ANONYMISIERUNG FÜR VERNETZTE MOBILITÄTSSYSTEME

Leitfaden und Anwendungsfälle zur Anonymisierung in vernetzten Mobilitätssystemen

www.anymos.de

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Finanziert von der
Europäischen Union
NextGenerationEU

Vorwort

Das Kompetenzcluster ANYMOS – Anonymisierung für vernetzte Mobilitätssysteme – hat sich zum Ziel gesetzt, Anonymisierung als Schlüsseltechnologie zu etablieren. Anonymisierung kann die Rechtssicherheit beim Teilen und Nutzen von Daten erhöhen und neue Möglichkeiten für datengetriebene Innovationen eröffnen.

Diese Broschüre fasst die Erfahrungen des Kompetenzclusters ANYMOS zusammen. Sie beleuchtet die komplexen Datenverarbeitungsprozesse, die datengetriebenen Innovationen zugrunde liegen, und erläutert die aktuelle rechtliche Auslegung der Begriffe Anonymisierung und Pseudonymisierung. Der Leitfaden bietet einen strukturierten Ansatz zur praktischen Anwendung von Anonymisierung und wird durch Anwendungsbeispiele der Projektpartner ergänzt.

Oliver Denninger
Konsortialleiter ANYMOS

Inhalt

1 Das Kompetenzcluster ANYMOS

Mobilität wird zukünftig stark datenbasiert gestaltet, getrieben durch Automatisierung und die Skalierung des öffentlichen Verkehrs. Autonome Fahrzeuge benötigen Echtzeitinformationen über das Verhalten anderer Verkehrsteilnehmenden, während eine effizientere Nutzung bestehender Infrastruktur durch detaillierte Auslastungsprognosen und personalisierte Empfehlungen ermöglicht werden muss. Um Innovationen durch Wettbewerb zu fördern und gleichzeitig die Privatsphäre zu schützen, sind Techniken zur Anonymisierung und Pseudonymisierung essenziell. Insbesondere die Risiken der Identifikation und Profilbildung durch ortsbezogene Daten erfordern daher einen ganzheitlichen Ansatz.

Das Kompetenzcluster ANYMOS verfolgt diesen ganzheitlichen Ansatz mit dem Ziel, Anonymisierung als Schlüsseltechnologie zu etablieren, um Rechtssicherheit bei der Datennutzung zu gewährleisten und die Wettbewerbsfähigkeit Deutschlands in den Bereichen Automotive und öffentlicher Verkehr zu sichern. Dafür wird erforscht, wie Anonymisierungstechniken in hochgradig vernetzten Mobilitätssystem effektiv eingesetzt werden können. Im Fokus stehen dabei die Identifizierung von Informationsquellen, deren Zusammenspiel und die darin enthaltenen personenbezogenen Daten.

Als Instrument zum Abbau von Unsicherheiten hat ANYMOS einen Leitfaden für die Prüfung und Bewertung einzelner Verarbeitungsschritte von Mobilitätsdaten entwickelt, der analytische und entscheidungsrelevante Fragen für verantwortliche Datenverarbeitende aufgreift.

Darüber hinaus analysiert das Kompetenzcluster anhand konkreter Anwendungsfälle im Bereich autonomes Fahren, vernetzter

Infrastruktur und öffentlichem Verkehr, wie sich Personen direkt oder indirekt über ihre Verhaltens- und Bewegungsprofile identifizieren lassen. Die Erkenntnisse basieren auf Daten aus der anwendungsorientierten Mobilitätsforschung in der Region Karlsruhe und werden durch den Austausch mit dem Forschungsnetzwerk Anonymisierung und relevanten Akteuren weiterentwickelt.

Das ANYMOS-Konsortium wird durch das FZI Forschungszentrum Informatik koordiniert und umfasst sowohl vier Partner aus der Wissenschaft als auch vier Partner aus der Wirtschaft:

FZI

Das FZI Forschungszentrum Informatik ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. Ein Schwerpunkt am FZI ist die Mobilitätsforschung, in deren Rahmen sowohl der Aufbau des Testfelds Autonomes Fahren Baden-Württemberg (TAF-BW) als auch die Umsetzung mehrerer Projekte mit autonomen Shuttles maßgeblich mitgestaltet wurde. Darüber hinaus wurde im Projekt regiomove die Entwicklung einer benutzendenzentrierten, intermodalen Mobilitätsanwendung unterstützt. Zudem verfügt das FZI über umfassende Expertise in der Rechtsforschung zur Analyse neuer Informations- und Kommunikationstechnologie-Systeme (IKT-Systeme) und der Weiterentwicklung relevanter Vorschriften. Mit dem Kompetenzzentrum für IT-Sicherheit und bringt das FZI darüber hinaus fundiertes Wissen in den Bereichen Anonymisierung, Kryptografie und IT-Sicherheit ein.

Als führende Forschungs- und Bildungseinrichtung vereint das Karlsruher Institut für Technologie (KIT) akademische Lehre mit angewandter Großforschung. Das Institut für Informationssicherheit und Verlässlichkeit (KIT-KASTEL) widmet sich der Entwicklung sicherer Lösungen für die fortschreitende Vernetzung technischer Systeme. Im Fokus stehen dabei digitale Risiken in kritischen Infrastrukturen wie der vernetzten Mobilität. Das TRIANGEL widmet sich als TRANSFER | KULTUR | RAUM des KIT mitten in Karlsruhe der Begegnung, dem Austausch, dem gemeinsamen Lernen und entwickelt innovative Projekte an der Schnittstelle von Wissenschaft, Wirtschaft und Gesellschaft. Hierdurch bildet es einen wichtigen Ort zur Einbindung verschiedener Interessenvertretungenund der breiten Öffentlichkeit.

Das Fraunhofer IOSB bringt seine Expertise in der Bildverarbeitung beziehungsweise für maschinelles Lernen im Bereich des autonomen Fahrens sowie im Bereich des technischen Datenschutzes und der digitalen Souveränität in das Vorhaben ein. Insbesondere zur Erfassung des Fahrzeuginnenraums und zur Überwachung von Datenverarbeitungsketten existieren zahlreiche Vorarbeiten am Fraunhofer IOSB.

Das Fraunhofer ISI bringt seinen Fokus auf technische, wirtschaftliche und gesellschaftliche Innovationen in das Projekt ein. Insbesondere führt das Fraunhofer ISI seit über 15 Jahren Forschung sowohl im Bereich Mobilität als auch Privatheit und Datenschutz durch und koordiniert seit 2013 die „Plattform Privatheit“[1].

Die AVL Deutschland GmbH forscht am Standort Karlsruhe in enger Zusammenarbeit mit akademischen und industriellen Partnern an neuen Methoden und Werkzeugen für die Validierung zukünftiger Mobilitätssysteme, ANYMOS – Kompetenzcluster Anonymisierung für vernetze Mobilitätssysteme insbesondere in Umfeld des automatisierten Fahrens. Im Projekt ANYMOS bringt AVL den Anwendungsfall autonomes Fahren ein und arbeitet an der Datenwertschöpfungskette und Datennutzwertdefinition.

Der Karlsruher Verkehrsverbund (KVV) organisiert den öffentlichen Nahverkehr in der Region Karlsruhe, er ist insbesondere Vertragspartner aller Nutzer*innen öffentlicher Verkehrsmittel und somit verantwortliche Stelle im Sinne des Datenschutzes für die von Nutzer*innen erfassten personenbezogenen Daten. Für die operative Durchführung des Öffentlichen Personennahverkehrs (ÖPNV) sowie die Bereitstellung entsprechender IT-Plattformen greift der KVV auf entsprechende Verkehrsbetriebe und Dienstleistende zurück. Neben dem ÖPNV in der Region Karlsruhe ist der KVV auch Betreiber des TAF-BW.

1 Plattform Privatheit: https://www.plattform-privatheit.de

INIT ist weltweit führender Anbieter von integrierten Planungs-, Dispositions-, Telematik- und Ticketing-Lösungen für den ÖPNV. Das Produktspektrum umfasst integrierte Hardware- und Softwarekomponenten, insbesondere für die Aufgabenbereiche Planung und Disposition, Ticketing und Fahrgeldmanagement, Betriebssteuerung und Fahrgastinformation sowie Analyse und Optimierung. So ist die INIT auch für das Ticketing in regiomove verantwortlich und verarbeitet im Auftrag des KVV die personenbezogenen Daten der Fahrgäste. Anonymisierung von Mobilitätsdaten sind für die INIT-Systeme für verschiedene Kunden innerhalb und außerhalb des Geltungsbereichs der EU-DSGVO von Interesse.

Die iris-GmbH infrared & intelligent sensors ist ein international agierendes Technologieunternehmen mit Hauptsitz in Berlin, das seit über drei Jahrzehnten innovative Hard- und Softwarelösungen für den öffentlichen Verkehr entwickelt. Im Mittelpunkt stehen intelligente Sensorsysteme und Embedded-Plattformen, die eine zuverlässige Erfassung, Verarbeitung und Analyse von Daten direkt im Fahrzeug ermöglichen.

Durch die Kombination aus eigener Hardwareentwicklung, wie Videorekordern, und langjähriger Erfahrung in Machine-Learning-Algorithmen, bietet iris skalierbare Lösungen für Anwendungen im Bereich Fahrgastzählung, Videoanalyse und Flottenmanagement. Die enge Integration von KI und Edge-Computing sorgt dabei für effiziente, datensichere und ressourcenschonende Systeme, die weltweit in Bus- und Bahnsystemen im Einsatz sind.

2

Anonymisierung versus Pseudonymisierung

Abgrenzung zwischen Anonymisierung und Pseudonymisierung – Rechtswissenschaftliche Zusammenfassung

I. Rechtsdogmatische Grundlagen

Anonymisierung (ErwGr. 26 DSGVO): Daten, die sich nicht auf eine identifizierte oder identifizierbare Person beziehen[1]. Alle vernünftigerweise zur Re-Identifikation einsetzbaren Mittel müssen beseitigt sein[2]. Rechtliche Folge: Keine Anwendung der DSGVO.

Pseudonymisierung (Art. 4 Nr. 5 DSGVO): Verarbeitung personenbezogener Daten ohne Zuordnung zu einer Person ohne zusätzliche, gesondert aufbewahrte Informationen[3]. Rechtliche Folge: Verbleib als personenbezogene Daten.

1 Verordnung (EU) 2016/679 (DSGVO), ErwGr. 26
2 BfDI, Positionspapier zur Anonymisierung unter der DSGVO, 2020
3 Verordnung (EU) 2016/679 (DSGVO), Art. 4 Nr. 5

II. Aktuelle Rechtsentwicklung 2025

A. EDPB Guidelines 01/2025 (Januar 2025)

Die neuen Leitlinien des European Data Protection Boards (EDPB) zur Pseudonymisierung schaffen erstmals umfassende Klarheit[4] auf europäischer Ebene. Die zentralen Neuerungen umfassen eine Präzisierung des relativen Personenbezugs: pseudonymisierte Daten gelten beim Empfänger nicht als personenbezogen, wenn dieser keine Re-Identifikationsmittel besitzt. Sofern eine Re-Identifizierung durch zusätzliche Informationen möglich ist, bleiben pseudonymisierte Daten personenbezogene Daten. Erleichterte Berufung auf berechtigte Interessen (Art. 6 Abs. 1 lit. f DSGVO), insbesondere für wissenschaftliche Forschung für personenbezogene Daten, werden mit den Guidelines geschaffen.

B. Rechtsprechungsentwicklung

Die Entscheidung des EuG (26.04.2023) beinhaltet eine liberale Auslegung, nämlich, dass fehlende Re-Identifikationsmöglichkeiten beim Empfänger zum Wegfall des Personenbezugs[5] führen können. Der EuGH (04.09.2025, C-413/23 P EDSB / SRB) stärkt die Rechtslage weiter, dadurch, dass in seiner Entscheidung pseudonymisierte Daten bei Übermittlung an Dritte anonymisierte Daten darstellen können[6]. Die kontextabhängige Bewertung der Übermittlungsumstände wird hier zentral.

III. Behördliche Positionen

Eine wirksame Anonymisierung erfordert die Beseitigung aller direkten und indirekten Identifikatoren. Dies ist jedoch herausfordernd, da dies kontext- und einzel-

4 EDPB, Guidelines 01/2025 on Pseudonymisation, Januar 2025
5 EuG, Urteil vom 26. April 2023
6 EuGH, Urteil vom 4. September 2025 , C-413/23 P

fallbezogen zu betrachten ist und somit abstrakt-generelle Empfehlungen schwer zu treffen sind.[7]

ENISA: Technische Leitfäden zu Pseudonymisierungstechniken („Data Pseudonymisation: Advanced Techniques", „Best Practices", „Deploying Techniques")[8] ergänzen rechtliche Vorgaben um konkrete Implementierungsempfehlungen, beinhalten jedoch auch Methoden, die aus technischer Sicht als klassische Anonymisierungsmethoden bezeichnet werden.

IV. Abgrenzungskriterien

A. Re-Identifizierbarkeit als Kernkriterium

Paradigmenwechsel: Von absoluter zu relativer Betrachtung. Maßgeblich ist die konkrete Re-Identifikationsfähigkeit beim jeweiligen Datenverarbeitenden, nicht die theoretische Möglichkeit.[9]

„Vernünftigerweise einsetzbare Mittel" umfassen: Kosten-Nutzen-Abwägung, verfügbare Technologie, Zeitaufwand, Motivation zur Re-Identifikation.

B. Technische vs. rechtliche Anonymisierung

Technische Anonymisierung: Irreversible, mathematisch unmögliche Re-Identifikation. Anonymisierungsmethoden funktionieren über Parametrisierung.

Rechtliche Anonymisierung: Praktische Unmöglichkeit der Re-Identifikation unter Berücksichtigung aller vernünftigerweise verfügbaren Mittel – kontextabhängig und akteursbezogen und als „ja" oder „nein"-Entscheidung.[10]

7 BfDI, Positionspapier zur Anonymisierung unter der DSGVO, 2020
8 ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases; Pseudonymisation Techniques and Best Practices; Deploying Pseudonymisation Techniques
9 Verordnung (EU) 2016/679 (DSGVO), ErwGr. 26; EuGH, Urt. v. 4.9.2025, C-413/23 P
10 EDPB, Guidelines 01/2025 on Pseudonymisation, Januar 2025

Für Verantwortliche:

- Auftragsverarbeitung: nach EuGH 2025 genauere Prüfung bei pseudonymisierten Datenübermittlungen erforderlich
- Rechtsgrundlagen: EDPB Guidelines erleichtern Berufung auf berechtigte Interessen
- Betroffenenrechte: können bei unverhältnismäßiger Re-Identifikation entfallen
- Dokumentation: detaillierte Dokumentation der Pseudonymisierungsverfahren wird essenziell
- Bei anonymisierten Daten: auch in der Zukunft die Re-Identifikationsmöglichkeiten zu einem Datensatz prüfen

Technische Umsetzung:

- Robuste technische Schutzmaßnahmen nach ENISA-Empfehlungen
- Strikte Trennung von Daten und Zuordnungsinformationen
- Implementierung entsprechender organisatorischer Maßnahmen

V. Rechtswissenschaftliche Bewertung

Die aktuelle Entwicklung zeigt eine Dynamisierung des Datenschutzrechts: Während die EDPB Guidelines Rechtssicherheit für pseudonymisierte Verarbeitungen schaffen, verschärft die jüngste EuGH-Rechtsprechung gleichzeitig die Anforderungen. Dies führt zu einer hochkontextualisierten Rechtslage, die einzelfallabhängige Bewertungen erfordert.

Zentrale Herausforderung: Die Spannung zwischen dem Bedürfnis nach praktikablen Lösungen (EDPB Guidelines) und dem hohen Schutzniveau (EuGH-Recht-

sprechung) prägt die aktuelle Rechtslage. Die Praxis muss diese komplexen Vorgaben in rechtssichere, technisch umsetzbare Lösungen übersetzen.

Offene Rechtsfragen: Harmonisierung nationaler Interpretationen, sektorspezifische Besonderheiten und die Herausforderungen durch KI-Technologien erfordern weitere rechtliche Klärungen.

VI. Fazit

Die Abgrenzung zwischen Anonymisierung und Pseudonymisierung entwickelt sich zu einem relationalen, kontextabhängigen Konzept. Die jüngsten Entwicklungen 2025 schaffen einerseits wichtige Klarstellungen durch die EDPB Guidelines, verschärfen andererseits durch die EuGH-Rechtsprechung die Anforderungen.

Maßgeblich sind künftig die Perspektive des jeweiligen Datenverarbeiters und die konkreten Umstände der Datenverwendung. Die Rechtspraxis steht vor der Aufgabe, diese komplexen rechtlichen Vorgaben in praxistaugliche, technisch robuste Lösungen zu übersetzen. Andernfalls wird eine Nutzung von Daten auch im Mobilitätsbereich weiter herausfordernd aufgrund der fehlenden Rechtsklarheit.

Stand: September 2025

3

Wirkung von Anonymisierung auf die Wertschöpfung

Analyse von Datenwertschöpfungsketten zur Bewertung datenschutzfreundlicher Geschäftsmodelle

Mit der steigenden Verbreitung datengetriebener Geschäftsmodelle steigt auch die Verantwortung im Umgang mit personenbezogenen Informationen. Wie lassen sich wirtschaftliche Interessen mit dem Schutz der Privatsphäre vereinbaren? Anonymisierung eröffnet hier nicht nur Möglichkeiten zur Einhaltung datenschutzrechtlicher Vorgaben, sondern auch Potenziale für neue, datenschutzfreundliche Geschäftsmodelle.

Die Arbeiten zur Datenwertschöpfung in ANYMOS greifen diesen Ansatz auf und untersuchen, wie sich Datenwertschöpfungsketten durch die Integration von Anonymisierung verändern und welche Implikationen daraus für einzelne Geschäftsmodellkomponenten entstehen.

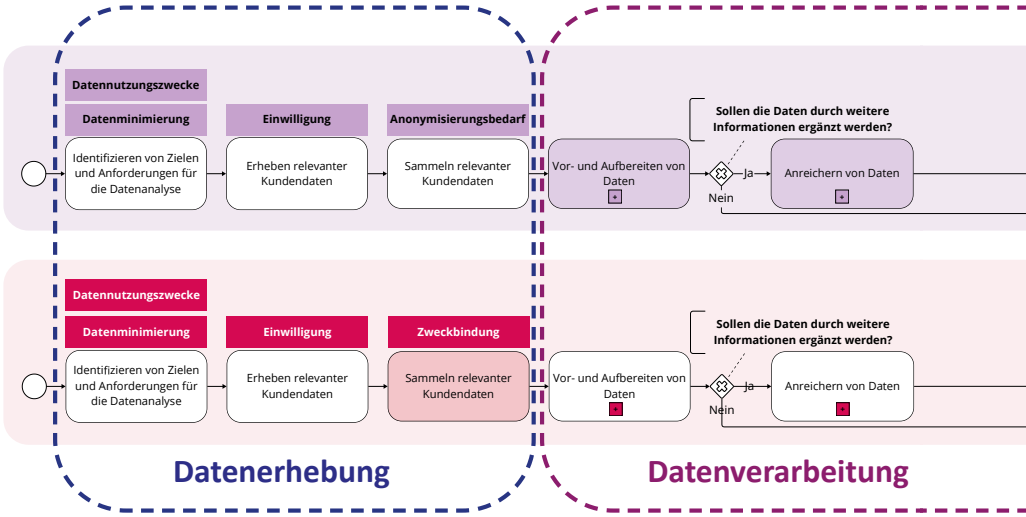
Ausgangspunkt ist eine modellhafte Prozesskette, die aufzeigt, an welchen Stellen in der Verarbeitung neue Anforderungen und Potenziale durch Anonymisierung entstehen. Mittels einer Gegenüberstellung anonymisierter und nicht-anonymisierter Datenprozesse werden Unterschiede systematisch herausgearbeitet und entlang der Dimensionen Value Creation, Value Proposition und Value Capture bewertet.

Value Creation bezeichnet alle Faktoren, die für die Werterstellung relevant sind. Hierzu gehören auch die Datenwertschöpfungs-

ketten, welche abbilden, wie die Daten fließen und verändert werden. Value Proposition bezieht sich auf das Wertversprechen, das Kundinnen und Kunden durch die datengetriebene Dienstleistung erhalten. Schließlich umfasst Value Capture alle monetären Aspekte, welche die Umsätze den Kosten gegenüberstellen.

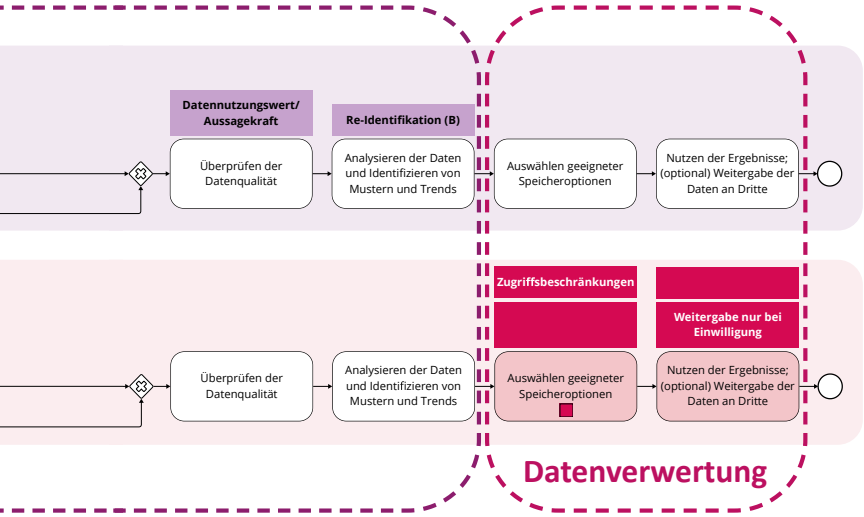
Im Ergebnis konnte anhand der Analysen aufgezeigt werden, wie sich bei Anonymisierungsverfahren, wie k-Anonymität, die Datenwertschöpfung verschiebt – weg von individualisierten, personenbezogenen Analysen hin zu aggregierten, datenschutzfreundlichen Verwertungsmodellen.

Datenwertschöpfungskette mit Anonymisierung (oberer Prozess) versus ohne Anonymisierung (unterer Prozess) nach Standard-Datenschutzmodell



Die Änderungen in der Geschäftsmodelldimension Value Creation, in der die geänderten Datenwertschöpfungsketten lokalisiert sind, haben Auswirkungen auf die zwei weiteren Komponenten. In der Dimension der Value Proposition können weiterhin individualisierte Wertversprechen angeboten werden, auch wenn bei der Anonymisierung Individualdaten aggregiert werden.

Der Gewinn an Privatsphäre muss jedoch aktiv an bestehende und neue Nutzende kommuniziert werden. In Bezug auf die Dimension der Value Capture ist die Erweiterung auf Dienstleistende denkbar, welche die



Daten gegen Entgelt nutzen könnten. Die Ergebnisse sind auf weitere datengetriebene Domänen übertragbar und unterstützen die strategische Entscheidungsfindung zwischen Datenschutz, Wertgenerierung und Monetarisierung.

Für die Analysen und Ergebnisse arbeiteten das Fraunhofer ISI und das FZI zusammen. In diesem Zusammenhang entstanden unter anderem folgende Veröffentlichungen.

Publikationen

Metzger & Krauss, Clarifying new urban mobility services based on a threefold business model framework, https://doi.org/10.1016/j.trip.2024.101207

Metzger et al., Privatheitswahrende Geschäftsmodelle: Analyse von Datenwertschöpfungsketten mithilfe des Standard-Datenschutzmodells (SDM), https://doi.org/10.24406/publica-4695

Beckert & Metzger, Collection and Use of Digital Mobility Data, Challenges in Their Anonymization, and Alternative Strategies, https://doi.org/10.24406/publica-5338

4

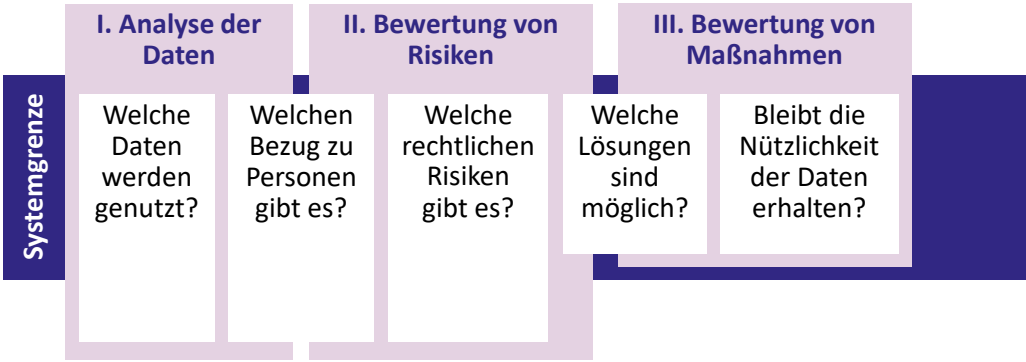
Leitfaden

Leitfaden zur Anwendung von Anonymisierung in der Praxis

*Der Leitfaden richtet sich an Verantwortliche, Entwickler*innen sowie Datenschutzfachkräfte, die in ihrer Arbeit mit der Verarbeitung personenbezogener Daten konfrontiert sind. Er bietet ein strukturiertes Vorgehen mit dem Anonymisierungs- und Pseudonymisierungstechniken gezielt eingesetzt werden können, um die Risiken für die betroffenen Personen zu minimieren und gleichzeitig die rechtlichen Vorgaben des Datenschutzes zu erfüllen.*

Aus den im Projekt ANYMOS bearbeiteten Anwendungsfällen zu Mobilitätsdaten sind zahlreiche Fragen hervorgegangen, die die Grundlage jeder Prüfung und Bewertung von Datenverarbeitungsvorgängen im Bereich der Mobilitätsanwendungen, aber auch darüber hinaus, bilden. Der Leitfaden stellt einen Rahmen für diese Fragen bereit und ermöglicht es, relevante Sachverhalte

Die fünf Phasen des Leitfadens



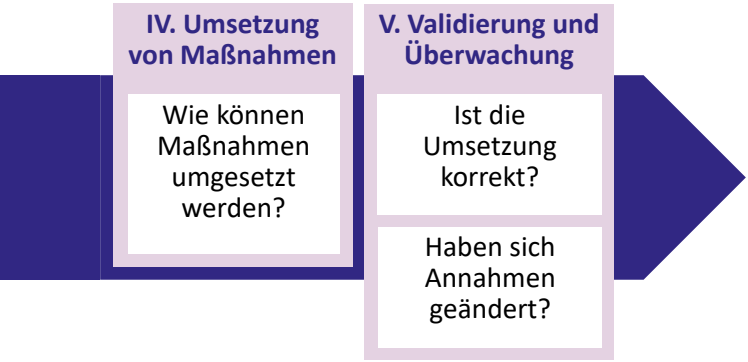
zu erfassen und auf dieser Basis fundierte Entscheidungen über geeignete technische und organisatorische Maßnahmen zu treffen.

Der Leitfaden und seine Struktur

Die fünf Phasen des Leitfadens beinhalten jeweils sowohl analytische als auch entscheidungsrelevante Aktivitäten. Zentral für den Leitfaden ist das Verständnis der Systemgrenze: Sie trennt den zu bewertenden Datenverarbeitungsvorgang samt zugehörigem technischem System von seiner Umgebung.

I. Analyse der Daten

Die Datenanalyse beinhaltet die Erfassung der zu verarbeitenden Daten und die Bestimmung des Bezugs zu Personen. Welche Datensätze werden gesammelt, gespeichert, übermittelt oder ausgewertet? Welche Datenquellen speisen das System? Welcher direkte Bezug zu Personen lässt



sich aus den Daten ableiten? Welche potenziellen Verknüpfungen mit weiteren Daten (innerhalb oder außerhalb der Systemgrenze) könnten einen indirekten Bezug zu Personen herstellen?

Ein wichtiger Aspekt ist dabei die Unterscheidung zwischen innerhalb und außerhalb der Systemgrenze liegenden Daten. Selbst wenn ein Datenverarbeitungsvorgang vollständig innerhalb der Systemgrenze abläuft, müssen mögliche Verknüpfungen mit externen Datenbeständen (Adressverzeichnisse, Mobilitätsdatenportale etc.) berücksichtigt werden. Beispielsweise haben die Geokoordinaten der Abstellpositionen von Leihfahrrädern zunächst keinen direkten Bezug zu Personen. Durch den Abgleich mit Adressdaten können sie jedoch Wohnorten zugeordnet werden und über entsprechende Verzeichnisse wiederum konkreten Personen. Solche Verknüpfungsrisiken sind bereits in der Analysephase zu erfassen, da sie die spätere Auswahl von Anonymisierungsmaßnahmen maßgeblich beeinflussen.

II. Bewertung von Risiken

Die Risikobewertung umfasst eine genauere Einordnung des während der Datenanalyse identifizierten Bezugs zu Personen und der sich daraus ergebenden rechtlichen Risiken. Für die Einordnung und Ermittlung des Risikos sollten die einschlägigen Listen von Datenkategorien mit Personenbezug genutzt werden, um diese strukturiert durchzugehen und nichts zu vergessen. Hierbei sind auch Überschneidungen mit anderen Schutzzielen der Informationssicherheit zu berücksichtigen.

III. Bewertung von Maßnahmen

Auf Basis der identifizierten Risiken werden im Rahmen der Maßnahmenbewertung technische und organisatorische Maßnahmen ausgewählt, die die Risiken mindern. Der Dreiklang aus möglichen Maßnahmen, rechtlicher Risikobetrachtung und Datennützlichkeit ermöglicht eine fundierte Entscheidungsgrundlage. Auf dieser Basis wird die empfohlene Maßnahme ausgewählt und im nächsten Schritt konkretisiert. Als

strukturiertes Vorgehen für die Bewertung von Maßnahmen empfiehlt sich die Durchführung einer Datenschutz-Folgenabschätzung.

IV. Umsetzung von Maßnahmen

Während der Maßnahmenumsetzung sollte bereits die anschließende Validierung und Überwachung mitgedacht werden. Die Umsetzung muss dokumentiert und messbar gemacht werden. Es sind Kriterien zur Validierung und zur Bewertung des Erfolgs festzulegen. Wie bei der IT-Sicherheit ist es auch für Anonymisierung und Pseudonymisierung kritisch, die korrekte Implementierung technischer Methoden zu prüfen und insbesondere für den Betrieb geeignete Parameter zu wählen. Zudem muss während des Betriebs des Systems regelmäßig geprüft werden, dass alle der ursprünglichen Bewertung zugrunde liegenden Annahmen noch zutreffen und keine Angriffe gegen die gewählten Methoden bekannt geworden sind.

Gerade die grundsätzliche Tendenz, die Datenerhebung schrittweise auszuweiten, kann jederzeit dazu führen, dass ein Bezug zu Personen entsteht, wo bis vor kurzem keiner vorlag. Die Überwachung ist ein wichtiger Schritt, um Zukunftsrisiken zu adressieren, die während der Maßnahmenbewertung noch nicht ausreichend berücksichtigt werden konnten.

V. Validierung und Überwachung

In den Phasen der Datenanalyse, der Risikobewertung und der Überwachung muss über die Systemgrenze hinaus gedacht werden, um dem Risiko der Verknüpfung von Daten und damit der Herstellung eines Bezugs zu Personen Rechnung zu tragen. Im Gegensatz dazu finden die Phasen der Maßnahmenauswahl, der Umsetzung und der Validierung innerhalb der Systemgrenze statt. Diese Unterscheidung ist wichtig, da meist nur innerhalb der Systemgrenzen Einfluss genommen werden kann.

5 Beispiele für Anonymisierung in der Praxis

Im Rahmen von ANYMOS hat IRIS in Zusammenarbeit mit dem FZI zwei zentrale Anwendungsfälle bearbeitet, die den Spagat zwischen Datenschutz und Mehrwert für Fahrgäste sowie ÖPNV-Betreibende adressieren. Ziel war es, innovative KI-basierte Lösungen zu entwickeln, die sowohl rechtliche Rahmenbedingungen einhalten als auch neue, datenbasierte Möglichkeiten eröffnen.

Pseudonymisierung von Videoüberwachungsmaterial im ÖPNV-Fahrzeug

ÖPNV-Unternehmen stehen vor der Herausforderung, Videoüberwachungsmaterial nur für 72 Stunden speichern zu dürfen. Gleichzeitig benötigen Ermittlungsbehörden oftmals längere Zeit, um Opfer oder Zeugen zu befragen und entsprechendes Beweismaterial anzufordern. Hinzu kommt,

dass in vielen Unternehmen nur eine sehr kleine Personenzahl Zugriff auf diese Daten hat.

Unser Ansatz:

- Entwicklung einer KI-basierten Echtzeit-Pseudonymisierung direkt im Fahrzeug
- Schutz besonders sensibler Bildbereiche durch moderne Verschlüsselungsverfahren
- Videos können ohne Identifizierbarkeit der Personen gesichtet werden
- Im Bedarfsfall ist eine gezielte De-Anonymisierung einzelner Betroffener möglich – unbeteiligte Personen bleiben dauerhaft unkenntlich.

Damit entsteht ein neuer Handlungsspielraum: Mehr befugte Personen können Videomaterial prüfen, ohne Datenschutzrechte zu verletzen, während Opfer und Ermittlungsbehörden schneller zu relevanten Informationen gelangen.

Anonymisiertes fahrzeugübergreifendes Tracking von Fahrgästen im Liniennetz

Bislang können ÖPNV-Betreiber nur ungenaue Vorhersagen zum Passenger Demand im gesamten Liniennetz treffen – insbesondere in komplexen, städtischen Netzen. Dies erschwert unter anderem die Planung von Schienenersatzverkehren oder die

Prognose der Auswirkungen von Verspätungen und Ausfällen.

Unser Ansatz:

- Entwicklung eines Konzepts zur KI-gestützten, datenschutzkonformen Re-Identifizierung auf Basis modernster Pseudonymisierungsverfahren
- Enge Einbindung von Datenschutzbeauftragten
- Erstellung einer Machbarkeitsstudie

Potenzial der gewonnenen Passenger-Flow-Daten:

- Analyse von kompletten Fahrgastreisen über Linien hinweg
- Erkennung hochfrequentierter Umstiegspunkte
- Eventbasierte Linienübergreifende Auslastungsprognosen (z. B. bei Großveranstaltungen)
- Datengestützte Optimierung des Liniennetzes
- Vorhersage, wie viele Passagiere tatsächlich von Verspätungen oder Ausfällen betroffen sind
- Integration von Auslastungsprognosen in MaaS-Apps (Mobility-as-a-Service)

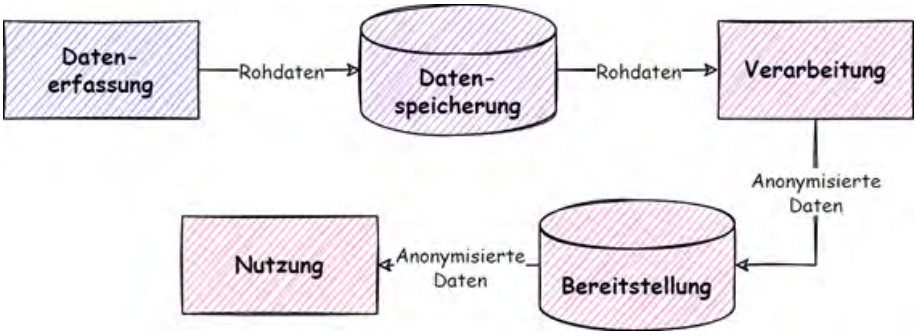
So können ÖPNV-Betreiber künftig zielgerichteter planen, auf Ereignisse reagieren und die Attraktivität ihres Angebots durch verlässliche Daten erhöhen.

Datenanonymisierung bei der Fahrzeug-Funktions-entwicklung

Messfahrzeug zur Erfassung von Referenzdaten in der Fahrzeugentwicklung

Die Partner AVL, FZI und Fraunhofer IOSB haben gemeinsam die Anforderungen an den Datenschutz im Kontext des autonomen Fahrens und der vernetzen Infrastruktur analysiert. Dabei wurden geeignete Anonymisierungsansätze erarbeitet und demonstriert.

Der dabei untersuchte Anwendungsfall umfasste alle relevanten Formen der Datenverwendung, von der Datenspeicherung zur Weiterentwicklung eigener (Fahrzeug-)Systeme, die Unterstützung der Entwicklung durch Ermöglichung des Datenaustauschs

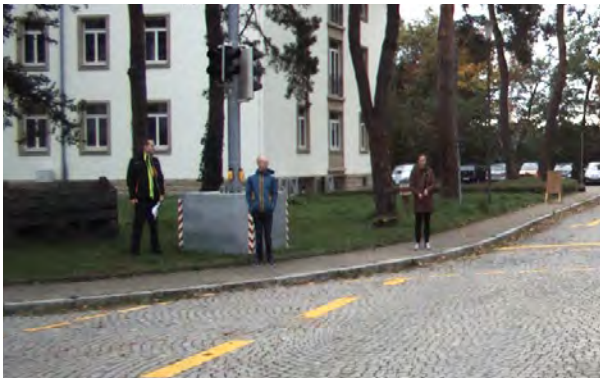


Datenfluss von der Datenerfassung bis hin zur Nutzung der Daten

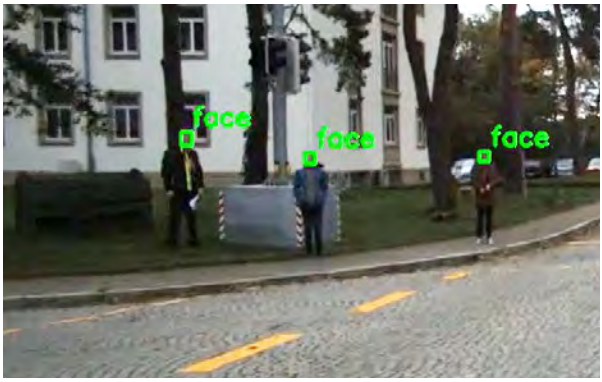
zwischen Entitäten, bis hin zur nachgelagerten Auswertung von Daten, beispielsweise bei Fehlverhalten oder Unfällen.

Für die Arbeiten im Anwendungsfall wurden Daten aus dem Förderprojekt KIsSME genutzt. Alle erkennbaren Beteiligten darin haben der Veröffentlichung der Rohdaten schriftlich zugestimmt.

Zu Beginn des Vorhabens wurde eine Übersicht über sämtliche, potenziell datenschutzrelevanten Sensor-, Verarbeitungs- und



Rohdaten



Gelabelte Daten vor der Anonymisierung

Anonymisierte Daten

Kommunikationsdaten geschaffen, wie sie bei der Entwicklung von autonomen Fahrzeugsystemen sowie beim Aufbau von intelligenter und vernetzter Infrastruktur vorkommen. Hierbei wurde explizit auch die Weiterentwicklung von Sensorsystemen – beispielsweise LiDAR und Radar mit immer feinerer Auflösung – mitberücksichtigt. Dabei wurden alle Schritte des Produktentwicklungsprozesses betrachtet, insbesondere die Datenerhebung in frühen Entwicklungsphasen zur Gewinnung von Trainingsdaten bis hin zur Validierung der Umfelderfassung für den Serieneinsatz.

Im Ergebnis konnten dabei Anonymisierungslösungen aus diesem Anwendungsfeld erarbeitet und dargestellt werden. Dies erfolgte sowohl für den Außenbereich als auch für den Innenbereich des Fahrzeugs mit den unterschiedlichen Anforderungen und Interaktionsformen, ohne sicherheitskritische Einschränkungen eingehen zu müssen.

Publikation

Gutenkunst et al., Werkzeuggetriebene Homologationsunterstützung für automatisierte Spurhalte- und künftige Fahrerassistenzsysteme, DOI:10.1007/s35658-024-1946-1

Simulation von Bewegungsdaten zum Test von Mobilitätsanwendungen

Im Rahmen des Projektes ANYMOS hat das FZI die Simulation realistischer Trajektorien basierend auf frei verfügbaren Datensätzen betrachtet und prototypisch implementiert.

Für verschiedene Anwendungsfälle – beispielsweise zum Test von Mobilitätsanwendungen – sind realistische Bewegungsverläufe nötig. Aufgrund des inhärenten Personenbezugs sind solche Datensätze allerdings nicht frei verfügbar. Durch die Simulation anhand frei verfügbarer Daten, die z. B. durch Befragungen entstanden sind, können allerdings realitätsnahe Simulationen des Bewegungsverhaltens erstellt werden. Diese Simulationen können anschließend genutzt werden, um Trajektorien zu erhalten.

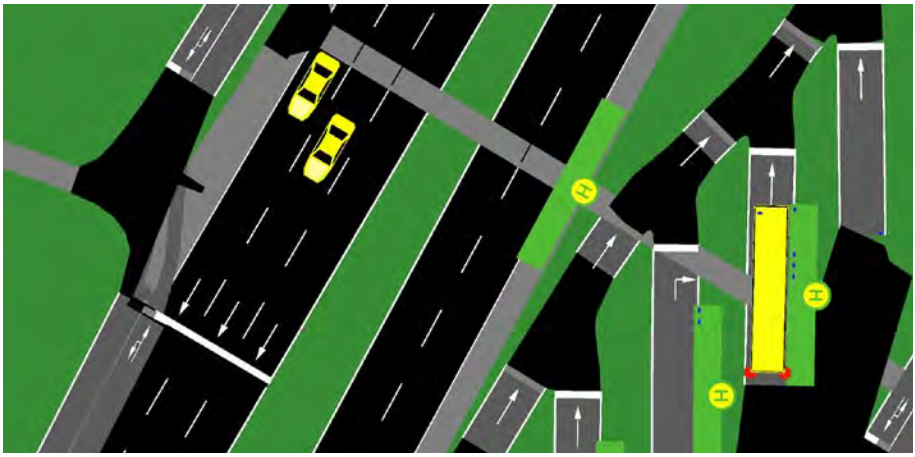


Abbildung 1: Darstellung der Simulation in der grafischen Benutzeroberfläche von SUMO

Simulation der Trajektorien in SUMO

Durch die Verwendung der Verkehrssimulation SUMO (siehe Abb.1) können, basierend auf Daten zur Verkehrsnachfrage, realistische Trajektorien inklusive damit verbundener demografischer Daten erzeugt werden.

Hierfür können eine Reihe unterschiedlicher Inputdaten verwendet werden. Von reinen Quell-Ziel-Matrizen über Ergebnisse aus Verkehrsbefragungen bis hin zu umfassenden Datensätzen aus Verkehrsnachfrage Simulationen wie mobiTopp.

Im Rahmen einer Werkzeugkette (siehe Abb.2) werden diese Inputdaten zu einer SUMO-Simulation verarbeitet, welche anschließend den Export von Trajektorien ermöglicht. Je nach verwendeten Inputdaten können diesen Trajektorien zusätzliche Attribute, wie beispielsweise das Alter der simulierten Reisenden oder deren Reisezwecke, zugeordnet werden.

Dabei erstellt SUMO aus den Start-Ziel-Koordinaten konkrete

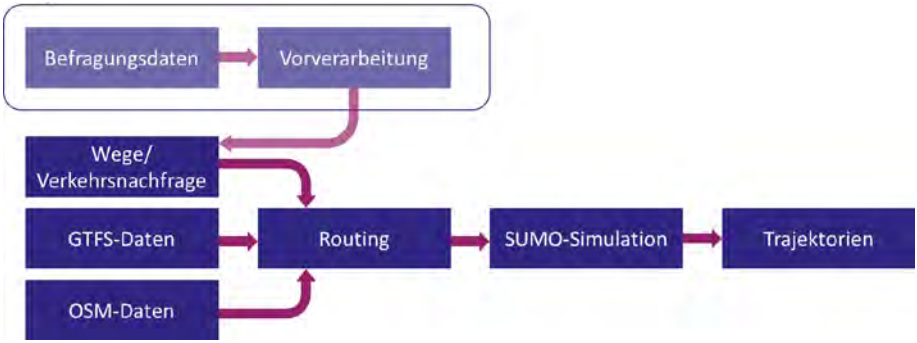


Abbildung 2: Aufbau der Wergzeugkette

Routen, welche im Simulationsdurchlauf aufgezeichnet werden. Die so erhaltenen Trajektorien können per ID wieder mit Metadaten, wie dem Reisezweck, in Verbindung gebracht werden.

Datenquellen

Um das für SUMO nötige Straßennetz zu erhalten, wird auf OpenStreetMap (OSM) zurückgegriffen.

Zusätzlich können öffentlich verfügbare Datenquellen, wie die Befragungsergebnisse „Mobilität in Deutschland“, eingespeist werden. Dieser Datensatz liefert Informationen über die Häufigkeit von Wegen abhängig von Wegzwecken, Demografie oder Verkehrsmittelwahl. Zusammen mit den OSM-Daten können dadurch eine Reihe von Wegen mit konkreten Start-Ziel-Koordinaten und Startzeitpunkt erstellt werden.

Um Fahrplan-Informationen in die Simulation von Trajektorien mit öffentlichen Transportmitteln zu integrieren, können zusätzlich Fahrpläne des öffentlichen Verkehrs in Form von GTFS-Dateien einfließen.

Als Ergebnis entsteht eine Werkzeugkette, die aus verschiedenen Inputdaten eine SUMO-Simulation und entsprechende Trajektorien erzeugen kann, welche abhängig von den verwendeten Inputdaten über zusätzliche Metadaten verfügen. Eine Evaluation der Utility dieser Trajektorien sowie eine weitergehende Parametrisierung für verschiedene Anwendungsszenarien steht noch aus.

Publikation

Kneis, Verwendung von MobiTopp als Grundlage für die Generierung von Bewegungsverläufen mit SUMO, DOI:10.18420/BTW2025-104

Multisensor-Failover-Anonymisierung

Das FZI Forschungszentrum Informatik hat im Rahmen von ANYMOS den Anwendungsfall „Multisensor-Failover-Anonymisierung“ entwickelt. Ziel ist es, eine robuste und datenschutzkonforme Verarbeitung von Sensordaten für typische Anwendungsfälle der vernetzten und autonomen Mobilität zu ermöglichen.

Für die Nutzung von Infrastruktursensorik im öffentlichen Raum ist die DSGVO-konforme Anonymisierung personenbezogener Daten eine zwingende Voraussetzung. Einzelne Sensorkanäle wie RGB-Kameras stoßen jedoch unter schwierigen Bedingungen (z. B. Nacht, Nebel, Blendung, Reflektionen) an ihre Grenzen.

Der vorgestellte Anwendungsfall kombiniert daher RGB-Kamera, Thermal-Kamera und LiDAR in einem Failover-fähigen Multisensorsystem. Fällt eine Detektionspipeline aus, können die verbleibenden Sensoren deren Aufgabe übernehmen, sodass die Anonymisierung lückenlos fortgeführt wird.

Durch die enge Verknüpfung verschiedener Sensormodalitäten entsteht das folgende technische Konzept:

1. Parallele Objektdetektion in allen Kanälen (RGB, Thermal, LiDAR) zur Erfassung relevanter Objekte wie Fußgänger*innen, Radfahrende und Fahrzeuge.

2. Extrinsische Kalibrierung zwischen den Sensoren, um Detektionsergebnisse präzise zwischen den Modalitäten zu übertragen.

3. Failover-Mechanismus: Standardmäßig erfolgt die Anonymisierung (z. B. Blurring von Gesichtern und Kennzeichen) direkt auf den RGB-Bildern.

Fällt die RGB-Detektion aus, werden Thermal- oder LiDAR-Detektionen in den RGB-Bildraum projiziert, sodass die Maskierung dennoch zuverlässig angewendet wird.

4. Kontinuierlicher Datenstrom: Die Anonymisierung wird stets im RGB-Rohbild ausgeführt, wodurch nachgelagerte Systeme einen konsistenten Datenfluss erhalten.

Der Demonstrator wurde in einer ROS-basierten Pipeline implementiert und an einem multisensorischen Testaufbau erprobt (RGB- und Thermal-Kameras sowie LiDAR an einem Sensorpfosten).

Die Tests zeigen, dass durch den Multisensor-Failover-Ansatz eine durchgängige Anonymisierung selbst unter widrigen Bedingungen möglich ist. Personen- und Fahrzeugmerkmale werden zuverlässig maskiert, auch wenn eine einzelne Detektionspipeline versagt. Damit wird die Robustheit und Ausfallsicherheit des Gesamtsystems deutlich erhöht.

Zukünftig soll das Verfahren weiterentwickelt werden, um eine dynamische Bewertung der Sensorqualität sowie eine adaptive Gewichtung der Modalitäten zu integrieren. Außerdem ist die Übertragung des Konzepts auf weitere Mobilitätsanwendungen vorgesehen, etwa zur sicheren Datennutzung an Verkehrsknotenpunkten oder in Testfeldern für automatisiertes Fahren.

Anonymisierung mittels Diffusion Modellen

In der heutigen digitalen Zeit gewinnt die Personenanonymisierung zunehmend an Bedeutung. Dies liegt vor allem daran, dass neue KI-Modelle eine enorme Menge an Trainingsdaten benötigen, um effektiv zu funktionieren. Diese Daten umfassen oft Bilder und Videos von Personen, die für die Entwicklung und Verbesserung von Bildgeneratoren und autonomen Fahrsystemen verwendet werden.

Um die Leistungsfähigkeit von KI-Modellen zu steigern, sind große und vielfältige Datensätze erforderlich. Diese Datensätze enthalten häufig personenbezogene Informationen, die geschützt werden müssen, um die Privatsphäre der Individuen zu wahren. Personenanonymisierung stellt sicher, dass die Identität der Personen in diesen Datensätzen nicht preisgegeben wird, während die Daten weiterhin für das Training von KI-Modellen genutzt werden können.

Ein Beispiel wären KI-basierte Bildgeneratoren, wie sie in der Kunst und Unterhaltung verwendet werden. Sie profitieren ebenfalls von anonymisierten Daten, da durch die Anonymisierung sichergestellt wird, dass die generierten Bilder keine erkennbaren Merkmale von realen Personen enthalten, was die Privatsphäre schützt und rechtliche Probleme vermeidet.

Ebenso sind autonome Fahrsysteme auf umfangreiche Bild- und Videodaten angewiesen, um sicher und effizient zu funktionieren. Diese Daten enthalten oft Aufnahmen von Fußgäng*innen und

Ergebnisse aus dem hier genannten Paper: Originalbilder oben und anonymisierte Bilder unten

anderen Verkehrsteilnehmenden. Personenanonymisierung hilft dabei, die Privatsphäre dieser Personen zu schützen, während die Daten weiterhin für die Entwicklung und Verbesserung der Fahrsysteme genutzt werden können.

In ANYMOS wurde ein auf Diffusion Modellen basierender Ansatz zur Anonymsierung untersucht. Dieser benutzt ein vortrainiertes Stable Diffusion Modell, um Personen in Bildern zu anonymisieren und dabei Eigenschaften, wie Hautfarbe, Haarfarbe, Kleidungsstil usw., beizubehalten. Es wurde ein Demonstrator entwickelt, um das Verfahren der Öffentlichkeit näher zu bringen. Dieser wurde in verschiedenen Wissenstransfer Formaten, wie der ANYMOS Wissenwoche, einem Stammtisch im Triangel und auf der IT-Trans Messe, gezeigt.

Publikationen

Zwick et al., Context-Aware Full Body Anonymization Using Text-to-Image Diffusion Models, DOI:2410.08551v1.

Zwick et al., LeDiFlow: Learned Distribution-guided Flow Matching to Accelerate Image Generation, DOI:10.48550/arXiv.2505.20723

Fahrzeuginnen-raumerfassung

Lokale Datenerhebung im Fahrzeuginnenraum

Das Fraunhofer IOSB erforscht im Projekt den sicheren Umgang mit Sensordaten für typische Anwendungsfälle des Autonomen Fahrens. Das erfasst unter anderem die Untersuchung der Anforderungen und Möglichkeiten zur Anonymisierung. Ebenfalls in den Fokus genommen werden die Speicherung, Weitergabe und Verwertung von Daten mit Personenbezug, welche bei der Erfassung der Insassenzustände und Situation im Fahrzeuginnenraum erforderlich sind. Gemeinsam mit Projektpartnern wurden Anwendungsfälle für das autonome Fahren mit begleitenden Risiken analysiert und grundlegende Methoden zur Aufnahme, Anonymisierung, Übertragung sowie Speicherung von Mobilitätsdaten ausgewählt und auf Bedarfe adaptiert.

Auf Basis einer vorangegangenen Analyse, die Sicherheitsanforderungen, Privacy- und Qualitätskriterien umfasste, wurde seitens des Fraunhofer IOSB ein Methodenbaukasten konzipiert, exemplarisch implementiert und validiert. Dieser ist dazu geeignet, auch anonymisierte Daten für das Training von ML-Modellen zu verwenden.

Das Lösungskonzept basiert auf vier Schichten der Datenverarbeitung im Fahrzeuginnenraum:

1. Sichere Systemarchitektur zur nachhaltigen und sparsamen Erfassung der Innenraumdaten

2. Online-Verarbeitung zur schnellen und leichtgewichtigen Anonymisierung aufgezeichneter Innenraumdaten in Echtzeit

3. Serverseitige Verarbeitung der Innenraumdaten mit rechenintensiven Anonymisierungsmethoden

4. Serverseitige Exportfunktion anonymisierter Daten mittels eines Privacy Brokers zur kontrollierten, sicheren und vertrauenswürdigen Weitergabe anonymisierter Daten an Dritte

Der Schwerpunkt bei anschließenden Tests und dem Aufbau von Demonstratoren lag auf einer sicheren und vertrauenswürdigen Fahrzeuginnenraumerfassung mit Online- & Offline-Anonymisierungsmethoden. Dabei wurde großer Wert auch darauf gelegt, eine leichte Anpassbarkeit der Lösungen auf weitere Mobilitätsanwendungen (z. B. die (Mit-)Erfassung der Fahrzeugumgebung) zu gewährleisten.

Für weitere Tests und die Validierung erarbeiteter Lösungen wurden drei Setups mit diverser Hard- und Software aufgebaut:

1. Echtzeit-Gesichtsmaskierung

Bei diesem Test wurden mobile iOS-Geräte (iPhone, iPad) mit apple VisionKit als Hardwarebeispiel mit eingeschränkter Rechenleistung eingesetzt zur Echtzeit-Anonymisierung von Videodaten mit Gesichtsmaskierung bei automatischer Regionsklassifikation.

2. Echtzeit-Videosegmentierung sowie Anonymisierung durch Gesichts-Blurring

In diesem Test wurde die Echtzeit-Anonymisierung von Videodaten durch das Blurring des Gesichtes erzielt. Hierzu wurde eine automatische Klassifikation durch das vortrainierte Model YOLO8 auf einem Laptop mit Intel-Grafik eingesetzt.

3. Echtzeit-Videosegmentierung und Klassifikation von Personen und Objekten

Für diesen Test wurde für die Klassifikation von Personen und Objekten in Videoaufnahmen das

Nvidia Jetson AGX Xavier Developer Kit genutzt zur Echtzeit-Segmentierung, Objekterkennung und fortgeschrittenen Anonymisierung der Videodaten auf Embedded Hardware. Dafür wurde das vortrainierte Model YOLO5 eingesetzt.

Mehrere Setups wurden auch benutzt, um die Übertragbarkeit und Erweiterbarkeit erarbeiteter Konzeptlösungen zu validieren. Alle Experimentalaufbauten sind im Fahrzeuginnenraum benutzbar und werden auch dort getestet.

Es ist davon auszugehen, dass die Nvidia Jetson-basierte Lösung besonders gut zum Skalieren geeignet ist, da viele moderne Server für KI auf Nvidia-Modulen basieren.

Die Sicherheit der Daten gewährleistet ein vom Fraunhofer IOSB prototypisch implementiertes TPM-basiertes Attestierungsprotokoll (TPM = Trusted Platform Module) für das in ROS2 eingesetzte Kommunikationsprotokoll DDS (Data Distribution Service).

Zukünftige Forschungen werden sich einerseits zunehmend der Erweiterung erarbeiteter Lösungen auf andere Anwendungsfälle der Mobilität widmen (z. B. Daten von Flugdrohnen, Fahrzeugumgebung). Andererseits wird an der Weiterentwicklung und Verfeinerung der Algorithmen gearbeitet, um nicht nur einen effizienteren und sichereren Schutz personenbezogener Daten in Mobilitätsanwendungen zu erreichen, sondern auch um eine gesetzeskonforme Verwendung und Verwertung (z. B. für Training von ML-Modellen) dieser Daten zu erzielen.

Digitale Mobilität mit vertraulicher Datennutzung

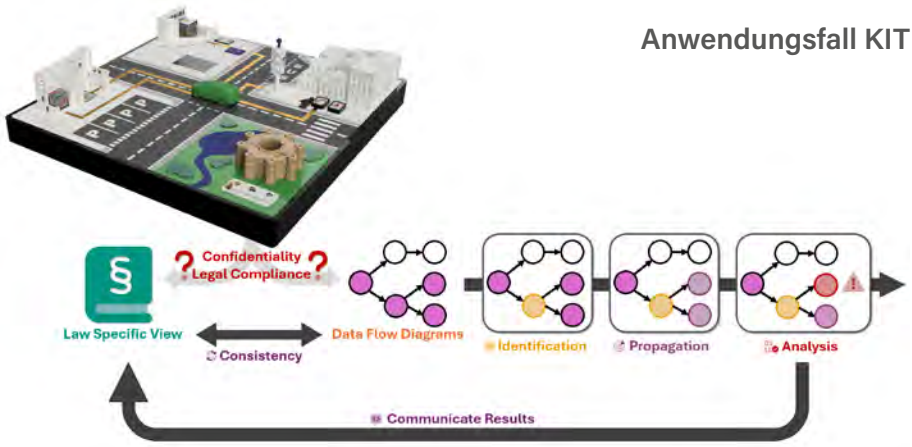
Im Projekt ANYMOS hat das Karlsruher Institut für Technologie (KIT) untersucht, wie Nutzendendaten im öffentlichen Verkehr datenschutzfreundlich verarbeitet werden können.

Im Mittelpunkt steht der Schutz der Privatsphäre der Fahrgäste. Gleichzeitig sollen Mobilitätsanbietende wichtige Informationen erhalten, zum Beispiel darüber, welche Ticketarten genutzt werden. Eine zentrale Lösung ist die sogenannte Anonymisierung durch Aggregation. Dabei werden Daten nicht einzeln erfasst, sondern direkt beim Sammeln zusammengefasst. So lassen sich statistische Aussagen treffen, ohne dass Rückschlüsse auf einzelne Personen möglich sind.

Das KIT hat ein technisches System entwickelt, das diese Aggregation direkt auf den Smartphones der Fahrgäste durchführt. Die Geräte bilden in einem Fahrzeug, etwa in einer Straßenbahn, eine temporäre Gruppe. Jeder Fahrgast gibt die eigene Ticketart ein. Die Daten werden gemeinsam aggregiert und anschließend an den Mobilitätsdienstleistenden übermittelt.

Durch moderne kryptographische Verfahren, wie verifiable secret sharing und Zero-Knowledge-Beweise, bleibt die individuelle Information jedes Fahrgasts geheim: Weder der Mobilitätsanbietende noch andere Fahrgäste erfahren, mit welcher Ticketart eine bestimmte Person unterwegs ist.

Diese Methode ermöglicht automatisierte Umfragen im öffentlichen Verkehr, ganz ohne personellen Aufwand. Dadurch können Mobilitätsanbietende häufiger und datenschutzkonform Einblicke in das Nutzungsverhalten ihrer Fahr-



System zur Erkennung und Behebung von Vertraulichkeitsverletzungen, die den Datennutzwert beinträchtigen

gäste gewinnen. Das verbessert die Planung und Optimierung des öffentlichen Verkehrs.

Zudem hat das KIT erforscht, wie vertrauliche Daten zuverlässig geschützt und gleichzeitig sinnvoll genutzt werden können. Ziel war es, Datenschutz von Beginn an in Softwarearchitekturen mitzudenken und technische Lösungen zu entwickeln, die Sicherheit und Vertrauen schaffen.

Ein wichtiges Ergebnis ist ein System (siehe Abb.), das Datenflüsse automatisch überwacht. Es erkennt mögliche Verletzungen der Vertraulichkeit und kann diese direkt beheben. So bleiben sensible Informationen auch in komplexen IT-Umgebungen geschützt. Ergänzend wurde ein interaktiver Katalog aufgebaut, in dem sich Softwarearchitekt*innen über Ungewissheiten in der Systemgestaltung austauschen können. Dadurch wächst das Bewusstsein für Risiken, die die Anonymität und Sicherheit von Daten beeinträchtigen könnten.

Darüber hinaus hat das KIT untersucht, wie sich der Wert von Daten bestimmen lässt. Die Ergebnisse zeigen klar: Vertraulichkeit und Datenwert sind untrennbar miteinander verbunden. Nur wenn Daten vertrauenswürdig verarbeitet werden, behalten sie langfristig ihren Nutzen für Forschung, Wirtschaft und Gesellschaft.

Bereitstellung von Quell-Ziel-Relationen im Öffentlichen Verkehr

Für die Qualitätssicherung und Weiterentwicklung von Angeboten im Öffentlichen Personennahverkehr möchte der KVV standortabhängige Analysen der Anfragestatistiken für Haltestellen durchführen. Gleichzeitig müssen jedoch Datensparsamkeit, „Privacy by Design" und Zweckbindung gewährleistet werden, um den Personenbezug und damit das Risiko einer Re-Identifikation so gering wie möglich zu halten. Ein einfacher, zentralisierter Ansatz mit Erfassung und Speicherung der Suchanfragen zur späteren Analyse würde zwar die funktionalen Anforderungen erfüllen, aber keine der Datenschutzanforderungen.

In Zusammenarbeit mit dem FZI wurden deshalb zwei Konzepte entwickelt, um den Datenschutz technisch bestmöglich umzusetzen, ohne jedoch bei den funktionalen Anforderungen Abstriche zu machen.

Der erste Ansatz umfasst die lokale Vorverarbeitung im Smartphone: Die Geo-Koordinaten der Suchanfrage der anfragenden Person werden in sogenannte „Zellen-Informationen" transformiert (z. B. die Voronoi-Zelle des Hauptbahnhofs). Diese Zelleninformation dient als Meta-Information für die Anfragequelle und wird zusätzlich durch einen Vektor ergänzt, der anzeigt, für welche Zielstation sich die Person interessiert. Der Vektor ist so lang, wie es Haltestellen im Stadt- und Landkreis Karlsruhe gibt, ist überall mit dem Wert 0 gefüllt und enthält an genau einer Stelle eine 1 (Index der Zielstation). Dieses Konzept adressiert bereits den Großteil

der Datenschutzanforderungen, ohne die Funktionalität der Statistiken zu beeinträchtigen.

Der zweite Ansatz beschreibt die Homomorphe Verschlüsselung. Sie soll auch das verbleibende Restrisiko einer Re-Identifikation durch den spezifischen (0,...,1,...,0)-Anfragevektor ausschließen. Dabei wird der Anfragevektor unverändert, aber verschlüsselt übertragen und aggregiert. So ist sichergestellt, dass selbst im schlimmsten Fall (z. B. durchinterne oder externe wie Malware) keine Re-Identifikation möglich ist, ohne die Korrektheit und Genauigkeit der Statistiken zu beeinträchtigen.

Beide Ansätze bieten Potenziale für Erweiterungen: Dank der breiten Einsatzmöglichkeiten homomorpher Verschlüsselung lassen sich Anwendungsfall und Architektur aus den beiden Konzepten beliebig erweitern – auch für statistische Berechnungen, die über eine einfache Aggregation hinausgehen. Auf diese Weise können zusätzliche Kennzahlen erhoben werden, während der Datenschutz sowie die volle Funktionalität jederzeit gewahrt bleiben.

Die INIT hat zusammen mit dem FZI und dem KVV ein Backend System, basierend auf Apache Airflow, bereitgestellt. Dies ermöglicht die automatisierte Abfrage von Nutzendendaten aus der KVV regiomove App sowie die homomorphe Verschlüsselung der Daten (FZI) und deren

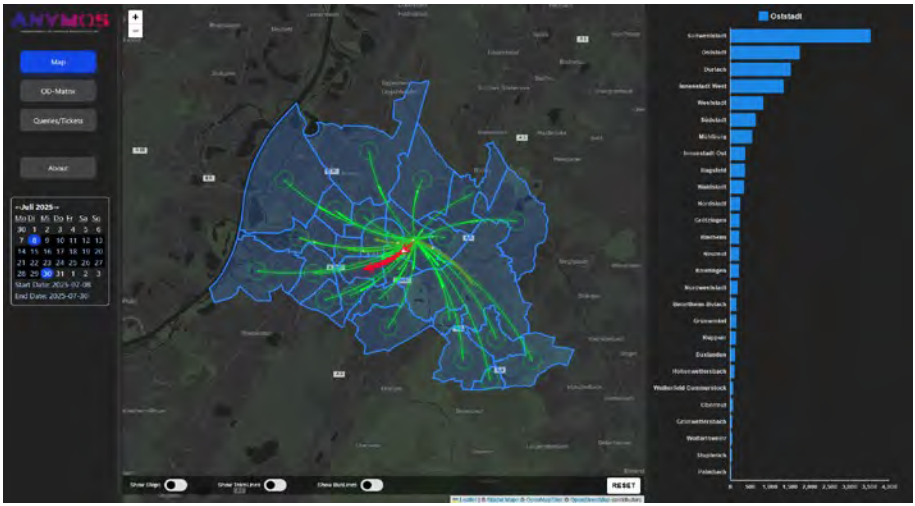


Abbildung 1: Nutzendenanfragen in Form von Quell-Ziel-Relation als Kartendarstellung

Aufbereitung. Anschließend werden die anonymisierten Daten in einer Datenbank gespeichert und nach Möglichkeit mit weiteren Daten datenschutzkonform verschnitten sowie in einem Frontend für die Nutzenden dargestellt.

Auf Basis der homomorphen Verschlüsselung ist es möglich, zusätzliche Kennzahlen zu erheben, während Datenschutz und volle Funktionalität jederzeit gewahrt bleiben. Im Anwendungsfall Öffentlicher Verkehr wurden die Nutzungsdaten aus der regiomove App aufbereitet, Fahrgastströme abgeleitet und diese in einem Dashboard visualisiert. Dies ermöglicht dem Verkehrsunternehmen, Angebote besser auf die Nachfrage abzustimmen. Durch die Anwendung der homomorphen Verschlüsselung ist es möglich, Daten weiteren Akteur*innen, wie unter anderem Verkehrsplaner*innen und externen Unternehmen, datenschutzkonform weiterzugeben (siehe Abb. 1).

Abbildung 2: O-D-Matrix der anonymisierten Quell-Ziel-Relationen

Des Weiteren ist es möglich, anonymisiert alle Quell-Ziel-Relationen zeitlich in einer sogenannten O-D-Matrix (siehe Abb. 2) abzubilden.

Darüber hinaus lässt sich die anonymisierte Bereitstellung der Daten mittels homomorpher Verschlüsselung beliebig erweitern. Zum Beispiel wurde im Anwendungsfall statistische Kennzahlen zu Ticketverkäufen ermittelt.

Publikation

Beskorovajnov et al., A Formal Treatment of Homomorphic Encryption Based Outsourced Computation in the Universal Composability Framework, https://eprint.iacr.org/2025/109

6

Wissenstransfer

Wissenschaftskommunikation – Wissenschaft erlebbar machen

Wie kann komplexe Forschung nicht nur präsentiert, sondern aktiv in die Gesellschaft eingebunden werden? Wie gelangen wissenschaftliche Erkenntnisse in die breite Öffentlichkeit? Wie fließen Impulse aus der Gesellschaft in die Wissenschaft zurück? Mit dem TRIANGEL Transfer | Kultur | Raum hat das Karlsruher Institut für Technologie (KIT) eine innovative Plattform geschaffen, die den Austausch zwischen Wissenschaft, Wirtschaft und Gesellschaft fördert. Im Herzen Karlsruhes bietet das TRIANGEL mit seinen flexiblen Räumen und interaktiven Formaten eine ideale Umgebung für kreativen Wissenstransfer und gesellschaftliche Partizipation.

ANYMOS präsentiert sich in verschiedenen Wissenstransferformaten

ANYMOS nutzt diese Struktur gezielt, um die Themen Datenschutz, Anonymisierung und Mobilität für verschiedene Zielgruppen greifbar zu machen. Mit Formaten, wie dem Stammtisch, der Mobility Café-Reihe oder dem interaktiven TRIALOG, werden wissenschaftliche Fragestellungen praxisnah diskutiert.

Veranstaltungen, wie KI:NO, ein Filmabend mit anschließender Expert*innendiskussion, oder die Wissenswoche, ein mehrtägiger Deep-Dive, machen wissenschaftliche Themen verständlich und erlebbar.

Durch die Verknüpfung mit bestehenden Initiativen wie dem Girls'Day, der Nacht der Wissenschaft oder dem Effekte Wissenschaftsfestival, wird der Wissenstransfer weiter gestärkt. Der offene Dialog im TRIANGEL ermöglicht es, Forschung mit gesellschaftlichen Perspektiven zu verbinden – ein essenzieller Schritt für eine partizipative und transparente Wissenschaft.

Technologietransfer – Forschung mit der Wirtschaft

Parallel und in Koordination zum Wissenschaftskommunikation koordinierte das FZI Forschungszentrum Informatik den Technologietransfer in ANYMOS. Die zentralen Aufgaben des Technologietransfers bestanden in der Vermittlung von Forschungsinhalten an Partnerunternehmen aus der Wirtschaft sowie dem Einholen von Feedback zu Forschungsansätzen, um diese ins Forschungsprojekt einfließen zu lassen. Dadurch können Projektergebnisse anwendungsgerecht entwickelt werden, was ihre Akzeptanz und Nutzung begünstigt.

Eine große Rolle spielte die Präsenz von ANYMOS auf diversen industrienahen Events und Messen. So wurden ANYMOS Demonstratoren auf der Hannover Messe, der IT-Trans, dem Zukunftskongress ÖPNV und der Regionalkonferenz Mobilitätswende präsentiert und mit Industrievertreter*innen diskutiert.

Zudem wurde ANYMOS auch im Netzwerk Intelligent Move vorgestellt und beim MobiData BW Barcamp im Zuge von geleiteten Barcamp Sessions demonstriert.

Abbildung 1 und 2: Eindrücke aus den Mobility Cafés mit Impulsvorträgen von Bastian Leferink von raumobil GmbH (links) und Dr. Thomas Freudenmann von EDI GmbH (rechts).

Durch den Austausch auf diversen Events konnte unter anderem festgestellt werden, dass das Thema Anonymisierung aktuell zwar ein Nischenthema ist, aber auch vereinzelt – z. B. bei Mobilitätsdienstleistenden – auf großes Interesse stößt.

Für tiefere Einblicke und einen längeren Austausch zu den Themen Mobilitätsdaten und Anonymisierung lud die Mobility Café-Reihe ein (Abb. 1 und 2). Dabei konnten sich Anwender*innen durch aktuelle Mobilitätsdaten-Anwendungsfälle aus der Praxis inspi-

Abbildung 3: ANYMOS-Demonstrator auf der Hannover-Messe 2024

rieren lassen und sich sowohl mit Speaker*innen aus Industrie und Forschung als auch untereinander austauschen und vernetzen.

Den finalen Abschluss der Technologietransferaktivitäten bildete das 1. Karlsruher Mobilitätsdatensymposium. Neben einem offenen Call für Speaker*innen wurden auch dediziert Speaker*innen und Interessenten aus Wirtschaft, Forschung und Gesellschaft eingeladen, um gemeinsam zur Verwertung von Mobilitätsdaten zu tagen.

Kontakt

Sie haben Fragen zu den vorgestellten Anwendungsfällen?
Sie möchten mit unseren Expertinnen und Experten in Kontakt treten?

Wir freuen uns über Ihre Nachricht!

Oliver Denninger
E-Mail: denninger@fzi.de
Web: www.anymos.de

Das Kompetenzcluster Anonymisierung ist ein Teil des Forschungsnetzwerks Anonymisierung:

https://www.forschungsnetzwerk-anonymisierung.de/

ANYMOS

ANONYMISIERUNG FÜR VERNETZTE MOBILITÄTSSYSTEME

Aktuelle Informationen unter:
www.anymos.de

Impressum

Herausgeber:
FZI Forschungszentrum Informatik
Haid-und-Neu-Straße 10-14
76131 Karlsruhe

Rechtsform:
Das FZI Forschungszentrum Informatik ist eine Stiftung des bürgerlichen Rechts.

Redaktion:
Oliver Denninger, Linshan Feng, Judith Junker

Grafik, Satz:
Marthe Schlösser, Sabine Schneider

Bilder:
S. 53, 56: © TRIANGEL Transfer | Kultur | Raum, Fotos: Sandra Göttisheim, Laila Tkotz
Alle andern Bilder und Grafiken © FZI Forschungszentrum Informatik und ANYMOS-Konsortium

Stand:
Oktober 2025