Anspruch. Die Voraussetzungslosigkeit bezieht sich lediglich auf materiellrechtliche Voraussetzungen.[161] Das IFG sieht eine Reihe von Ausnahmetatbeständen vor, wann der Anspruch auf Informationszugang nicht besteht oder nicht erfüllt werden kann, vgl. §§ 3 ff. IFG. Nach § 5 Abs. 1 IFG darf der Zugang zu personenbezogenen Daten nur gewährt werden, *soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat*. Da es sich, wie bereits aufgeführt, bei Mobilitäts- und Verkehrsdaten in der UDM oftmals um personenbezogene Daten handelt, wird der § 5 IFG zu beachten sein.

Auch einige **Länder** haben **Informationsfreiheitsgesetze** erlassen, welche sich dann an die jeweiligen Landesbehörden richten. Bis auf Bayern, Sachsen und Niedersachsen verfügen alle Bundesländer über ein Informationsfreiheitsgesetz. Allerdings schwankt der Ausbau der Informationsfreiheit in den einzelnen Ländern stark. Während in Hamburg und Schleswig-Holstein, die Informationstransparenz am höchsten ist, ist diese in Hessen oder Baden-Württemberg am niedrigsten.[162] Besonders

---

[159] Informationsfreiheitsgesetz vom 5. September 2005 (BGBl. I S. 2722), das zuletzt durch Artikel 44 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

[160] *Schoch*, IFG, § 2 Rn. 47.

[161] *Schoch*, IFG, § 1, Rn. 17.

[162] Vgl. hierzu *Semsrott,* Transparenzranking 2021 von Mehr Demokratie e.V. und der Open Knowledge Foundation e.V., 1. Auflage 2021. Nach den Kategorien des Autors liegt Hamburg auf Platz 1 mit einer Transparenzquote von 66%, gefolgt von Schleswig-Holstein mit 65%. Die Bundesländer ohne Informationsfreiheitsgesetze belegen die Plätze 16, sodass Bremen mit einer Transparenzquote von 12% auf dem 13. Platz liegt. Davor auf dem 12.Platz liegt Baden-Württemberg mit 31%. Zum Vergleich: das IFG des Bundes erreicht bei diesen Kriterien eine Transparenzquote von 37%. https://transparenzranking.de.

hervorzuheben ist dabei, dass nach dem Hamburgischen Transparenzgesetz (HmbTG)[163] die Bürger:innen, nicht nur einen Anspruch auf Auskunft haben, sondern, im Vergleich zum IFG, die hamburgischen Behörden von sich aus auskunftspflichtig sind. Nach § 1 Abs. 2 HmbTG hat jede Person nach Maßgabe des Gesetzes Anspruch auf den unverzüglichen Zugang zu allen amtlichen Informationen der **auskunftspflichtigen** Stellen sowie auf Veröffentlichung der in § 3 Abs. 1 HmbTG genannten Informationen. Ein vorheriger Antrag ist nicht notwendig. Die hamburgischen Behörden müssen die Informationen proaktiv zur Verfügung stellen, vgl. auch § 2 Abs. 7 und Abs. 9 HmbTG. Auch in den Gesetzen der Länder wurde dem Schutz von personenbezogenen Daten Rechnung getragen, auch wenn dieser zum Teil unterschiedlich ausgestaltet wurde; vgl. z.B. § 4 HmbTG, § 10 Nr. 1 IZG-SH[164], § 6 IFG-Bln[165] und § 5 LIFG-BaWü[166]. Bei der Zurverfügungstellung der Informationen muss der Schutz personenbezogener Daten entsprechend dem Landesrecht beachtet werden.

5.2.2 Aus dem Personenbeförderungsgesetz

Eine Verpflichtung zur Datenweitergabe kann sich weiterhin aus dem Personenbeförderungsgesetz (PBefG) ergeben.[167] Nach **§ 3a PBefG** sind Unternehmer und Vermittler von Personenbeförderungsdiensten verpflichtet, gewisse statische und dynamische Daten, die im Zusammenhang mit der Beförderung von Personen im Linienverkehr und im Gelegenheitsverkehr in der „Mobilithek" bereitzustellen.

Zu den personenbefördernden Unternehmen i. S. d. § 3a PBefG gehören gem. § 2 Abs. 1 S. 2 i. V. m. § 1 Abs. 1 PBefG natürliche oder juristische Personen, die gegen Entgelt geschäftsmäßig Personen befördern. Aufgrund von § 1a PBefG sind weiterhin Dienstleister erfasst, deren Tätigkeit in einer Vermittlung besteht, die allerdings organisatorisch und vertraglich die gesamte Abwicklung bereitstellen. Eine Bereitstellungsverpflichtung greift weiterhin nach § 2 Abs. 1b i. V. m. § 1 Abs. 3 PBefG für Unternehmen, die im Wesentlichen zum Zwecke des Vertragsschlusses über Personenbeförderungen, Mobilitätsplattformen betreiben, ohne dabei jedoch selbst Beförderungen vorzunehmen (z.B. Taxizentralen).[168] Da der Betreiber einer UDM weder direkt noch organisatorisch oder vertraglich Personenbeförderung betreibt, kann er nur von § 3a PBefG erfasst sein, wenn die UDM als Mobilitätsplattform zum Zwecke der Personenbeförderung gilt. Die UDM hat zum Zweck, dass Verkehrsabläufe optimiert und sicherer gestaltet werden können.

Allerdings soll die UDM erstmals der Allgemeinheit zur Verfügung gestellt werden. Welche Anwendungen aus der UDM heraus später durch andere Unternehmer:innen entwickelt werden, soll nicht Gegenstand dieses Projekts sein. Auch wenn es möglich ist, dass die UDM künftig als Mobilitätsplattform zur Personenbeförderung (z.B. durch autonome Shuttles, welche man direkt hierüber buchen kann)

---

[163] Hamburgisches Transparenzgesetz (HmbTG) vom 19. Juni 2012 (HmbGVBl. 2012, S. 271) Zuletzt geändert durch Artikel 1 des Gesetzes vom 19. Dezember 2019 (HmbGVBl. 2020, S. 19).

[164] Informationszugangsgesetz für das Land Schleswig-Holstein (IZG-SH) vom 19. Januar 2012, letzte berücksichtigte Änderung: Inhaltsübersicht, §§ 1 und 12 geändert, § 14 neu gefasst (Art. 5 Ges. v. 16.03.2022, GVOBl. S. 285).

[165] Gesetz zur Förderung der Informationsfreiheit im Land Berlin (Berliner Informationsfreiheitsgesetz - IFG) vom 15. Oktober 1999, letzte berücksichtigte Änderung: § 4 a eingefügt, §§ 6 und 17 geändert, § 18 neu gefasst durch Artikel 5 des Gesetzes vom 12.10.2020 (GVBl. S. 807).

[166] Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg (Landesinformationsfreiheitsgesetz - LIFG) vom 17. Dezember 2015, zuletzt geändert am 12.06.2018.

[167] Personenbeförderungsgesetz in der Fassung der Bekanntmachung vom 8. August 1990 (BGBl. I S. 1690), das zuletzt durch Artikel 23 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert wo

[168] *Mayer/Bomhard/Etzkorn*, Mobilitätsdatenverordnung, RDi 2022, 446 ff., Rn. 5ff.

genutzt wird und die Verkehrsteilnehmende mit ihrer Hilfe planen können, so ist dies im jetzigen Stadium noch nicht der Fall. Danach fällt allein der Betrieb der UDM ohne entsprechende Anwendungen, die in Beziehung zur Personenbeförderung stehen, nicht unter § 3a PBefG. Aus dem PBefG ergeben sich somit keine Pflichten zur Datenweitergabe.

5.2.2.1 Exkurs: Die „Mobilithek“ und der Gemeinsame Europäische Mobilitätsdatenraum (EMDS)

Der (staatliche) Betreiber einer UDM kann und muss nicht nur selbst Daten zur Verfügung stellen. Durch die „Mobilithek“ kann er schon jetzt auf eine Reihe Mobilitätsdaten zugreifen. Künftig kann er auch den sich in der Entwicklung befindlichen Gemeinsamen Europäischen Mobilitätsdatenraum (EMDS) nutzen.

Der § 3a PBefG schreibt zusammen mit der Mobilitätsdatenverordnung (MDV)[169] eine Pflicht zur Bereitstellung von Mobilitätsdaten vor. Diese Daten sollen in der Mobilithek zur Verfügung gestellt werden. Die Mobilithek hat den Mobilitäts-Daten-Marktplatz (MDM) und mCloud als Nationalen Zugangspunkt für Mobilitätsdaten abgelöst und setzt so die Anforderungen aus der delegierten Rechtsverordnung zur europäischen IVS-Richtlinie (vgl. § 2 Nr. 11 IVS-Gesetz) sowie des PBefG um. Hersteller:innen und Betreiber:innen der UDM sind jedoch nicht datenlieferpflichtig in Bezug auf die NAPs.[170]

Allerdings ist die Mobilithek umso nützlicher, je mehr Daten eingespeist werden. Demnach darf jede:r freiwillig Daten bereitstellen.[171] Eine vorherige Registrierung oder Einspeisung von eigenen Daten in die Mobilithek ist nicht notwendig, um auf die Daten zuzugreifen. Allerdings können registrierte Nutzer:innen auf mehr Daten zugreifen. Insofern empfiehlt sich für den Betreiber der UDM, sich in der Mobilithek zu registrieren.

Auch die Entwicklung eines Gemeinsamen Europäischen Mobilitätsdatenraums (EMDS) wird dadurch vorangetrieben. Die Initiative startete im März 2022. Eine Annahme durch die EU-Kommission ist für das zweite Quartal 2023 geplant, aber noch nicht erfolgt (Stand: 31. Juli 2024).[172] Der Aufbau eines EMDS ist Teil der „EU-Datenstrategie“. Nationale Initiativen, sowie die Nationalen Zugangspunkte, sollen dabei als „Säulen“ oder “Rückgrat“ des EMDS dienen. Ziel ist es eine große Datenmenge in maschinenlesbarem Format bereitzustellen und die Interoperabilität zwischen einzelnen (nationalen) Initiativen zu verbessern.[173] Wie genau der EMDS dabei ausgestaltet werden soll, ist noch nicht ganz klar. Die Abbildung zeigt, wie die Struktur des EMDS und der Datenfluss nach den Vorstellungen der EU-Kommission aussehen soll. Der EMDS ist dabei auf andere (nationale) Initiativen und Datenökosysteme angewiesen.

---

[169] Mobilitätsdatenverordnung vom 20. Oktober 2021 (BGBl. I S. 4728), die zuletzt durch Artikel 1 der Verordnung vom 1. Juli 2022 (BGBl. I S. 1039) geändert worden ist.

[170] Vgl. „4.4.14.4.1. **Datenlieferungspflicht für Nationale Zugangspunkte**“.

[171] *Mayer/Bomhard/Etzkorn*, Mobilitätsdatenverordnung (MDV) – Neuer Rechtsrahmen für die Bereitstellung von Mobilitätsdaten, RDi 2022, 446 (449).

[172] Mitteilung der EU-KOM „Verkehrsdaten- Schaffung eines gemeinsamen europäischen Datenraums“, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Verkehrsdaten-Schaffung-eines-gemeinsamen-europaischen-Mobilitatsdatenraums-Mitteilung- de (zuletzt aufgerufen am 07. Juni 2023); vgl. https://digital-strategy.ec.europa.eu/en/news/completion-prepdspace4mobility („still in finalization“), (zuletzt aufgerufen am 01. April 2024.

[173] Vgl. „Erschließung des Potenzials von Mobilitätsdaten“, https://digital-strategy.ec.europa.eu/de/policies/mobility-data (zuletzt aufgerufen am 31. Juli 2024).

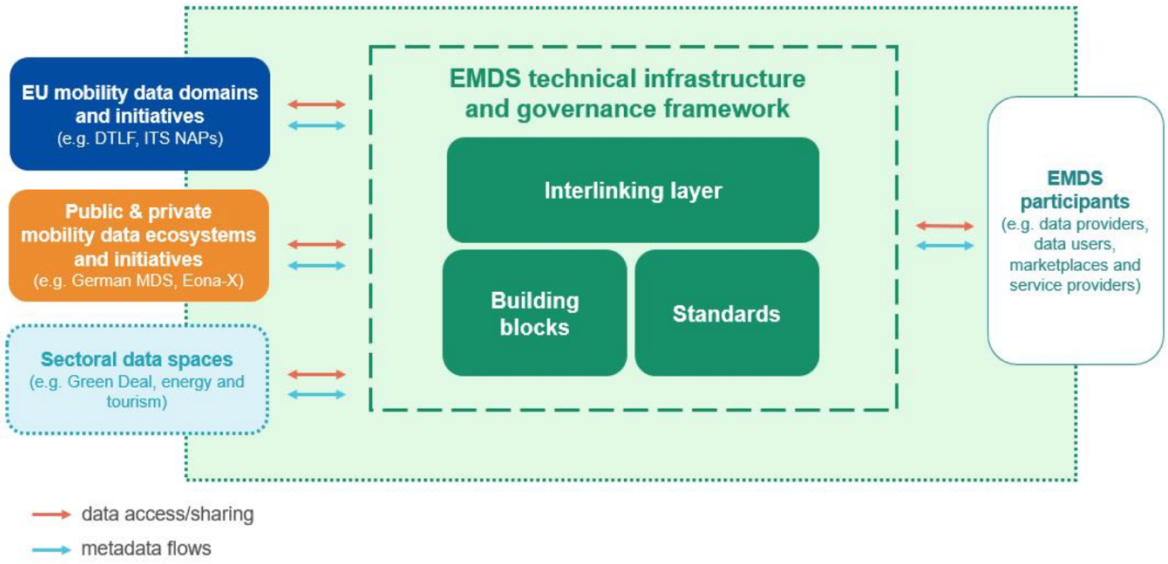

Abbildung 3: Geplantes Konzept für den EMDS[174]

Jedenfalls aber kann der EMDS, wie im Moment die nationale „Mobilithek", genutzt werden, um notwendige Daten zu beziehen. So kann der Betrieb der UDM von den im EMDS bereitgestellten Daten profitieren. Auch durch Teilen eigens ermittelter Daten, kann EDDY einen Beitrag zur verbesserten Datennutzung in der EU und zur Förderung des Datenaustausches im Mobilitätssektor leisten.

5.2.3 Aus dem Datennutzungsgesetz

Das Datennutzungsgesetz (DNG)[175] setzt die Richtlinie (EU) 2019/1024[176] um. § 1 Abs. 2 DNG stellt fest, dass eine Bereitstellungspflicht oder ein Anspruch auf Zugang zu Daten aufgrund dieses Gesetzes nicht begründet wird. Allerdings muss sich das Handeln der Verwaltung an Art. 3 Abs. 1 GG, am Grundsatz der Selbstbindung, messen lassen, sodass ein Gleichbehandlungsanspruch entsteht, sobald die Verwaltung die Daten einem Akteur zugänglich macht.[177] Dies schlägt sich in § 2 Abs. 1 DNG nieder. Eine Ungleichbehandlung ließe sich nur durch einen „*vernünftigen, sich aus der Natur der Sache ergebenden oder sonst wie sachlich einleuchtenden Grund*"[178] rechtfertigen. Zum einen dürfte eine Reihe der Ansprüche zur Datenweitergabe schon nicht bestehen, wenn personenbezogene Daten betroffen sind, vgl. z.B. § 5 IFG. Zum anderen stellt der Schutz von personenbezogenen Daten einen sachlich

[174] Bild Quelle: COM(2023) 751 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Creation of a common European mobility data space", 29. November 2023, Punkt 4.2; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0751 (zuletzt aufgerufen am 31. Juli 2024).

[175] Gesetz für die Nutzung von Daten des öffentlichen Sektors – Datennutzungsgesetz (DNG), vom 16. Juli 2021 (BGBl. I S. 2941, 2942; 4114).

[176] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. L 172/56.

[177] Vgl. *Martini/Haßecker/Wagner*, Das DNG als digitalpolitischer Ordnungsrahmen für die Monetarisierung kommunaler Daten, NVwZ-Extra 11/2022, 8 f.

[178] BVerfGE NJW 1951, 877 (878); seitdem ständige Rechtsprechung.

einleuchtenden Grund dar. So kann auch unter dem DNG der Konflikt zwischen Transparenz und Datenschutz gelöst werden.

5.2.4 Data Act und Data Governance Act

Sowohl der Data Act als auch der Data Governance Act bedürfen als europäische Verordnungen keines Umsetzungsakts, sondern gelten nach ihrem Inkrafttreten unmittelbar und verbindlich in jedem EU-Mitgliedstaat, vgl. Art. 288 Abs. 2 AEUV.

Der **Data Act** beinhaltet keine Pflicht bestimmte Daten zu veröffentlichen. Er enthält u. A. Regelungen, die Anreize setzen um das Teilen von Daten durch sog. Data Sharing Agreements, zu vereinfachen. Er stellt klar, wer aus welchen Daten Wert schöpfen darf, und soll eine gerechte Verteilung des Datenwertes ermöglichen, indem klare und faire Bedingungen für den Zugriff und die Nutzung der Daten innerhalb des „Europäischen Binnenmarktes für Daten" festgelegt werden.[179]

Das Ziel des **Data Governance Act**s ist es, die Entwicklung vertrauenswürdiger Datenaustauschsysteme durch vier Maßnahmenpakete voranzutreiben. In dem Text sind Mechanismen vorgesehen, die die Weiterverwendung bestimmter Daten des öffentlichen Sektors, die nicht als öffentliche Daten zur Verfügung gestellt werden können (wodurch die Open Data Richtlinie nicht anwendbar ist), verbessern sollen. Weiterhin sind Regelungen zu sog. Datenintermediären als vertrauenswürdige Organisatoren für Datenaustausch oder Bündelung von Daten enthalten. Bürger:innen und Unternehmer:innen soll es erleichtert werden, ihre Daten zum Wohle der Gesellschaft zur Verfügung zu stellen. Weiterhin sind Maßnahmen enthalten, die den Austausch von Daten erleichtern, insbesondere um eine sektor- und grenzübergreifende Nutzung von Daten zu ermöglichen. Auch der Data Governance Act enthält damit keine Bereitstellungspflichten.[180] Er regelt das „Wie" der Datenbereitstellung, wenn eine Behörde Informationen herausgibt. Andere Gesetze müssen aber die Bereitstellungpflicht als solche regeln.

Aus dem Data Act und dem Data Governance Act folgen somit keine Bereitstellungspflichten. Allerdings können insbesondere aus dem Data Governance Act Regelungen folgen, wie und in welcher Form die Behörde manche Informationen bereitstellen muss (z.B. Format, Inhalt, Interoperabilität etc.).

5.2.5 Aus sonstigen Gesetzen

Das Bundesdatenschutzgesetz (BDSG) sieht in § 25 BDSG Voraussetzungen für die Datenvermittlung von personenbezogenen Daten von öffentlichen Stellen an andere öffentliche Stellen (Abs. 1) und nicht öffentliche Stellen (Abs. 2) vor. Während diese, die personenbezogenen Daten schützenden Regelungen, zwingend eingehalten werden müssen, enthalten sie allerdings keine Pflicht zur Übermittlung von (Mobilitäts-)Daten. Auch aus dem BDSG ergeben sich somit für den (staatlichen) Betreiber der UDM keine Pflichten zur Datenweitergabe.

---

[179] Vgl. Europäische Datenstrategie: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de#:~:text=Die%20Europäische%20Datenstrategie%20soll%20die,Unternehmen%2C%20Forschenden%20und%20öffentlichen%20Verwaltungen.&text=This%20is%20a%20modal%20window., zuletzt aufgerufen am 31. Juli 2024.

[180] Vgl. *Schemmel* in Wolff/Brink/v.Ungern-Sternberg, BeckOK DatenschutzR, Art. 5 DGA, Rn. 40.

5.3 Ausblicke: Die UDM als Teil der digitalen Infrastruktur? Google Maps vs. Kommunale Lösungen

Der Aufbau und Betrieb einer UDM gehört nicht zur öffentlichen Daseinsvorsorge. Damit besteht keine Pflicht für Kommunen die UDM als Teil der digitalen Infrastruktur aufzubauen. Die UDM kann allerdings einen Beitrag dazu leisten, die Verkehrsplanung der Kommunen zu optimieren. Große private Navigationsdienste stören zunehmend die kommunale Verkehrsplanung. Durch eine öffentliche Alternative kann die Kommune ihre Planungshoheit durchsetzen. Die geplante Reform des Straßenverkehrsgesetzes hätte die Rolle der Kommunen in der Verkehrsplanung noch weiter gestärkt, ist aber (vorerst) gescheitert.

5.3.1 Gehört der Betrieb einer UDM zur öffentlich-rechtlichen Daseinsvorsorge?

In diesem Teil (Kapitel 5) wurden bisher Themen untersucht, die sich mit der Frage beschäftigen, welche Voraussetzungen eingehalten werden müssen, wenn eine UDM durch die öffentliche Hand (z.B. durch eine Stadt oder Kommune) betrieben wird und welche Konsequenzen ein solcher Betrieb hätte. In dem folgenden Ausblick wird der Gedanke untersucht, ob (ungeachtet der Hindernisse) die staatlichen Institutionen verpflichtet sind, eine UDM als Teil der digitalen Infrastruktur/öffentlichen Daseinsvorsorge aufzubauen und zu betreiben.

Wenn der Aufbau und Betrieb einer UDM, Teil der öffentlichen (digitalen) Daseinsvorsorge wäre, dann hätten Kommunen allgemein die Pflicht eine solche UDM einzurichten und zu betreiben. So könnte der Übernahme der verkehrsrechtlichen Planungshoheit von Städten und Kommunen durch große Unternehmen entgegengewirkt werden. Die Hoheit über digitale Infrastrukturen würde dann von den Städten und Kommunen zurückerlangt werden.

Die **öffentlich-rechtliche Daseinsvorsorge** umfasst alle Infrastrukturleistungen, die die Bürgerinnen und Bürger zur freien Entfaltung ihrer Persönlichkeit benötigen und die den sozialen Zusammenhalt in einer Gesellschaft durch die Produktion öffentlicher Güter gewährleisten. Zu diesen Infrastrukturen zählen zum Beispiel Bildung, Energie, Gesundheit, Wasser und Verkehr.[181] Umstritten ist, ob und inwieweit zur Grundversorgung der Gesellschaft auch Informations- und Kommunikationstechnologien sowie die dazu nötigen Infrastrukturen gehören. Sowohl der Zugang zum Internet als auch ein Mindestangebot an Bandbreite könnte über § 78 Abs. 2 Telekommunikationsgesetz[182] als Teil der „e-Daseinsvorsorge“ angesehen werden. Ein Recht auf Internet dürfte es allerdings (noch) nicht geben.[183]

Dafür, dass auch der Betrieb einer UDM unter die öffentliche Daseinsvorsorge fällt, spricht, dass die Aufgabe der **Verkehrsplanung bei den Kommunen** liegt. Allerdings werden immer mehr größere Navigationsdienste, wie z.B. Google Maps, genutzt. Diese können in die Planung der Kommunen eingreifen. Wenn z.B. eine Kommune eine Straße wegen Straßenarbeiten sperrt, wird diese auch eine Umleitung empfehlen, die den Verkehrsplänen der Kommune entspricht. In diesen Plänen ist die Kommune unter anderem zum (Lärm-) Immissionsschutz verpflichtet. Sie wird daher eher die eventuell

[181] *Kersten* in Görres-Gesellschaft Staatslexikon, Stichwort „Daseinsvorsorge“, Rn. 1.

[182] Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 5 des Gesetzes vom 14. März 2023 (BGBl. 2023 I Nr. 71) geändert worden ist.

[183] *Wernicke* in Grabitz/Hilf/Nettesheim, Das Recht der EU, Art. 106 Rn. 127.

längere Umleitung durch die Stadt empfehlen als die kürzere Umleitung durch das verkehrsberuhigte Wohngebiet. Durch Verkehrsnavigationsdienste besteht die Gefahr, dass viele Verkehrsteilnehmende die kürzere Route durch das Wohngebiet wählen. Ohne eigenes Navigationssystem gibt die Kommune Verkehrsplanungsoptionen aus der Hand. Damit kommt sie eventuell dem Schutz einiger Bewohner:innen nicht mehr nach (z.B. durch vernachlässigten Immissionsschutz).

Nicht nur Privatpersonen setzen vermehrt auf solche Navigationsdienstleister, sondern auch große Unternehmen. So hat Mercedes angekündigt, dass seine Flotte künftig mit Hilfe von Google Maps navigiert werden soll. Bei der Kooperation soll es sich um eine langfristige strategische Partnerschaft handeln, wobei das erste Google-basierte Betriebssystem 2025 auf den Markt gehen soll.[184] Dies zeigt, dass wenn staatliche Akteure nicht selbst Navigationskarten zur Verfügung stellen, auch größere Unternehmen sich gezwungen sehen, mit Navigationsdiensten zu operieren, die immer wieder wegen Datenschutzverstößen in der Kritik stehen[185]. Dem würde der Betrieb einer UDM durch eine staatliche Stelle vorbeugen.

Gegen eine solche Pflicht, eine UDM zu betreiben, sprechen allerdings pragmatische und verfassungsrechtliche Gesichtspunkte. Alle oben genannten **Haftungsfragen**, die sich Betreiber:innen stellen müssen, können zwar vertragsrechtlich zwischen Betreiber:innen und Nutzer:innen der UDM geregelt werden. Allerdings würde der staatliche Betreiber damit, wie in Kapitel 3.2.43.2.2. skizziert, ein unüberschaubares Haftungsrisiko übernehmen. Dem könnte zwar entgegengehalten werden, dass ein staatlicher Betreiber sich aufkommenden Haftungsfragen stellen muss. Es scheint aus einer schutzrechtlichen Perspektive nicht erstrebenswert, dass es Ziel der öffentlichen Hand ist, so wenig wie möglich zu haften. Wie § 6 Abs. 1 Straßenverkehrsgesetz (StVG)[186] vorgibt, sind die obersten Ziele der Verkehrsplanung die Sicherheit und Leichtigkeit des Verkehrs, nicht die Haftungsvermeidung. Die lang erwartete Novelle des StVG, in dem auch Klima- und Umweltaspekte stärker berücksichtigt werden sollten, hing zunächst zusammen mit anderen Reformen fest und scheiterte schließlich (vorerst).[187] Die Arbeitsgruppe Verkehr der regierungstragenden SPD-Bundestagsfraktion bekräftigte noch in einem Positionspapier vom 09. Mai 2023, dass sie das StVG so anpassen würden, dass „*neben der Flüssigkeit und Leichtigkeit des Verkehrs die Ziele des Klima- und Umweltschutzes, der Gesundheit und der städtebaulichen Entwicklung berücksichtigt werden, um Kommunen Entscheidungsspielräume zu eröffnen.*“[188] Das Papier sah weiterhin vor, dass ein Antragsrecht von Kommunen für Verkehrsmaßnahmen verankert werden soll, welche von den Straßenverkehrsbehörden verpflichtend entschieden werden

---

[184] *Mortsiefer* in Tagesspiegel Background vom 23. März 2023: „Auto-Software: Mercedes navigiert mit Google“.

[185] Vgl. Datenschutz.org „Google und der Datenschutz: eine moderne Kontroverse“, https://www.datenschutz.org/google-datenschutz/#:~:text=Seit%20Jahren%20steht%20Google%20in,Gewinnzwecken%20auch%20an%20Dritte%20verkauft (zuletzt aufgerufen am 31. Juli 2024); LTO: „Französische Datenschützer verhängen Bußgeld gegen Google – Die Datenschutzdiskussion ist eröffnet“, https://www.lto.de/recht/kanzleien-unternehmen/k/datenschutz-DS-GVO-verstoss-frankreich-google-bussgeld-zustaendigkeit-namentliche-nennung/ (zuletzt aufgerufen am 31. Juli 2024).

[186] Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch Artikel 16 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert wo

[187] Vgl. *JMA,* Städteinitiative enttäuscht nach Wissing-Treffen, Tagesspiegel-Background vom 06. Juni 2023.

[188] Positionspapier der Arbeitsgruppe der SPD-Bundestagsfraktion zur Modernisierung des Straßenverkehrsgesetzes (StVG): „Mehr Rechte für Kommunen, mehr Sicherheit für alle“, 09. Mai 2023, S. 1 (Mehr Entscheidungsspielraum für Straßenverkehrsbehörden).

müssen. Nur so könnten dann Kommunen ihrem rechtlichen Auftrag aus Art. 28 Abs. 2 GG künftig auch bei der Regelung des Verkehrs nachkommen.[189]

Allerdings scheiterte die StVG-Novelle (vorerst) im Bundesrat.[190] Die vorgeschlagenen Änderungen hätten durchaus die Rolle der UDM als Werkzeug für die kommunale Planungshoheit stärken können. Wenn die vorgeschlagenen Änderungen in das StVG implementiert würden, ließe sich zumindest argumentieren, dass der Aufbau und Betrieb einer UDM in erheblichem Maße zum Klima- und Umweltschutz beitragen kann. Unter diesen Gesichtspunkten ist der Betrieb einer UDM empfehlenswert und sollte von den Kommunen angestrebt werden. Damit kann ein regulierter Rechtsrahmen für die Verkehrsplanung entwickelt werden, sodass Kommunen auch weiterhin ihren schutz- und verkehrsplanungsrechtlichen Aufgaben nachkommen können. Die Steuerung von Verkehrsströmen liegt im öffentlichen Interesse, vor allem im Hinblick auf die Verkehrssicherheit und den Umweltschutz.[191] Zwar können sich aus intensivem Nutzungsverhalten auch problematische Situationen ergeben (sollten z.B. nachhaltige Verkehrsstörungen dazu führen, dass viele Nutzer von Navigationsdiensten die Autobahn vorzeitig verlassen, dann kommt es im nachgeordneten Streckennetz oft zu gravierenden Störungen).[192] Durch die UDM können Städte und Kommunen aber das Fahrverhalten der Verkehrsteilnehmenden digital und in Echtzeit beeinflussen. Dadurch können auch die Sekundärauswirkungen einer Störung besser bewältigt werden. Die Städte und Kommunen können Ziele wie Verkehrssicherheit, Umweltschutz und Immissionsschutz besser einhalten.

Auch nach der Ablehnung im Bundesrat ist es jedoch wahrscheinlicher, wie schon die Open-Source Anwendung Stadt-Navi zeigt, dass zwar auf kommunale, jedoch unverbindlichere Instrumente gesetzt wird. Ob diese den großen Navigationsdienstleistungen, wie z.B. Google Maps, Konkurrenz machen können, bleibt abzuwarten. Dafür müssen die entsprechenden kommunalen Lösungen nicht nur mit einem höheren Datenschutzniveau überzeugen, sondern auch mit Services, die nur in den kommunalen Anwendungen zu finden sind. Stadt-Navi versucht dies mit einigen Live-Funktionen wie zum Beispiel der Anzeige von freien Parkplätzen, Buspositionen und Auslastung des ÖPNV oder der Möglichkeit Mitfahrangebote zu schalten.[193] Um die UDM noch attraktiver zu machen, könnten **freie Parkplätze** nicht nur angezeigt werden, sondern direkt über die UDM „**versteigert**“ werden. Dadurch wird zwar der freie Gemeingebrauch von öffentlichen Parkplätzen in Frage gestellt, rechtlich gesehen wird dieser jedoch nicht beschränkt. Das Versteigern von öffentlichen Parkplätzen ist weder sanktionierbar noch unter zivilrechtlichen Gesichtspunkten bedenklich.[194] Durch die zusätzlichen Einnahmen durch die Versteigerung wäre eine UDM zudem besser finanzierbar. Somit hätte die UDM einen signifikanten Vorteil gegenüber anderen Anbietern, wie Google Maps. Diese Faktoren müssen auch bei dem Aufbau, Betrieb und der Weiterentwicklung einer UDM berücksichtigt werden, damit die UDM tatsächlich von einer Vielzahl von Verkehrsteilnehmenden genutzt wird.

---

[189] Positionspapier der Arbeitsgruppe der SPD -Bundestagsfraktion zur Modernisierung des Straßenverkehrsgesetzes (StVG): „Mehr Rechte für Kommunen, mehr Sicherheit für alle“, 09. Mai 2023, S. 1. (Mehr Rechte für Kommunen).

[190] BRat Drucksache 548/23, Beschluss des Bundesrates bzgl. des Zehnten Gesetzes zur Änderung des Straßenverkehrsgesetzes vom 24. November 2023.

[191] *Jochum*, Verkehrsdaten für Intelligente Verkehrssysteme Rechtsrahmen und (noch) offene Fragen, ZD 2020, 497 (501).

[192] VGl. IVS-Aktionsplan „Straße“ – Koordinierte Weiterentwicklung bestehender und beschleunigte Einführung neuer Intelligenter Verkehrssysteme in Deutschland bis 2020, https://bmdv.bund.de/SharedDocs/DE/Anlage/DG/ivs-aktionsplan-strasse-broschuere.pdf?__blob=publicationFile (zuletzt aufgerufen am 31. Juli 2024), S. 16.

[193] Vgl.: https://stadtnavi.de (zuletzt aufgerufen am 31. Juli 2024).

[194] *Hartwig*, Parkplatzversteigerung via App: der Verkauf öffentlichen Parkraums durch Private, IR Energie, Verkehr, Abfall, Wasser 4/2016, 74 (77).

5.4 Wofür kann die UDM verlässlich genutzt werden?

Mangels Verbindlichkeit der Daten der UDM kann die UDM nicht zur alleinigen Navigation von autonomen und automatisierten Fahrzeugen genutzt werden. Allerdings ist die UDM für verwaltungsinterne Anwendungen und zur Unterstützung des Verkehrsmanagements einsetzbar. Eine vollautomatisierte Verwaltungsvollstreckung ist dabei nicht zulässig, wohl aber die IT-basierte Unterstützung von Verwaltungsentscheidungen („IT-Legal-Enforcement-Support").

Aus rechtlicher Sicht kann die UDM nicht zum ausschließlichen Navigieren von autonomen Fahrzeugen dienen, da die eingespeisten Daten (im Moment) nicht verlässlich genug sind. Wie bereits in Abschnitt 5.3.1 dargestellt, können überzeugende kommunale Navigationsdienste, eine Alternative zu großen gewinnorientierten Lösungen liefern und so gleichzeitig die Hoheit über die kommunale und städtische Verkehrsplanung und -steuerung zurückgewinnen. Die Daten können an anderer Stelle für das Gemeinwesen, insbesondere in Planungsfragen, genutzt werden.

Eine **vollautomatisierte Vollstreckung von Verwaltungszwang ist nicht möglich**. Das Bundesverfassungsgericht entschied kürzlich, dass schon die automatisierte Datenanalyse und -auswertung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) darstellt und daher nur unter engen Voraussetzungen, wie zum Beispiel zum Schutz besonders wichtiger Rechtsgüter möglich ist.[195] Unter diesem Gesichtspunkt scheint erst recht die automatisierte Vollstreckung und Anzeige von Ordnungswidrigkeiten unzulässig.

Allerdings können die Daten zur **Unterstützung der Verwaltung** genutzt werden (**„IT-Legal-Enforcement-Support"**). Die UDM könnte so z.B. darstellen, wann in einem bestimmten mit einem Park- oder Halteverbot belegten Straßenabschnitt, vermehrt Fahrzeuge für einen längeren Zeitraum angezeigt werden. So kann zwar anhand der Datenlage keine von Künstlicher Intelligenz (KI) generierte vollautomatisierte Entscheidung getroffen werden. Allerdings können aus den in der UDM aggregierten Daten, Hinweise erstellt werden, an welchem Ort in der Kommune oder der Stadt es sich lohnt, Polizei-Vollzugsbeamt:innen zu positionieren.

Die Behörden können gewisse Informationen nutzen, um entsprechende Maßnahmen zu ergreifen. Wenn zum Beispiel an einem bestimmten Abschnitt gehäuft Unfälle erfolgen, könnte die Höchstgeschwindigkeit behördenseitig angepasst werden bzw. anderweitige Sicherheitsmaßnahmen umgesetzt werden. Wenn die Fahrzeugsensorik durch LiDAR oder durch ein Rütteln an einer bestimmten Stelle Schlaglöcher meldet, kann die Strecke mit dem dringendsten Ausbesserungsbedarf prioritär an die entsprechende Behörde gemeldet werden. Anhand von Auffälligkeiten, Lärm, usw. können dann sog. „Fokuspunkte" erstellt werden. Das System könnte diese Punkte auf der Karte markieren. Projektintern sind noch weitere Anwendungsmöglichkeiten im Gespräch.

[195] Vgl. BVerfG, Urteil des ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1BvR 2634/20, Leitsatz 4. Das BVerfG stellte in diesem Urteil fest, dass entsprechende Passagen des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (PolDVG) und des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG), die den Einsatz einer Software zur Erkennung und Verknüpfung verschiedener Datenquellen und zur automatisierten Analyse der erfassten Daten erlaubten gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (hieraus wird das Recht auf informationelle Selbstbestimmung abgeleitet) verstoßen.

Im Moment sind die in die UDM eingespeisten Daten noch nicht verlässlich genug, damit autonome Fahrzeuge allein mit ihnen navigiert werden könnten. Dies liegt insbesondere daran, dass niemand, selbst wenn die UDM durch die öffentliche Hand betrieben wird, die Haftung für die Daten übernimmt und übernehmen will. Obwohl die Daten und die UDM in verschiedenen (Planungs-) Bereichen für öffentliche Betreiber:innen nützlich sind, besteht weiterhin ein erheblicher Forschungsbedarf zum Thema Haftung für Daten. Erst durch die Entwicklung eines überzeugenden Haftungsregimes für Daten, kann das Potential einer UDM voll ausgeschöpft werden. Als mögliche Anwendungsmöglichkeiten der UDM für autonome und automatisierte Fahrzeuge verbleiben daher z. B.:

- Ableitung von Empfehlungen für Fahrspur, Geschwindigkeit oder Abstand unter Berücksichtigung des Verkehrsgeschehens sowie der Umgebungsbedingungen wie das Wetter;
- optimiertes Routing von Fahrzeugen zur besseren Auslastung des Verkehrsnetzes;
- Verwendung tages- bis stundenaktueller Daten zu Baustellen, Staus, etc.;
- Identifikation und Kommunikation von Konfliktschwerpunkten zur Empfehlung einer vorsichtigeren Fahrweise in dem betreffenden Bereich.

6 Handlungsempfehlungen

In diesem Abschnitt werden aus den oben gefundenen Ergebnissen praktische Handlungsempfehlungen abgeleitet. Abschließende und konkrete Handlungsempfehlungen sind zu diesem Zeitpunkt nicht möglich, da es kein einheitliches Betreibermodell gibt. Handlungs- und Diskussionsbedarf wird in den Handlungsfeldern Interoperabilität von IVS, Datenherkunft, Datenverbindlichkeit, Datenmanagement, und Datennutzung identifiziert. Einige aufgeworfene Rechtsprobleme können aber nicht allein von Betreiber:innenseite gelöst werden. Entsprechend gibt es auch Möglichkeiten für den Gesetzgeber, den Aufbau und Betrieb der UDM zu fördern, die im Gutachten angesprochen wurden.

6.1 Übersicht über die Handlungsempfehlungen

In der nachfolgenden Tabelle sind in dem jeweiligen Handlungsfeld Handlungsempfehlungen an die Betreiber:innen und die Handlungsmöglichkeiten für den Gesetzgeber zusammengefasst.

Handlungsfeld	Handlungsempfehlung an die Betreiber:innen	Handlungsmöglichkeiten für den Gesetzgeber
1 Sicherheitsanforderungen an UDM (für VRU)	- Schutzmechanismen für VRU einrichten; – jederzeit bestmöglichen Schutz gewährleisten	
2 Datenverbindlichkeit und Datennutzung	- Begrenzte Nutzbarkeit wirkt sich auf Anwendungsmöglichkeiten aus und muss für die Auswahl der Einsatzmöglichkeiten beachtet werden	- Haftungsregime für die sicherheitsrelevanten Daten schaffen, um das Potential der UDM über eine verwaltungsinterne Anwendung hinaus zu etablieren; - Haftungsübernahme für gewisse Daten(Qualität) bedarf Rechtsgrundlage
3 Datenherkunft	- Selbstkontrolle ob, DSGVO beachtet werden muss und, ob die Daten rechtmäßig verarbeitet werden (siehe Kontrollfrage); - Wenn möglich, Anwendbarkeit der DSGVO umgehen; sonst Hinweispflicht etc. beachten	

4 Interoperabilität von IVS und UDM	- Spezifikationen für IVS beachten, soweit relevant; - die bereitgestellten Daten in der Mobilithek und künftig EMDS nutzen; - Pflicht zur Eigenerklärung beachten	
5 Datenmanagement/ Datenökonomie	- Datenweitergabepflichten beachten, insbesondere, wenn Betrieb der UDM durch öffentliche Hand; – Wenn stationsloser Tretrollerverleih Erlaubnis bedarf und UDM durch öffentliche Hand betrieben: Verwaltung kann Erlaubnis von Pflicht des Verleihers zur Datenweitergabe abhängig machen	- Landesgesetzgeber können Straßen- und Wegerecht so ändern, dass der stationslose Tretrollerverleih eine straßenrechtliche erlaubnisbedürftige Sondernutzung darstellt (für Hamburg: § 19 HWG oder eine entsprechende Satzung auf Grundlage des § 19 Abs. 7 HWG erlassen)

Abbildung 4: Übersicht über die Handlungsempfehlungen[196]

6.2 Handlungsfeld 1: Sicherheitsanforderungen an die UDM (für VRU)

Um einen verfassungsmäßigen Schutz von VRU zu wahren, muss nicht nur ein diskriminierungsfreier Zugang zu IVS gewährleistetet werden. Schon bei dem technischen Aufbau und der Programmierung der UDM müssen besondere Schutzmaßnahmen für VRU getroffen werden (z.B. Umfahrung von VRU-Hotspots etc.). Es müssen, auch wenn keine VRU in der Nähe detektiert werden, immer alle technischen Möglichkeiten ausgeschöpft werden, um das Navigieren mit der UDM so sicher wie möglich zu gestalten. Alarmmodi, bei denen gewisse sicherheitsrelevante Technik nur im Notfall aktiviert wird, sind nicht möglich.

6.3 Handlungsfeld 2: Datenverbindlichkeit und Datennutzung

Für Daten gibt es kein (europäisches) Haftungsregime. Für die Soft- und Hardware der UDM gilt das Produkthaftungsrecht hingegen. Daraus lässt sich aber keine Haftung für die inhaltliche Richtigkeit der Daten ableiten. Der Betreiber der UDM muss sich bewusst sein, dass Daten, für die keine Haftung übernommen wird, nicht verlässlich sind. Autonome Fahrzeuge können, Stand jetzt, nicht nur durch UDM navigiert werden. Wenn der Betreiber staatlich ist, kann das Haftungsrisiko nicht durch eine entsprechende Versicherung minimiert werden, jedenfalls nicht, solange keine entsprechende Rechtsgrundlage besteht.

[196] Eigene Darstellung des IKEM, 2024.

Die UDM kann somit nicht zur verbindlichen Navigation genutzt werden. Die Daten der UDM können nur für unverbindliche Empfehlungen bereitgestellt werden. Allerdings können diese unverbindlichen Empfehlungen der UDM zu einer Verhaltenssteuerung der UDM-Nutzenden beitragen: Je besser und präziser die Empfehlungen der UDM sind, desto mehr werden sich die Nutzenden auf die Empfehlungen verlassen. Auch wenn die Betreiber:innen der UDM nicht unmittelbar für die Daten haften, führt dies faktisch dazu, dass die Daten der UDM über ihren empfehlenden Charakter hinaus gehen. Verbraucher:innen werden sich mehr und mehr auf die UDM verlassen. Einerseits ist genau dies gewünscht, um eine gesellschaftlich akzeptierte UDM aufzubauen. Andererseits können Betreiber:innen der UDM sich ihrer faktischen Verantwortung nicht entziehen.

Die Daten der UDM können verlässlich, insbesondere von staatlichen Betreiber:innen, für andere Zwecke genutzt werden. Städte und Kommunen können mit Hilfe der UDM die Hoheit über die Verkehrsplanung zurückerlangen. Diese öffentliche Aufgabe, mit Auswirkungen auf die Verkehrssicherheit, den Immissions- und Umweltschutz, sollte nicht zur Disposition von großen privaten Navigationsdienstleistern gestellt werden. Die Verwaltung kann durch die Datensätze in Entscheidungsprozessen unterstützt werden („IT-Legal-Enforcement-Support“).

Um das Potential der UDM aber über eine verwaltungsinterne Anwendung hinaus zu etablieren, bedarf es einer Haftungsregelung für diese sicherheitsrelevanten Daten.

6.4 Handlungsfeld 3: Datenherkunft

Für den Aufbau und Betrieb sind eine Vielzahl von Mobilitätsdaten notwendig. Diese Daten müssen rechtmäßig erhoben und verarbeitet werden. In einem ersten Schritt müssen die Betreiber:innen sich fragen, ob die DS-GVO Anwendung findet. Solange es möglich ist, natürliche Personen anhand der Datensätze zu re-identifizieren (auch in Verbindung mit anderen Informationen) liegt noch Personenbezug vor. Die Daten sind dann höchstens pseudonymisiert, nicht aber anonymisiert. So handelt es sich z.B. bei Live-Standortdaten um personenbezogene Daten. Die Einwilligung der betroffenen Personen muss eingeholt werden. Die Zwecke müssen genau angegeben werden. Ein Vertragsschluss zur Miete von E-Scootern darf nicht von der Erteilung dieser Einwilligung abhängig gemacht werden.

Wenn möglich, sollte die Anwendbarkeit der DSGVO umgangen werden (sonst folgen weitere Pflichten, z.B. Hinweispflicht). Dies ist möglich durch eine automatische Anonymisierung oder die Verwendung geschlossener Systeme, beides ist aber bei der Datenverarbeitung im Rahmen der UDM wohl nicht umsetzbar.

6.5 Handlungsfeld 4: Interoperabilität von IVS und UDM

Sowohl IVS untereinander als auch die UDM als Teil eines IVS sollten mit anderen IVS interoperabel sein. Die UDM ist als digitale Karte kein IVS.

Die Intention für die europäische IVS-Richtlinie ist vor allem die innereuropäische Kompatibilität von IVS. Es soll verhindert werden, dass in den Mitgliedstaaten verschiedene IVS etabliert werden, die nicht miteinander interagieren können. Ziel der IVS-Regulierung ist es gerade nicht, Vorgaben für die Technologie von IVS und deren Entwicklung zu machen. Nichtsdestotrotz müssen diese (Mindest-) Standards für IVS bei Entwicklung und Betrieb eingehalten werden. UDM-Betreiber:innen müssen sich regelmäßig informieren, ob die EU-Kommission neue Spezifikationen erlassen hat, die auch für sie relevant sind.

Betreiber:innen können und sollten die in den Nationalen Zugangspunkten (in Deutschland die sog. „Mobilithek“) bereitgestellten Verkehrsdaten für die UDM nutzen. Auch die Nutzung des noch im Aufbau befindlichen European Mobility Data Space (EMDS) kann zum Aufbau und Betrieb der UDM beitragen. Diese Datenplattformen können von den Betreiber:innen der UDM genutzt werden, um auf eine Vielzahl von Datensätzen zuzugreifen und so die UDM zu optimieren.

Auch wenn die Hersteller:innen und Betreiber:innen der UDM nicht verpflichtet sind Daten an den NAP zu liefern, sind sie in Deutschland doch verpflichtet eine Eigenerklärung gegenüber der Nationalen Stelle für Verkehrsdaten abzugeben (nur Kontrollpflicht, keine Datenlieferpflicht). Darin müssen die Hersteller:innen der digitalen Karten u. A. die Einhaltung der Anforderungen der EU-Spezifikationen in Bezug auf Ermittlung, Zugänglichkeit, Verfügbarkeit, Austausch, Aktualisierung und Format der Daten zusichern. Abgesehen davon sind Hersteller:innen von digitalen Karten nur als Nutzer:innen von IVS in den entsprechenden Rechtsakten angesprochen, die sicherstellen sollen, dass von den Endnutzer:innen weitergegebene Daten pseudonymisiert werden und fehlerhafte Daten der zur Verfügung stellenden Stelle gemeldet werden. Eine freiwillige Bereitstellung von Daten in der „Mobilithek“ und dem EMDS ist möglich.

6.6 Handlungsfeld 5: Datenmanagement/Datenökonomie

Staatliche Betreiber:innen unterliegen gewissen Informationspflichten. Sie sind gegebenenfalls verpflichtet, Daten (anonymisiert) weiterzugeben. Dies gilt insbesondere, wenn die Betreiber:innen die Daten bereits an andere Stellen weitergegeben haben (Selbstbindung der Verwaltung aus Art. 3 Abs. 1 GG).

Staatliche Betreiber:innen einer UDM befinden sich konstant in einem Spannungsfeld zwischen (Informations-)Weitergabepflichten und der Verpflichtung sich an Datenschutz- und Cybersecurity-Regelungen zu halten. Die UDM ist keine kritische Infrastruktur. Die Betreiber:innen müssen nicht die Voraussetzungen der Cybersecurity-VO einhalten. Trotzdem ist empfohlen, mindestens „technisch-fehlerhafte“ Daten durch eine automatisierte Kontrolle vor Einspeisung in die UDM auszusortieren. Im Moment ist in Hamburg für den stationslosen E-Scooter-Verleih keine Sondernutzungserlaubnis notwendig. Der Landesgesetzgeber kann allerdings das Straßen- und Wegerecht entsprechend ändern. So kann die Erteilung der Sondernutzungserlaubnis vom Datenteilen durch den Verleiher abhängig gemacht werden, wenn die UDM durch die öffentliche Hand betrieben wird.

7 Literaturverzeichnis

Autor/Herausgeber	Werk
Auer-Reinsdorff, Astrid/**Conrad**, Isabell (Hrsg.)	Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019.
Auernhammer, Artur	DSGVO/BDSG Kommentar, 8. Auflage, 2024
Blickfeld	LiDAR-Sensoren erzeugen präzise, dreidimensionale Informationen über die Form und Oberflächeneigenschaft der umliegenden Objekte, vgl.: https://www.blickfeld.com/de/blog/was-ist-lidar/ (zuletzt aufgerufen am 31. Juli 2024).
BMDV	Artikel des BMDV vom 15. Juli 2020, „Intelligente Verkehrssysteme“, https://bmdv.bund.de/DE/Themen/Digitales/Intelligente-Verkehrssysteme/intelligente-verkehrssysteme.html (zuletzt aufgerufen am 31. Juli 2024).
BDMV	IVS-Aktionsplan „Straße“ – Koordinierte Weiterentwicklung bestehender und beschleunigte Einführung neuer Intelligenter Verkehrssysteme in Deutschland bis 2020, https://bmdv.bund.de/SharedDocs/DE/Anlage/DG/ivs-aktionsplan-strasse-bro-schuere.pdf?__blob=publicationFile (zuletzt aufgerufen am 31. Juli 2024).
Borges, Georg et. al.	Stiftung Datenschutz, Potenziale von Künstlicher Intelligenz mit Blick auf das Datenschutzrecht (Gutachten), Handreichung zum Vortrag vom 13. Dezember 2021, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Gutachten-Studien/Stiftung-Datenschutz-Wiebke-Froehlich-Handreichung-Datenschutz-und-Gleichstellung-2021-12.pdf (zuletzt aufgerufen am 14. April 2023).
Cahn, Andreas	Produkthaftung für verkörperte geistige Leistungen, NJW 1996, 2899-2905.
Car2Car Communication Consortium	Glossary, Definition of VRU, https://www.car-2-car.org/about-c-its/c-its-glossary (zuletzt aufgerufen am 31. Juli 2024).
CPM	Collective Perception Messages (CPM), vgl. https://www.etsi.org/deliver/etsi_tr/103500_103599/103562/02.01.01_60/tr_103562v020101p.pdf (zuletzt aufgerufen am 31. Juli 2024).
DGVP (Deutsche Gesellschaft für Verkehrspsychologie)	Nichtmotorisierte Verkehrsteilnehmer/Vulnerable Road Users, https://www.dgvp-verkehrspsychologie.de/unsere-arbeitsbereiche/strasse/fahrzeug-und-verkehrsraum/nichtmotorisierte-

	verkehrsteinehmer-vulnerable-road-user-vru/ (zuletzt aufgerufen am 31. Juli 2024).
Ehmann, Eugen/**Selmayr**, Martin (Hrsg.)	Datenschutz-Grundverordnung (DS-GVO) – Kommentar, 2. Auflage, München 2018.
Elektronik Kompendium	Standard für Konzepte wie die Vehicle-to-Everything- und Car-to-car-Kommunikation, vgl. https://www.elektronik-kompendium.de/sites/net/2407231.htm#:~:text=ITS%2DG5%20ist%20ein%20Standard,WLAN%2DSpezifikation%20IEEE%20802.11a (zuletzt aufgerufen am 31. Juli 2023).
Europäische Kommission	https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (zuletzt aufgerufen am 31. Juli 2024).
Europäische Kommission	Pressemitteilung der Europäischen Kommission „Fragen und Antworten: Intelligente Verkehrssysteme“ vom 14. Dezember 2021; https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_6727 (zuletzt aufgerufen am 31. Juli 2024).
Europäische Kommission	Mitteilung der EU-Kommission „Verkehrsdaten – Schaffung eines gemeinsamen europäischen Mobilitätsdatenraums“, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Verkehrsdaten-Schaffung-eines-gemeinsamen-europaischen-Mobilitatsdatenraums-Mitteilung-_de (zuletzt aufgerufen am 31. Juli 2024).
Europäische Kommission	„Erschließung des Potenzials von Mobilitätsdaten“, https://digital-strategy.ec.europa.eu/de/policies/mobility-data (zuletzt aufgerufen am 31. Juli 2024).
Ethik-Kommission des Bundesministeriums für Verkehr und digitale Infrastruktur	Automatisiertes und Vernetztes Fahren, Bericht 2017, abrufbar unter: https://bmdv.bund.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt aufgerufen am 31. Juli 2024).
ETSI	ETSI Technical Report 102 863 (V1.1.1 2011-06) Intelligent Transport Systems (ITS); Vehicular Communications; basic Set of Applications; Local Dynamic Map (LDM); Rationale for guidance on standardization, Abschnitt 3.1.
Gola, Peter/**Heckmann**, Dirk (Hrsg.)	Datenschutz-Grundverordnung VO (EU) 2016/679 Bundesdatenschutzgesetz – Kommentar, 3. Auflage, München 2022.
Görres-Gesellschaft (Hrsg.)	Staatslexikon für Recht, Wirtschaft und Gesellschaft, Band 1: ABC-Waffen – Ehrenamt, 8. Auflage, Freiburg 2017.
Grabitz, Eberhard/**Hilf**, Meinhard/**Nettesheim**, Martin	Das Recht der Europäischen Union, Band I EUV/AEUV, 78. Ergänzungslieferung, München, Januar 2023.

Hamburgische Beauftragte für Datenschutz — Pressemitteilung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (Johannes Casper): „E-Scooter – Die Daten Fahren mit“ vom 13. September 2019, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2019/2019-09-13_E-Scooter.PDF (zuletzt aufgerufen am 31. Juli 2024).

Hartwig, Matthias — Parkplatzversteigerung via App: der Verkauf öffentlichen Parkraums durch Private, IR Energie, Verkehr, Abfall, Wasser 4/2016, 74-77.

Hau, Wolfgang/**Poseck**, Roman (Hrsg.) — Beck’scher Online-Kommentar BGB, 65. Edition, Stand: 01.02.2023.

Hofmann, Kai — Autonomes Fahren – kein Problem des Datenschutzes, ZD 2023, 18-22.

Jandt, Silke — Biometrische Videoüberwachung – was wäre wenn …, ZRP 2018, 16-19.

Jarass, Hans D./**Kment**, Martin (Hrsg.) — Jarass/Pieroth Grundgesetz für die Bundesrepublik Deutschland, 17. Auflage, München 2022.

JMA — Städteinitiative enttäuscht nach Wissing-Treffen, Tagesspiegel-Background vom 06. Juni 2023.

Jochum, Georg — Verkehrsdaten für Intelligente Verkehrssysteme Rechtsrahmen und (noch) offene Fragen, ZD 2020, 497-501.

Johannisbauer, Christoph — E-Scooter in deutschen Großstädten – Erlaubnispflichtige Sondernutzung oder bloßer Gemeingebrauch?, NJW 2019, 3614-3617.

Klink-Straub, Judit/**Straub**, Tobias — Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201-3206.

Knezevic, Giverny — Rechtsrahmen zum autonomen Fahren: Kommunikation zwischen fahrerlosen Fahrzeugen und straßenseitiger Infrastruktur, KlimaR 2022, 279-283.

Kühling, Jürgen — Das „Recht auf Vergessenwerden“ vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, NJW 2020, 275-280.

Kühling, Jürgen/**Buchner**, Benedikt (Hrsg.) — Datenschutz-Grundverordnung BDSG - Kommentar, 3. Auflage, München 2020.

Martini, Mario/**Haßecker**, Dietrich/**Wagner**, David — Das Datennutzungsgesetz als digitalpolitischer Ordnungsrahmen für die Monetarisierung kommunaler Daten, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 11/2022, 1-12.

Mayer, Christian A./**Bomhard**, David/**Etzkorn**, Phillip — Mobilitätsdatenverordnung (MDV) – Neuer Rechtsrahmen für die Bereitstellung von Mobilitätsdaten, Recht Digital (RDi) 2022, 446-452.

Mortsiefer, Henrik — Artikel in Tagesspiegel Background vom 23. März 2023: „Auto-Software: Mercedes navigiert mit Hilfe von Google“, https://background.tagesspiegel.de/mobilitaet/mercedes-benz-navigiert-mit-google (zahlungspflichtig, zuletzt aufgerufen am 31. Juli 2024).

Nationale Stelle für Verkehrsdaten — Auslegung der IVS-Richtlinie und der DA durch die Nationale Stelle für Verkehrsdaten, „Muss ich Daten liefern?“, https://nationalestelle-verkehr.de/nast/DE/Daten/Lieferung/Daten_node.html (zuletzt aufgerufen am 31. Juli 2024)

Oppermann, Bernd H./**Stender-Vorwachs**, Jutta (Hrsg.) — Autonomes Fahren – Rechtsprobleme, Rechtsfolgen, technische Grundlagen, 2. Auflage, München 2022.

Paal, Boris P./**Pauly**, Daniel A. — Beck’sche Kompakt-Kommentare Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage, München 2021.

Plath, Kai-Uwe — DSGVO/BDSG/TTDSG Kommentar, 4. Auflage, München 2023

Reuter, Wiebke — Umgang mit sensiblen Daten bei allgemeiner Videoüberwachung, ZD 2018, 564-569.

Roßnagel, Alexander — Pseudonymisierung personenbezogener Daten – Ein zentrales Instrument im Datenschutz nach der DS-GVO, ZD 2018, 243-247.

Schaar, Katrin — DS-GVO: Geänderte Vorgaben für die Wissenschaft – Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen?, ZD 2016, 224-226.

Schoch, Friedrich — Informationsfreiheitsgesetz Kommentar, 2. Auflage, München 2016.

Schröder, Meinhard — Datenschutz beim Kameraeinsatz im Automobil – Personenbezug von Daten bei Dashcams & Co., ZD 2021, 302-307.

Schulte, Martin/**Kloos**, Joachim — Handbuch Öffentliches Wirtschaftsrecht – Teil C Der Staat als Marktteilnehmer, 1. Auflage, München 2016.

Schulz, Thomas — Sicherheit im Straßenverkehr und autonomes Fahren, NZW 2017, 548-553.

Seufert, Julia — Datensicherheit in autonomen Fahrzeugen, ZD 2023, 256-261.

Steege, Hans — Ist die DS-GVO zeitgemäß für das autonome Fahren? Datenschutzrechtliche Aspekte der Entwicklung, Erprobung und Nutzung automatisierter und autonomer Fahrzeuge, MMR 2019, 508- 513.

Stoklas, Jonathan/**Wendt**, Kai — Das vernetzte und autonome Fahrzeug – Datenschutzrechtliche Herausforderungen, Gutachten im Rahmen des Projekts ABIDA (Assesing Big Data), 2018, abrufbar unter: https://www.repo.uni-hannover.de/bitstream/handle/123456789/5169/Vertiefungsstudie_Das%20vernetzte%20und%20smarte%20Fahrzeug_v02.pdf?sequence=1&isAllowed=y (zuletzt aufgerufen am 14. April 2023).

Sydow, Gernot/**Marsch**, Nikolaus — Datenschutz-Grundverordnung Bundesdatenschutzgesetz Handkommentar, 3. Auflage, Baden-Baden 2022.

Wolff, Heinrich Amadeus/**Brink**, Stefan/**von Ungern-Sternberg**, Antje (Hrsg.) — Beck'scher Online-Kommentar (BeckOK) Datenschutzrecht, 46. Edition, München 2023, Stand: 01.11.2023.

Xu, Fengli/**Tu**, Zhen/**Li**, Yong/**Zhang**, Pengyu/**Fu**, Xiaoming/**Jin**, Depeng — Trajectory Recovery From Ash: User Privacy is NOT Preserved in Aggregated Mobility Data, April 2017 (in the proceedings of the 26th international conference on world wide web pp. 1241-1250.

Datenschutzkonferenz (DSK) — Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, Stand Juli 2020.

Volkmann, Sebastian/**Feiten**, Linus/**Zimmermann**, Christian/**Sester**, Sebastian/**Wehle**, Laura/**Becker**, Bernd — Digitale Tarnkappe: Anonymisierung in Videoaufnahmen. Informatik 2016, 2016.