



ANONYMISIERUNG FÜR VERNETZTE MOBILITÄTSSYSTEME

Förderkennzeichen 16KISA091

## Teil II – Sachbericht



iris-GmbH infrared & intelligent sensors

Finanziert durch die Europäische Union – NextGenerationEU. Die geäußerten Ansichten und Meinungen sind ausschließlich die des Autors/der Autoren und spiegeln nicht unbedingt die Ansichten der Europäischen Union oder der Europäischen Kommission wieder. Weder die Europäische Union noch die Europäische Kommission können für sie verantwortlich gemacht werden.



**Finanziert von der  
Europäischen Union**  
NextGenerationEU

Gefördert durch:



Bundesministerium  
für Forschung, Technologie  
und Raumfahrt

## 1. Zielsetzung des Teilvorhabens

Die iris-GmbH infrared & intelligent sensors war im Kompetenzcluster ANYMOS als industrieller Anwendungspartner im Themenfeld „Öffentlicher Verkehr“ eingebunden. Das Unternehmen entwickelt und vertreibt weltweit Videosicherheitslösungen für den ÖPNV, bestehend aus Kamerasystemen, mobilen Rekordern sowie Softwarelösungen zur Videoauswertung und Systemintegration.

Ziel des Teilvorhabens war es, bestehende und zukünftige Videosicherheitsprodukte systematisch unter datenschutztechnischen Gesichtspunkten weiterzuentwickeln und damit einen substanziellen Beitrag zur datenschutzkonformen Nutzung videobasierter Sensordaten im öffentlichen Verkehr zu leisten. Im Mittelpunkt stand die konsequente technische Vorverlagerung des Datenschutzes im Sinne eines integrierten „Privacy-by-Design“-Ansatzes. Personenbezogene Informationen sollten nicht erst organisatorisch geschützt, sondern bereits bei ihrer Entstehung im Fahrzeug technisch abgesichert werden.

Konkret sollte eine echtzeitfähige, KI-gestützte und selektiv reversible Pseudonymisierung von Videodaten direkt im Fahrzeug realisiert werden. Ziel war es, personenbezogene Bildbereiche automatisiert zu schützen, ohne die funktionale Nutzbarkeit der Videos für sicherheitsrelevante Zwecke einzuschränken. Damit verfolgte das Unternehmen das strategische Ziel, regulatorische Anforderungen nicht lediglich zu erfüllen, sondern als Impuls für innovative Systemarchitekturen zu nutzen und sich im Marktumfeld als Anbieter datenschutzintegrierter Videosicherheitslösungen zu positionieren.

Ein zweiter Innovationspfad betraf die Konzeption datenschutzkonformer Verfahren zur Erhebung sogenannter Passenger-Flow-Daten. Videobasierte Sensordaten sollten so aufbereitet werden, dass anonymisierte Bewegungs- und Umstiegsinformationen gewonnen werden können, ohne einzelne Fahrgäste identifizierbar zu machen. Solche Daten ermöglichen Verkehrsunternehmen eine belastbare Analyse von Auslastung, Umsteigebeziehungen und Nachfrageentwicklungen und bilden eine Grundlage für eine datenbasierte Optimierung von Linienführung, Taktung und Fahrzeugeinsatz.

Das Teilvorhaben adressierte somit zwei komplementäre Zielrichtungen:

1. die technische Absicherung videobasierter Sicherheitssysteme durch integrierte Pseudonymisierung und
2. die Entwicklung datenschutzkonformer, datenbasierter Analyseverfahren zur qualitativen Verbesserung und Effizienzsteigerung öffentlicher Verkehrssysteme.

## **2. Ausgangssituation und Handlungsbedarf zu Projektbeginn**

### **2.1 Videosicherheitssysteme im ÖPNV**

#### **Technischer Status quo**

Zur Zeit basieren marktübliche Videosicherheitssysteme im ÖPNV auf rekorderzentrierten Architekturen. Mehrere Kameras im Fahrzeug übertragen ihre Videoströme an einen zentralen Rekorder, der die Daten lokal speichert. Im Ereignisfall werden die Daten durch autorisierte Mitarbeitende mithilfe spezialisierter Software gesichtet. Die Speicherdauer ist in der Regel auf 48–72 Stunden, je nach regulatorischen Vorgaben, begrenzt.

Die Videoüberwachung ist zweckgebunden zur Aufklärung sicherheitsrelevanter Vorfälle zulässig. Gleichwohl enthalten die Aufzeichnungen regelmäßig personenbezogene Daten, da Fahrgäste identifizierbar erfasst werden. Technische Schutzmechanismen, die personenbezogene Bildbereiche automatisiert absichern, sind im Marktumfeld nicht etabliert. Videodaten wurden überwiegend im Klarzustand gespeichert und verarbeitet.

#### **Datenschutzrechtliche Risiken und Einschränkungen**

Der unmittelbare Personenbezug führt zu organisatorischen Beschränkungen hinsichtlich Zugriff und Auswertung. Verzögerungen zwischen Vorfalleinschätzung und Sichtung können dazu führen, dass relevante Daten vor ihrer Sicherung überschrieben werden.

Vor dem Hintergrund steigender regulatorischer Anforderungen und zunehmender Sensibilität im Umgang mit personenbezogenen Informationen besteht daher Bedarf an einer systematischen technischen Absicherung innerhalb der Systemarchitektur selbst.

#### **Identifizierter Innovationsbedarf**

Erforderlich ist eine Lösung, die Videomaterial bereits bei Aufnahme und Speicherung schützt und zugleich eine betriebliche Nutzung ermöglicht. Ziel ist eine selektive, reversible Pseudonymisierung, bei der:

- schützenswerte Bildbereiche automatisiert unkenntlich gemacht werden,
- pseudonymisierte Videos einer erweiterten Nutzergruppe zur Erstbewertung bereitgestellt werden können,
- eine autorisierte und technisch kontrollierte Deanonymisierung einzelner Personen im Bedarfsfall möglich bleibt.

### **2.2 Datenbasierte Netzoptimierung**

#### **Stand der Fahrgastdatenerhebung**

Für die Optimierung von Liniennetzen sind belastbare Informationen zu Ein-, Um- und Aussteigeverhalten erforderlich. Diese werden bislang überwiegend durch manuelle Fahrgastbefragungen erhoben. Solche Verfahren sind kostenintensiv, punktuell und liefern nur eingeschränkt repräsentative Daten. Eine kontinuierliche, flächendeckende Analyse von Fahrgastströmen ist damit nicht realisierbar.

In diesem Konsortium wurden unterschiedliche Ansätze zur Passenger-Flow-Erhebung untersucht. Ticketbasierte Ansätze ermöglichen, bei weniger datenschutzrelevanten Bedenken, nur eine Teilabdeckung, da nicht alle Fahrgäste entsprechende Systeme nutzen. Eine kamerabasierte,

fahrzeugübergreifende Analyse, wobei datenschutzrechtlich schwieriger umzusetzen, umfasst grundsätzlich alle Fahrgäste und war zu Projektstart und ist derzeit im Markt nach unserem Kenntnisstand nicht verfügbar.

### **Datenschutzrechtliche Herausforderungen**

Fahrwege einzelner Personen stellen personenbezogene Daten dar. Wiederkehrende Bewegungsmuster können in Kombination mit weiteren Informationen eine Reidentifizierung ermöglichen. Eine datenschutzkonforme Passenger-Flow-Erhebung erfordert daher:

- eine geschützte Verarbeitung potenziell reidentifizierbarer Merkmale im Fahrzeug,
- eine verschlüsselte Übertragung fahrzeugverlassender Daten,
- zusätzliche Anonymisierungsmechanismen wie k-Anonymität,
- den Ausschluss langfristiger personenbezogener Nachverfolgung.

### 3. Durchgeführte Arbeiten und erzielte Ergebnisse

#### 3.1 Integrierte Pseudonymisierung von Videosicherheitsdaten

##### 3.1.1 Systemkonzeption

Zu Beginn wurde die bestehende Systemarchitektur analysiert, insbesondere hinsichtlich der Frage, zu welchen Zeitpunkten Videodaten das Fahrzeug verlassen. Dies ist typischerweise bei Einrichtung und Konfiguration der Systeme der Fall sowie bei sicherheitsrelevanten Vorfällen, wenn sich eine Leitstelle live auf ein Fahrzeug aufschaltet. Im regulären Betrieb werden die Videodaten lokal auf dem Rekorder gespeichert. Daraus ergab sich die zentrale Anforderung, personenbezogene Bildbereiche spätestens auf Ebene des Rekorders zu pseudonymisieren.

Ein technischer Schwerpunkt lag auf der Verarbeitung H.264-komprimierter Videoströme. Aufgrund der verlustbehafteten Kompression sind einfache bytebasierte Verfahren (bspw. XOR-Verschlüsselung) nicht geeignet, um eine robuste reversible Pseudonymisierung zu gewährleisten. In Zusammenarbeit mit dem KIT wurde daher ein kryptographisch abgesichertes Verfahren konzipiert, das selektive Bildbereiche schützt und eine autorisierte Deanonymisierung ermöglicht.

Parallel erfolgte eine konzeptionelle Abwägung zwischen zentraler und dezentraler Umsetzung. Während beim zentralen Ansatz alle Streams im Rekorder dekodiert, verarbeitet und erneut kodiert werden, erfolgt beim dezentralen Ansatz die Verarbeitung direkt auf der Kamera vor der Kompression.

Mit der neu verfügbaren Plattform Hailo15 für leistungsfähige KI-Kameras wurde die dezentrale Architektur technisch realisierbar.

##### 3.1.2 KI-basierte Detektions- und Pseudonymisierungspipeline

Zur automatisierten Identifikation schützenswerter Bildbereiche wurde eine KI-basierte Detektionspipeline entwickelt. Hierfür wurde ein projektspezifischer Datensatz mit rund 60.000 annotierten Bildern zur Kopferkennung erstellt. Auf dieser Grundlage wurden zwei etablierte Detektionsarchitekturen – CenterNet sowie YOLOv7-tiny – trainiert und systematisch evaluiert.

Beide Modelle wurden zunächst auf dem COCO-Datensatz vortrainiert und anschließend mittels Transfer Learning auf den projektspezifischen Datensatz feinjustiert. In der quantitativen Evaluation zeigte YOLOv7-tiny eine signifikant bessere Performance hinsichtlich Präzision und Inferenzgeschwindigkeit und wurde daher für die weitere Integration in den Demonstrator ausgewählt.

Im Anschluss erfolgte die Portierung der Modelle auf Embedded-Hardware. Für die eingesetzte Hailo-Plattform standen Werkzeuge zur Quantisierung und Kompilierung der Netze zur Verfügung. Auf dem Hailo8-KI-Beschleuniger wurden Echtzeitgeschwindigkeiten von etwa 50 FPS (CenterNet) beziehungsweise 60 FPS (YOLOv7-tiny) erreicht. Die Quantisierung wurde mit dem klaren Ziel vorgenommen, die Detektionsgenauigkeit möglichst hoch zu halten und insbesondere False Negatives – also nicht erkannte Personen – zu minimieren, da diese aus Datenschutzperspektive kritisch sind.

##### Technisches Verfahren der Pseudonymisierung

Nach erfolgter Detektion werden die schützenswerten Bildbereiche in einem zweistufigen Verfahren verarbeitet. Das Bild wird hierzu logisch in einen **Background** (Hintergrund mit pseudonymisierten Bereichen) und einen **Foreground** (Originaldaten der relevanten Bildausschnitte) unterteilt. (s. Abb. 1.1)

## **Background**

Im Background werden die detektierten Bildbereiche so modifiziert, dass eine Identifizierung der betroffenen Personen nicht mehr möglich ist. Die konkrete Unkenntlichmachung kann mittels geeigneter Verfahren erfolgen, die den Anforderungen an Pseudonymität genügen, beispielsweise durch Blockmittelung der Pixelwerte (typischerweise 16×16 Pixel große Blöcke). Ein entsprechendes Beispiel ist im Anhang dargestellt.

Der so erzeugte Background wird mit H.264 oder einem vergleichbaren Videokodierungsverfahren kodiert. Wesentlich ist dabei die Fähigkeit des Kodierungsstandards, synchron zu den Videobildern zusätzliche Daten in den Bitstrom einzubetten. Im Fall von H.264 werden hierzu sogenannte „User Data Unregistered SEI Messages“ verwendet.

Diese Zusatzdaten enthalten:

- die mit einem symmetrischen Blockchiffreverfahren (z. B. AES) verschlüsselten Original-Bytefolgen der relevanten Bildausschnitte,
- sowie sämtliche Metadaten, die für eine spätere Rekonstruktion und korrekte Überlagerung erforderlich sind – mit Ausnahme des geheimen Schlüssels.

## **Foreground**

Der Foreground umfasst die Originaldaten der detektierten Bildbereiche. Diese können optional vor der Verschlüsselung komprimiert werden – entweder verlustfrei oder verlustbehaftet –, um Speicherbedarf und Datenrate zu reduzieren. Die Wahl des Kompressionsverfahrens erfolgt in Abhängigkeit von den verfügbaren Systemressourcen, da höhere Kompressionsraten in der Regel zusätzliche Rechenleistung oder Hardwarebeschleunigung erfordern.

Die resultierende Bytefolge wird anschließend mittels eines symmetrischen Blockchiffreverfahrens (z. B. AES) unter Verwendung eines geheimen Schlüssels verschlüsselt und als Bestandteil der SEI-Metadaten in den Videostrom integriert.

## **Wiedergabe- und Deanonymisierungskonzept**

Auf der Wiedergabeseite kann das kodierte Video ohne Kenntnis des geheimen Schlüssels von jedem standardkonformen Player abgespielt werden. In diesem Fall wird ausschließlich der Background dargestellt, in dem die relevanten Bildbereiche pseudonymisiert sind. Zwar können die SEI-Metadaten technisch aus dem Videostrom extrahiert werden, sie sind jedoch aufgrund der kryptographischen Absicherung nicht interpretierbar. Die Pseudonymität bleibt somit gewahrt.

Ist der geheime Schlüssel autorisiert verfügbar, kann ein spezialisierter Player die verschlüsselten Foreground-Daten entschlüsseln und anhand der übertragenen Metadaten positionsgenau über das Background-Bild legen. Dadurch werden die betreffenden Bildausschnitte selektiv deanonymisiert.

Durch in den Metadaten enthaltene Tracking-IDs ist es zudem möglich, diese Überlagerung gezielt nur für ausgewählte Personen durchzuführen. Die Pseudonymität aller übrigen Bildbereiche bleibt dabei erhalten. Dies ermöglicht eine streng kontrollierte, selektive und nachvollziehbare Deanonymisierung einzelner, vorfallsrelevanter Personen.

## **RAW- versus H.264-Verarbeitung**

Ein zentraler architektonischer Aspekt betraf die Entscheidung zwischen einer Verarbeitung auf RAW-Frames und einer Verarbeitung bereits komprimierter H.264-Streams. Während der zentrale Ansatz eine Dekodierung und erneute Kodierung der Videoströme erfordert, erlaubt die dezentrale Umsetzung auf KI-fähigen Kameras eine Verarbeitung der RAW-Frames vor der Kompression. Dadurch entfallen rechenintensive Transkodierungsschritte, was die Systemeffizienz deutlich erhöht und die Skalierbarkeit bei mehreren Kamerastreams verbessert.

### **3.1.3 Architekturentwicklung und Demonstrator**

Ein erster Demonstrator wurde rekorderbasiert umgesetzt. Skalierungstests zeigten jedoch Leistungsgrenzen bei mehreren parallelen Streams. Vor diesem Hintergrund wurde die Architektur auf eine kamerabasierte Verarbeitung umgestellt.

In der dezentralen Lösung führt jede Kamera Detektion, Pseudonymisierung und Tracking lokal aus und überträgt einen bereits geschützten H.264-Stream an den Rekorder.

Pseudonymisierungsinformationen werden als verschlüsselte SEI-Messages integriert.

Ein spezieller Videoplayer ermöglicht nach Schlüsselfreigabe die temporäre Deanononymisierung einzelner Personen (s. Abb. 1.2). Die Lösung arbeitet echtzeitfähig. Die Dateigröße erhöhte sich in Tests um etwa 10 %, abhängig von der Anzahl pseudonymisierter Bereiche.

Offene Punkte betreffen ein skalierbares Key-Management sowie die weitere Steigerung der Detektionsgenauigkeit.

## **3.2 Datenschutzkonforme Passenger-Flow-Analyse**

### **3.2.1 Technisches Konzept**

Für die Erhebung von Passenger-Flow-Daten wurde ein Konzept zur temporären, nicht-biometrischen Reidentifizierung entwickelt. Basierend auf Pedestrian-Reidentification-Ansätzen werden aus Personenbildern Embeddings erzeugt, die äußerliche Merkmale repräsentieren. (s. Abb. 2)

Diese Embeddings werden im Fahrzeug mit einem Public Key homomorph verschlüsselt und an einen Matching-Server übertragen. Eine Zuordnung der Embeddings kann über die Euklidische Distanz getroffen werden, ohne dass Klartextinformationen vorliegen. Nur aggregierte Resultate werden entschlüsselt.

Zusätzlich soll k-Anonymität implementiert. Eine Reidentifizierung erfolgt nur bei ausreichender Personenanzahl, und eine langfristige Verfolgung wird durch Key-Rotation ausgeschlossen.

### **3.2.2 Machbarkeitsanalyse**

Die Systemarchitektur umfasst eine Personendetektion im Fahrzeug, die Erstellung von Embeddings sowie deren verschlüsselte Übertragung an einen Matching-Server. Dieser berechnet Ähnlichkeiten aufgrund von Distanzen zwischen Merkmalsvektoren verschiedener Personen aus unterschiedlichen Fahrzeugen, um Umsteigebeziehungen zu identifizieren.

Vorgezogene Tests mit State-of-the-Art-Modellen (SOLIDER-ReID) zeigten grundsätzlich die technische Machbarkeit der Reidentifizierung von Personen im ÖPNV-Kontext. Auf einem projektspezifisch erstellten Datensatz mit ca. 1.000 Bildern wurde eine Genauigkeit von  $meanAveragePrecision = 49\%$  erreicht, was zeigt, dass das Modell grundsätzlich für die

Reidentifikation im Kontext ÖPNV geeignet ist. Für eine produktreife Lösung wird jedoch ein deutlich höhere Genauigkeit vorausgesetzt, was einen domänenspezifischer Datensatz (ca. 30.000 Bilder) erfordert. Öffentlich verfügbare ReID-Datensätze im ÖPNV-Kontext waren zur Projektlaufzeit nicht verfügbar.

### **3.3 Zusammenfassende Bewertung**

Der dezentrale Pseudonymisierungsansatz wurde technologisch konkretisiert und zur Demonstratorreife geführt und die Echtzeitfähigkeit ist nachgewiesen.

Die Passenger-Flow-Lösung befindet sich noch im Entwicklungsstadium, weist jedoch erhebliches Marktpotenzial auf. Zusätzlich wurde in Machbarkeitsstudien gezeigt, dass ein solches System technisch und datenschutzkonform umsetzbar ist.

## **4. Notwendigkeit und Angemessenheit**

### **Pseudonymisierung von Videoüberwachungsmaterial**

In Gesprächen mit ÖPNV-Unternehmen zeigte sich, dass die gesetzlich vorgeschriebene Löschung von Videoüberwachungsmaterial nach kurzen Speicherfristen sowie die Beschränkung des Sichtungszugangs auf wenige autorisierte Personen organisatorische Herausforderungen darstellen. Eine reversible, selektive Pseudonymisierung ermöglicht es, Videodaten breiter auszuwerten, ohne die Identität von Fahrgästen offenzulegen.

Die Entwicklung dieser Lösung erforderte eine praxisnahe Forschung mit Fokus auf Echtzeitfähigkeit, Skalierbarkeit bei mehreren Kameras pro Fahrzeug und Robustheit unter realen Betriebsbedingungen. Zugleich musste die Systemarchitektur entlang der tatsächlichen Verwertungskette im ÖPNV – von der Aufzeichnung im Fahrzeug bis zur möglichen Weitergabe – konzipiert werden. Die Arbeiten waren damit technisch notwendig, um Datenschutz und betriebliche Nutzbarkeit in Einklang zu bringen.

### **Passenger-Flow-Analyse**

Der Bedarf seitens der Verkehrsunternehmen an einer datenschutzkonformen Erhebung von Passenger-Flow-Daten ist erheblich, da sie präzise Informationen zu Umsteigepunkten, Auslastungsspitzen oder eventbezogenen Nachfrageschwankungen eine optimierte Netzplanung ermöglichen.

Technisch erfordert dies eine Reidentifikation von Personen über Fahrzeuggrenzen hinweg. Diese ist notwendig, um Bewegungsereignisse korrekt zu verknüpfen, darf jedoch nicht zu einer dauerhaften Identifizierbarkeit führen. Daher mussten geeignete Anonymisierungs- und Schutzmechanismen entwickelt werden, die einerseits die Datenqualität erhalten und andererseits den Personenbezug wirksam reduzieren. Die Arbeiten waren Voraussetzung für eine datenschutzrechtlich vertretbare und zugleich funktional nutzbare Lösung.

### **Angemessenheit der eingesetzten Ressourcen**

Die Entwicklung der beschriebenen Lösungen erforderte die enge Verzahnung unterschiedlicher Fachgebiete: Training und Evaluation neuronaler Netze, Portierung auf Embedded-Hardware, Systemarchitektur, kryptographische Absicherung sowie datenschutzrechtliche Bewertung. Diese interdisziplinäre Komplexität entspricht den technologischen Anforderungen der Aufgabenstellung.

Insbesondere im Bereich Embedded-KI, hardwarebeschleunigter Bildverarbeitung und Anonymisierungs bzw. Kryptografie-Technologien mussten im Unternehmen zunächst Kompetenzen aufgebaut und geeignete Hardwareplattformen evaluiert werden.

## **5. Voraussichtlicher Nutzen und Verwertbarkeit**

Die entwickelten Lösungen adressieren zentrale Herausforderungen des ÖPNV: die Vereinbarkeit datengetriebener Optimierung bei einem hohen und technisch abgesicherten Datenschutzniveau. Sowohl die integrierte Pseudonymisierung von Videodaten als auch das fahrzeugübergreifende Tracking schaffen die Grundlage für neuartige, marktfähige Systeme mit erheblichem wirtschaftlichem Potenzial.

### **Pseudonymisierung von Videoüberwachungsmaterial**

Durch die selektiv reversible Pseudonymisierung kann der Kreis der Personen, die Videomaterial sichten und bewerten dürfen, signifikant erweitert werden, ohne dass die Identität der erfassten Fahrgäste offengelegt wird. Dies ermöglicht eine beschleunigte Erstbewertung von Vorfällen und unterstützt Verkehrsunternehmen dabei, Opfern von Gewalt- oder Vandalismusereignissen schneller und zielgerichteter Hilfe zu leisten. Die zeitnahe Auswertung von Vorfällen stellt im heutigen ÖPNV-Betrieb eine organisatorische und datenschutzrechtliche Herausforderung dar, für die die entwickelte Lösung einen strukturellen Lösungsansatz bietet.

Aus wirtschaftlicher Sicht eröffnet die Pseudonymisierung die Möglichkeit, bestehende Videosicherheitsprodukte um ein klar differenzierendes, datenschutzintegriertes Funktionsmerkmal zu erweitern. Das technische Umsetzungsrisiko wird auf Basis der bisherigen Arbeiten als sehr gering eingeschätzt. Das Marktpotenzial wird im nationalen Umfeld als mittel bis hoch bewertet, mit zusätzlichem Potenzial in europäischen und internationalen Märkten. Eine Integration in das Produktportfolio ist mit Verfügbarkeit geeigneter KI-Kameras vorgesehen.

### **Fahrzeugübergreifendes Tracking und Passenger-Flow-Analyse**

Das anonymisierte fahrzeugübergreifende Tracking adressiert eines der strukturellen Kernprobleme des ÖPNV: die belastbare, kontinuierliche und datenschutzkonforme Erhebung von Passenger-Flow-Daten. Bislang basieren entsprechende Planungen häufig auf punktuellen Fahrgastbefragungen oder indirekten Erhebungsverfahren, die entweder kostenintensiv, nur eingeschränkt repräsentativ oder datenschutzrechtlich kritisch (z. B. WLAN-Sniffing) sind.

Die im Projekt entwickelte Architektur nutzt bestehende Videoinfrastruktur im Fahrzeug und kombiniert diese mit KI-gestützter Merkmalsvektorgenerierung sowie kryptographisch abgesicherter Verarbeitung. Dadurch wird eine nicht-biometrische Reidentifikation zur Ermittlung von Umsteigebeziehungen ermöglicht, ohne eine dauerhafte personenbezogene Nachverfolgung zu erlauben.

Durch das Aufsetzen auf vorhandene Kamerasysteme und die Nutzung von KI-Beschleunigern, die perspektivisch auch für weitere Funktionen eingesetzt werden können, fügt sich die Lösung in eine industrieorientierte Digitalisierungsstrategie ein und stärkt die technologische Wettbewerbsfähigkeit des Standorts Deutschland im Bereich datenschutzkonformer Mobilitätslösungen.

Das technische Umsetzungsrisiko wird aktuell als gering eingeschätzt, wenngleich für eine produktreife Lösung noch ein domänenspezifischer Trainingsdatensatz erweitert werden

muss. Das Marktpotenzial wird als hoch bis sehr hoch bewertet, insbesondere im deutschen Markt, mit zusätzlichem Wachstumspotenzial im europäischen und internationalen Umfeld.

## **6. Fortschritt bei anderen Stellen**

Relevante Entwicklungen im Bereich Anonymisierung, Embedded-KI und datenschutzfreundlicher Videoanalyse wurden kontinuierlich beobachtet. Wissenschaftliche Arbeiten zu Differential Privacy oder k-Anonymität existieren, adressieren jedoch nicht die spezifische Kombination aus Echtzeitfähigkeit, Embedded-Umsetzung, selektiver Reversibilität und fahrzeugübergreifender datenschutzkonformer Auswertung im ÖPNV-Kontext.

Nach aktuellem Kenntnisstand sind keine inhaltlich vergleichbaren, marktnahen Umsetzungen bekannt. Externe technologische Entwicklungen, insbesondere bei KI-Beschleunigern, wurden berücksichtigt, ohne dass eine grundlegende Anpassung der Projektziele erforderlich war.

Abbildung 1.1, Background – Foreground Konzept

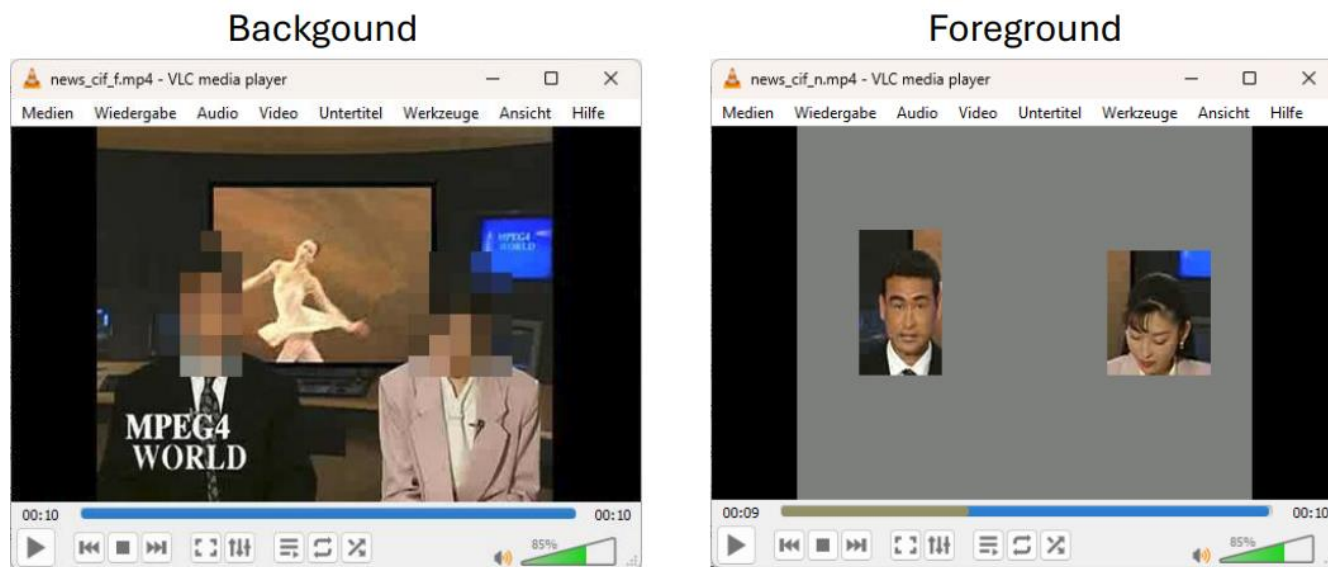


Abbildung 1.2, Videoplayer zur deanonymisierung einzelner Fahrgäste

