

Treuhandstelle für Mobilitätsdaten

TreuMoDa

Abschlussbericht zum Teilvorhaben des Karlsruher Instituts für Technologie

Projektlaufzeit: Januar 2022- Dezember 2023

Projektkronym: TreuMoDa

Förderkennzeichen: 16DTM112A

Koordinator:

Prof. Dr. rer. Nat. Frank Gauterin (frank.gauterin@kit.edu)

Karlsruher Institut für Technologie

Institut für Fahrzeugsystemtechnik
Rintheimer Querallee 2
D-76133 Karlsruhe

Autoren:

Czech, Andreas (BIB); Geenen, Vivien (FAST); Krauß, Peter (SCC);
Lee, Jueun (TM); Riedel, Till (TM); Winandi, Achim (FAST)

DOI: 10.5445/IR/1000172026



This work is licensed under CC BY-SA 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>.



Finanziert von der
Europäischen Union
NextGenerationEU

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Inhalt

1 Einleitung	1
2 Verwendung der Zuwendung und erzielte Ergebnisse im Einzelnen.....	1
2.1 Arbeitspaket 1: Konzipierung eines tragfähigen Datentreuhandmodells für den fairen, transparenten und einfachen Datenaustausch	1
2.1.1 AP 1: Die Zielsetzung.....	1
2.1.2 AP 1: Die wesentlichen Ergebnisse	1
2.2 Arbeitspaket 2: Technisches Konzept Datenspeicherung und Datenaustausch	9
2.2.1 AP 2: Die Zielsetzung.....	9
2.2.2 AP 2: Die wesentlichen Ergebnisse	10
2.3 Arbeitspaket 3: Organisatorisches Konzept der Treuhandstelle für Mobilitätsdaten.....	14
2.3.1 AP 3: Die Zielsetzung.....	14
2.3.2 AP 3: Die wesentlichen Ergebnisse	14
2.4 Beteiligung des KITs an weiteren Arbeitspaketen	19
3 Die wichtigsten Positionen des zahlenmäßigen Nachweises.....	20
4 Die Notwendigkeit und Angemessenheit der geleisteten Projektarbeit	20
5 Nutzen und Verwertbarkeit des Ergebnisses.....	21
6 Fortschritte auf dem Gebiet des Vorhabens	21
7 Veröffentlichungen der Ergebnisse	22
Literaturverzeichnis	22
Abbildung 1: Realistisches vs. Optimistisches Konzept.....	2
Abbildung 2: Beispielhafte Modellberechnung innerhalb des Finanzierungskonzept unter Einbezug der Ergebnisse	6
Abbildung 3: Die wesentlichen Aspekte der SWOT-Analyse zum realistischen Konzept	8
Abbildung 4: Eine abstrakte Struktur der technischen Umsetzung der TreuMoDa-Plattform.....	12
Abbildung 5: Initialer Mockup in Balsamiq	15
Abbildung 6: Prozessübersicht realistisches Konzept.....	15
Abbildung 7: Beispielprozess Stichprobenanonymisierung als BPMN	16
Abbildung 8: Beispiel Mockup für Datensatz	18
Abbildung 9: Beispiel Mockup zu Kontrolle des Anonymisierungsniveaus.....	18
Abbildung 10: Auswertung des Bedarfs an Metadaten aus Erprobung	19
Abbildung 11: Einbindung der am FZI entwickelten Verfahren in Mockup	19
Abbildung 12: Anonymisierung tracebasierter Daten	20

1 Einleitung

Das Projekt TreuMoDa zielte darauf ab, nach dem aktuellen juristischen Rahmen eine Treuhandstelle zu entwerfen. Besonders wichtig ist hierbei eine rechtliche Umsetzbarkeit des Konzepts nach Abschluss des Projektes. TreuMoDa definiert die Hauptaufgaben einer Treuhandstelle für Mobilitätsdaten in der Anonymisierung und Pseudonymisierung von personenbezogenen Daten aus dem Mobilitätsbereich und im Informieren und Beraten über den Datenaustausch.

2 Verwendung der Zuwendung und erzielte Ergebnisse im Einzelnen

Innerhalb dieses Kapitels werden schwerpunktmäßig die von KIT geleiteten Arbeitspakete des Gesamtvorhabens und die erreichten Ergebnisse vorgestellt (Abschnitt 2.1-2.3). Das KIT hat zusätzlich zu weiteren Arbeitspaketen gearbeitet (Abschnitt 2.4). Zusammen mit den Schlussberichten der anderen beteiligten Partner (Förderkennzeichen 16DTM112B und 16DTM112C) ergibt sich ein vollständiges Bild zur Konzeptionierung einer Treuhandstelle für Mobilitätsdaten.

2.1 Arbeitspaket 1: Konzipierung eines tragfähigen Datentreuhandmodells für den fairen, transparenten und einfachen Datenaustausch

2.1.1 AP 1: Die Zielsetzung

Ziel dieses Arbeitspakets war es, die Fortschritte jedes Arbeitspakets zu begleiten und die Bedarfe der Stakeholder in ein Gesamtkonzept der Treuhandstelle zu überführen. Dazu wurden in einem iterativen Prozess Gespräche oder Workshops mit den assoziierten Partnern geführt, um die Bedarfe der assoziierten Partner zu erfassen und darauf aufbauend das Gesamtkonzept zu entwerfen. Die aus dieser Arbeit resultierenden wesentlichen Ergebnisse sind die Aufschlüsselung der verschiedenen Positionen und Bedarfe der Stakeholder, sowie die Identifikation von Zielkonflikten, das Geschäftsmodell der Treuhandstelle und eine Analyse der Stärken, Schwächen, Chancen und Risiken dieses Geschäftsmodells.

2.1.2 AP 1: Die wesentlichen Ergebnisse

Positions- und Bedarfsanalyse

Die assoziierten Partner wurden entlang eines Fragebogens zu Ihren Bedarfen befragt und Antworten in einer Analyse zusammengestellt. Die Vorstellungen über eine Treuhandstelle waren sehr verschieden. Wesentliche Punkte, die genannt wurden, sind:

- Aufbau eines Datenpools an Mobilitätsdaten
- Treuhänder trägt die Verantwortung für Datenschutz
- Verwaltung von (anonymisierten) Daten
- Vertrauensvolle, uneigennützige Institution
- Diskriminierungsfrei und unparteiisch
- Qualitätsbewertung von Daten/Datensätzen
- Anwendungsgerechter Datenaustausch: Datennutzer erhält nur die sensiblen Daten, die er auch benötigt

- alle relevanten Daten an einem Ort (z. B. auch Wetterdaten)
- Erhalt der Kontrolle über eigene Daten
- Klärung von Haftungsfragen über die Treuhandstelle verhindern

Für 8 von 10 Befragten werden aktuell oder sollen zukünftig Mobilitätsdaten für die Produktoptimierung genutzt werden. Die 70 Prozent der Befragten kennen GAIA-X, wohin gegen International Data Spaces (IDS) etwas unbekannter war. Zur Frage, ob eine Treuhandstelle nach den Prinzipien dieser Initiativen entworfen werden soll, haben 50 Prozent (GAIA-X) bzw. 70 Prozent (IDS) der Befragten keine Meinung.

Zielkonflikte

In der Positions-, Bedarfsanalyse und rechtlichen Analyse durch AP 5 (siehe Abschlussbericht des FIZ Karlsruhe zum Projekt TreuMoDa, FKZ 16DTM112C) wurden einige Zielkonflikte identifiziert. Eine Anpassung nach dem ersten Konzeptentwurf wurde von den assoziierten Partnern vor allem im Bereich der Datenvermittlung sowie der Übernahme der Verantwortung für die Daten durch die Treuhandstelle gewünscht. Dabei war die Vorstellung einer Treuhandstelle mit Datenpool sehr präsent. Das Konsortium entschied am Kern des bestehenden Konzepts festzuhalten, da solch ein Konzept als tragfähiger für eine Umsetzung erachtet wurde. Daher wurden Anpassungen am bestehenden Konzept vorgenommen und es wurde ein neues, weiteres Konzept entworfen, um die Interessen der assoziierten Partner zu berücksichtigen.

Das Projektteam unterschied seitdem zwischen zwei Konzepten für eine mögliche Treuhandstelle: dem „realistischen Konzept“ und dem „optimistischen Konzept“ (siehe Abbildung 1). Das Projektteam möchte das realistische Konzept nach weiteren Entwicklungsstufen nach der Konzeptionierungsphase umsetzen. Daher muss das realistische Konzept in einem aktuell sicheren rechtlichen Rahmen liegen, nachhaltig finanzierbar sein und einen Beitrag für eine Förderung des Datenaustausches zwischen Parteien liefern. Das optimistische Konzept dient dazu, einen treuhänderisch idealen Aufbau einer Treuhandstelle aufzuzeigen. Hiermit möchte das Projektkonsortium auf rechtliche Grenzen und technische Herausforderungen aufmerksam machen.

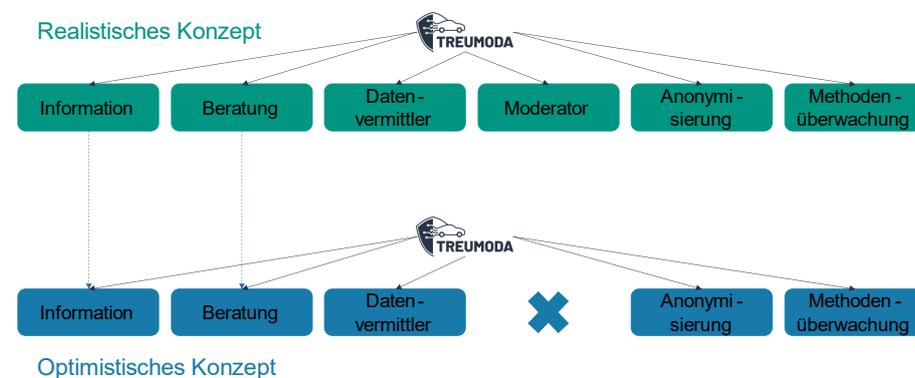


Abbildung 1: Realistisches vs. Optimistisches Konzept

Bei dem realistischen Konzept wurde entschieden, keine Daten bei einer Datenweiterleitung durch die Treuhandstelle langfristig zu speichern. Daher wird im realistischen Konzept keine Schaffung eines Datenpools vorgesehen. Das Projektkonsortium hat sich aus mehreren Gründen dagegen entschieden: Nur die Speicherung von anonymisierten Daten birgt für eine Treuhandstelle ein geringes Risiko. Die Speicherung von anonymen Daten lässt aber keine individuelle Anonymisierung von Daten nach den Anforderungen eines Datennehmers zu. Die Schaffung von individuellen Angeboten für Kunden der Treuhandstelle beurteilt das Projektteam als wichtiger als die Schaffung eines Datenpools von anonymisierten Daten. Hierfür sollten bestehende Initiativen genutzt werden, wie Datenmarktplätze (beispielsweise der Mobility Data Space), die Datenbestände und -bedarfe durch Angebote und Gesuche aufzeigen.

Im optimistischen Konzept sollen Rohdaten, also Daten mit Personenbezug, durch die Treuhandstelle gespeichert werden. Hierzu erhält die Treuhandstelle eine Lizenz des Datengebers, wodurch die Treuhandstelle in voller Verantwortung Daten teilen kann. Eine konsequente Umsetzung der individuellen Angebote für Datennnehmer kann dadurch realisiert werden und Datengeber werden in ihrer Verantwortung entlastet.

Geschäftsmodell

Das realistische Konzept kann in drei Hauptaktivitäten der Treuhandstelle untergliedert werden, welche größtenteils ohne Abhängigkeit voneinander gestartet werden können: zum einen die Datengebervermittlung, die treuhänderische Anonymisierungsdienstleistung sowie die Methodenüberwachung. Zur Erfüllung der Datenvermittlerrolle sollen anonymisierte Stichproben als Testdaten von Datengebern für Vermittlungszwecke durch die Treuhandstelle gespeichert werden und bei Bedarf an potenzielle Datennnehmer weitergeleitet werden. Datennnehmer können so über die Treuhandstelle nach passenden Datengebern suchen, indem sie die Testdaten auf Qualität und Nutzbarkeit prüfen. Der treuhänderische Anonymisierungsdienst sieht vor, dass sich Datengeber und Datennnehmer bilateral über einen Datenaustausch von zu anonymisierenden oder personenbezogenen Daten einig sind. Beispielsweise könnte der Kontakt über die Treuhandstelle nach der Weitergabe von Testdaten aufgebaut worden sein. Datengeber und Datennnehmer wenden sich an die Treuhandstelle, um die Voraussetzungen für den Datenaustausch mit der Treuhandstelle zu besprechen. Zunächst sichtet die Treuhandstelle die Daten, schätzt die Machbarkeit sowie den Aufwand einer Anonymisierung ein und erstellt ein entsprechendes Angebot. Nachdem Datennnehmer und -geber dieses akzeptiert haben, vergibt der Datengeber den Auftrag zur Verarbeitung und Anonymisierung der Daten. Für die Dienstleistung zahlt der Datennnehmer, da dieser das Interesse an der Nutzung der anonymisierten Daten hat. Nach erfolgreichem Abschluss eines Anonymisierungsprozesses oder bei Übermittlung entsprechender Informationen zu verwendeten Anonymisierungsverfahren können die Verantwortlichen eines Datensatzes ein Abonnement zur Überwachung der genutzten Methoden bei der Treuhandstelle abschließen. Die Treuhandstelle überprüft die Anonymisierungsmethoden in regelmäßigen Abständen auf Qualität oder nach Schadsoftware, sodass nach der Datenschutz-Grundverordnung (DSGVO) dauerhaft eine bestmögliche Anonymisierung vorliegt und im Falle einer Reidentifikation die Verantwortlichen frühzeitig eine Warnung und Handlungsempfehlung durch die Treuhandstelle erhalten.

Die Treuhandstelle selbst bleibt zu jedem Zeitpunkt eine neutrale Instanz zwischen Datennnehmern und Datengebern, da sie selbst kein Interesse an der Datennutzung hat und auch nicht gewinnorien-

tiert arbeiten möchte. Gleichzeitig sind für den Ablauf des Datenaustausches die Interessen von Datengeber und -nehmer von gleicher Relevanz für die Treuhandstelle. Ohne den Datengeber stehen keine Daten für einen Datenaustausch zur Verfügung und ohne den Datennehmer erfolgt keine Bezahlung für die Arbeit der Treuhandstelle. Daher ist die Treuhandstelle intrinsisch motiviert die Interessen beider Parteien gleichermaßen zu vertreten. Auch das gemeinnützige, nicht-profitorientierte Auftreten der Treuhandstelle begünstigt die Neutralität der Treuhandstelle. Auf der anderen Seite hat die juristische Analyse ergeben, dass sich die Treuhandstelle am geeignetsten als GmbH gründet (siehe Abschlussbericht des FIZ Karlsruhe zum Projekt TreuMoDa, FKZ 16DTM112C). Um die Glaubwürdigkeit der Neutralität einer Treuhandstelle zu gewährleisten, empfiehlt es sich nach den Rückmeldungen der assoziierten Partner, dass der Staat oder Hochschulen als Gesellschafter fungieren.

Die Treuhandstelle übernimmt im Auftrag des Datengebers die Verarbeitung/Anonymisierung der Daten. Der Datengeber behält hierdurch die Verantwortung der Einhaltung der datenschutzrechtlichen Bestimmungen nach der DSGVO. Die Treuhandstelle hat aber die Aufgabe, die Umsetzung der rechtmäßigen Datenweitergabe zu unterstützen. Beispiele hierfür könnten die passende Auswahl eines Anonymisierungsverfahrens oder eine erneute Prüfung der anonymisierten Daten beim Datennehmer nach aktuellem Stand der Technik sein.

Zur Beschreibung des Geschäftsmodells orientiert sich die Treuhandstelle an dem Business Modell Canvas (BMC) (Wohllebe 2022). Hierzu wird im Folgenden nach den neun Rubriken des BMC die Treuhandstelle TreuMoDa beschrieben.

Key Resources

Die *Key Resources* der Treuhandstelle sind Daten. Es handelt sich dabei um externe Daten, die der Treuhandstelle selbst nicht gehören. Die Daten stammen von einem Datengeber, der zusammen mit einem Datennehmer eines der Angebote der Treuhandstelle (siehe Offering) in Anspruch nehmen möchte. Die Treuhandstelle spezialisiert sich auf Mobilitätsdaten im Anwendungsfeld automatisiertes Fahren. Daher handelt es sich bei den potentiellen Daten um beispielsweise Kamera-, Radar- und Lidardaten aus Fahrzeugen oder der Straßeninfrastruktur. Auch konventionelle Fahrzeugdaten wie Positions-, Geschwindigkeits- und Beschleunigungsdaten werden im Bereich der Automatisierung benötigt. Beim automatisierten Fahren werden für die Orientierung der Fahrzeuge zusätzlich Daten aus der Umgebung benötigt, wie z. B. Positionen von Gebäuden, Straßenbeschaffenheit, Orte von Baustellen oder die Witterung. Auch diese Daten können über die Treuhandstelle ausgetauscht werden.

Zusätzlich kann die Expertise der Beschäftigten der Treuhandstelle als Key Resources verstanden werden. Es werden Experten für die Anonymisierungsmethoden sowie für die rechtliche Beratung benötigt.

Ebenso relevant ist die IT-Infrastruktur der Treuhandstelle, welche das Speichern der Testdaten und die Verarbeitung der Daten mit den KI-Modellen ermöglicht.

Key Activities

Die Treuhandstelle sieht ihre Kompetenzen im Bereich der Anonymisierung von personenbezogenen Daten aus dem Mobilitätsbereich. Hierzu zählen unter anderem das Anonymisieren von Kameradaten

ohne Verlust an dem für den Datennehmer relevanten Informationsgehalt, beispielsweise die Erfassung der Blickrichtung von Personen im Straßenverkehr oder die Anonymisierung von Positionsdaten wie GPS-Daten (Global Positioning System). Um eine Anonymisierung zu realisieren, ist die passende Auswahl der Anonymisierungsmethode sowie deren sichere Anwendung durch Beschäftigte der Treuhandstelle notwendig.

Für das Angebot der technischen Beratung und rechtlichen Information recherchiert die Treuhandstelle entsprechende Informationen. Um dem Bedarf der Beratung gerecht zu werden, gehören ebenfalls der Aufbau von KI-Modellkarten zur Erläuterung der verwendeten Verfahren und Visualisierungen der Stufen der Anonymisierung sowie der Risiken der verwendeten Verfahren zu den Key Activities der Treuhandstelle.

Für die Datengebervermittlung wird mit Erlaubnis des Datengebers eine anonymisierte Stichprobe auf den Servern der Treuhandstelle gespeichert und auf Anfrage von potenziellen Datengebern an diese weitergeleitet.

Für die Moderationsaufgabe zwischen Datengeber und Datennehmer organisiert die Treuhandstelle gemeinsame Meetings und stellt ein Muster für einen Datenerwerbsvertrag zur Verfügung. Dieser wird von den Experten der Treuhandstelle entworfen. Zum Abschluss des Vertrages sollen durch den Datengeber und Datennehmer beispielsweise die Verwendungszwecke oder die Speicherdauer der Daten bestimmt werden.

Zur Realisierung des Methodenüberwachungsangebots im Abonnement ist es notwendig, in regelmäßigen Abständen eine Recherche zum Stand der Technik der verwendeten Methode sowie entsprechender Schadsoftware durchzuführen.

Offering

Das Angebot der Treuhandstelle beinhaltet verschiedene Aspekte. Zum einen bietet die Treuhandstelle einen individuellen Anonymisierungsdienst für Mobilitätsdaten an. Die besonderen Bedürfnisse eines Datengebers oder Datennehmers werden wahrgenommen und umgesetzt. Die Treuhandstelle erleichtert Datennehmern den Erhalt von anonymisierten Daten, welche auf ihren Anwendungsfall zugeschnitten sind. Die individuelle Anonymisierungsdienstleistung ermöglicht die Vermeidung von Informationsverlust. Für den Datengeber bietet die Treuhandstelle Unterstützung im datenschutzkonformen Austausch. Hierzu bringt die Treuhandstelle ihre Expertise über die rechtlichen und technischen Aspekte des datenschutzkonformen Datenaustausches ein und verarbeitet die Daten im Auftrag des Datengebers.

Um die Bedürfnisse von Datengeber und Datennehmer in Einklang zu bringen, sind Absprachen zwischen diesen beiden Parteien nötig. Die Treuhandstelle unterstützt dabei den Kommunikationsaustausch und ermöglicht ein Zusammenkommen auf Augenhöhe.

Zusätzlich wird die Treuhandstelle nicht gewinnorientiert tätig, was eine unabhängige Beratung hinsichtlich der Nutzung der Treuhandstelle begünstigt. Die Treuhandstelle informiert über technisch und rechtlich notwendige Schritte, um personenbezogene Daten auszutauschen, sowie über die Folgen eines fehlerhaften Datenaustausches und die Verantwortung, die ein Datenaustausch mit sich bringt. Jeder Datengeber kann mit Hilfe dieser Informationen prüfen, ob er selbst das nötige Know-how für

einen sicheren Datenaustausch hat oder ob er die Dienste der Treuhandstelle in Anspruch nehmen möchte.

Neben diesen Angeboten bietet die Treuhandstelle einen Service, der bei Änderungen im Stand der Technik oder bekannten Sicherheitsproblemen der verwendeten Anonymisierungsmethoden warnt und individuelle Handlungsempfehlungen ausspricht. Dadurch kann die Sicherheit der DSGVO-Konformität über den Zeitraum des Abonnements verbessert werden.

Customer Segment

Die Treuhandstelle ist auf das Business to Business (B2B) Geschäft fokussiert, wobei gleichzeitig die Rechte von Privatpersonen geschützt werden müssen.

Die Treuhandstelle ist auf den Sektor Mobilität (insbesondere automatisiertes Fahren) spezialisiert, daher stammen Datengeber und Datennehmer primär aus diesem Bereich. Die Kundinnen und Kunden der Treuhandstelle forschen, entwickeln oder analysieren im Bereich der Mobilität. Datengeber können Automobilhersteller, Testfeld- oder Infrastrukturbetreiber sein. Unter potenziellen Datennehmern finden sich Automobilzulieferer, statistische Ämter oder Softwareentwickler.

Revenue Model

Damit die Treuhandstelle ihre Dienste zur Verfügung stellen kann, muss ein kostendeckendes Arbeiten ermöglicht werden. Daher ist eine Bezahlung durch den Datennehmer für die Anonymisierungsdienstleistung vorgesehen. Der Datennehmer ist hier in der Zahlungspflicht, da er derjenige ist, der ein Interesse an der Anonymisierung hat, um eine eigene Datennutzung zu ermöglichen. Erteilt ein Datengeber der Treuhandstelle häufiger einen Auftrag zur Datenaufbereitung mit denselben Metadaten, reduziert sich der Aufwand für die Treuhandstelle und die Entgelte für den Datennehmer können neu berechnet werden.

Neben der Anonymisierungsdienstleistung werden durch das Abonnement zur Methodenüberwachung Einnahmen für die Treuhandstelle generiert. Auch in diesem Angebot werden lediglich die entstehenden Kosten für diesen Dienst finanziert. Die Treuhandstelle erwartet aktuell, dass zumindest eine Anschubfinanzierung des Staates zum Start/Betrieb der Treuhandstelle benötigt wird. Aus Sicht der Treuhandstelle bietet sich eine Fehlbedarfsfinanzierung durch Gesellschafter der Treuhandstelle an.

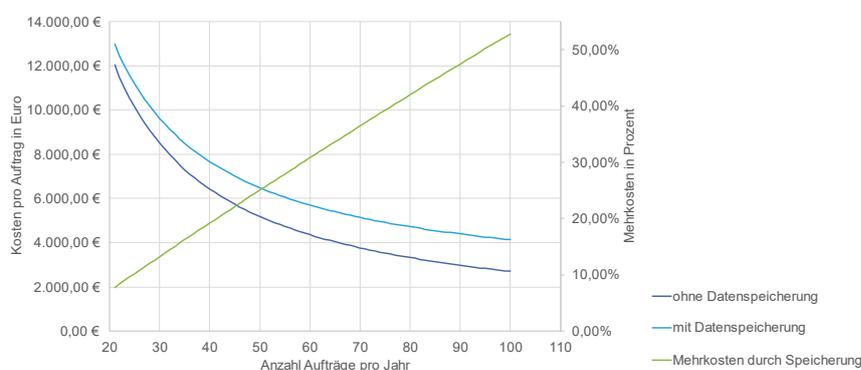


Abbildung 2: Beispielhafte Modellberechnung innerhalb des Finanzierungskonzept unter Einbezug der Ergebnisse

Cost Structure

Die Treuhandstelle erwartet in folgenden Bereichen Kosten, welche im Finanzierungskonzept beziffert werden.

- Fixkosten:
 - Personalkosten
 - Betrieb von Servern
 - Softwarelizenzen
 - Büroinfrastruktur (Heizkosten, Miete, Strom, Wasser, digitale Infrastruktur (Internet))
- Investitionskosten:
 - Server
 - Ausrüstung für Mitarbeiter: PC, Büroartikel...
- Variable Kosten:
 - Reisekosten
 - Weiterbildung
 - Kosten für die Datenverarbeitung (abhängig von Komplexität der Anonymisierung und zur Verfügung stehender Bearbeitungszeit)
 - Kosten für die Datenspeicherung (abhängig von Speicherdauer und Speichervolumen)
 - Zertifikate

Channels

Ein wichtiges Anliegen der Treuhandstelle ist die persönliche Kontaktaufnahme und Kontaktpflege mit den Datennehmern und Datengebern. Dieser kann über E-Mailverkehr, Online-Meetings oder per Telefon stattfinden. Das Ziel ist dabei eine individuelle Unterstützung beim datenschutzkonformen Datenaustausch zu ermöglichen und die Parteien Datengeber und Datennehmer auf Augenhöhe zusammenzubringen.

Wichtige Informationen, die während des aktiven Prozesses mit der Treuhandstelle an Datengeber und Datennehmer weitergegeben werden müssen, werden in dem Nutzerportal der Treuhandstelle erfasst. Hier werden beispielsweise Angebote, Verträge, Metadaten und der Verarbeitungsstand durch die Treuhandstelle an die Kunden und Kundinnen weitergeleitet.

Customer Relationships

Da das Angebot der Treuhandstelle vor allem die individuellen Bedürfnisse der Kundinnen und Kunden erfüllen soll, steht eine persönliche Beziehung mit sowohl Datennehmer als auch Datengeber im Vordergrund. In einem Kundenbindungskonzept, welches eine langfristige Zusammenarbeit über mehrere Datenaustauschvorgänge anstrebt, werden Maßnahmen zur Kundenbindung und deren Wirkungsbereich aufgezeigt.

Key Partners

Die Treuhandstelle möchte einen gleichberechtigten Austausch zwischen Datengebern und Datennehmern fördern. Beide Parteien haben zudem gleiche Relevanz für die Arbeit der Treuhandstelle,

weshalb beide Parteien Schlüsselpartner für die Treuhandstelle darstellen. Allgemein muss aus der Interessensgruppe heraus die Bereitschaft bestehen, Daten auszutauschen.

Zusätzliche Geldgeber wie Forschungseinrichtungen oder das Land/ der Staat sind notwendig für die Einrichtung einer Treuhandstelle.

SWOT Analyse

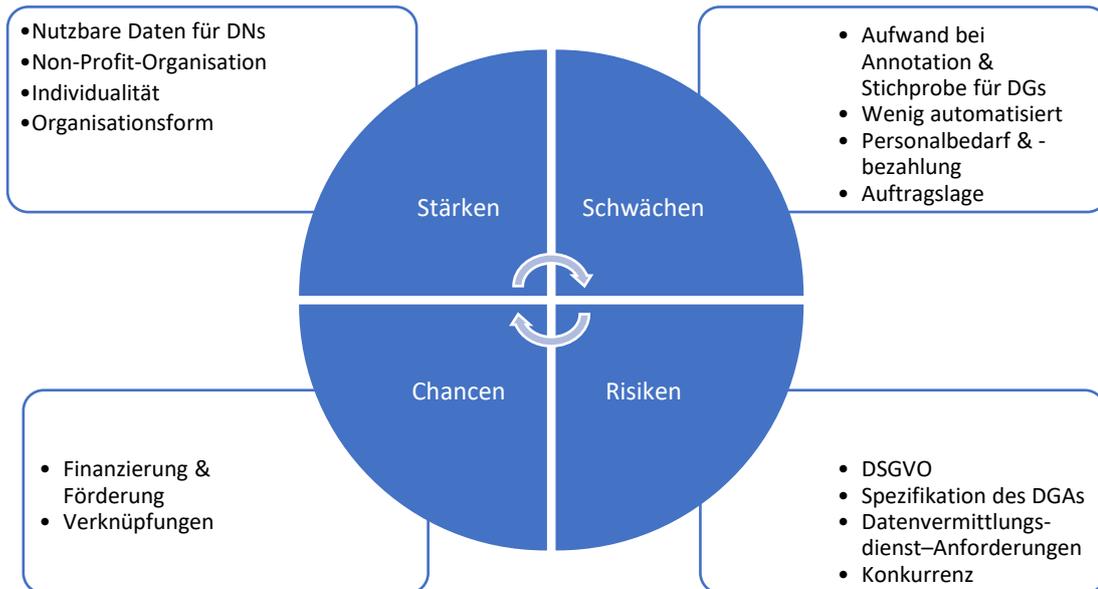


Abbildung 3: Die wesentlichen Aspekte der SWOT-Analyse zum realistischen Konzept

Es wurde eine Analyse der Stärken, Schwächen, Chancen und Risiken des realistischen Konzeptes durchgeführt. Abbildung 3 fasst die wesentlichen Aspekte übersichtlich zusammen. Die größte Stärke des Konzeptes liegt in der Ermöglichung von anwendungsspezifischen nutzbaren Daten für den Datenehmer. Dies erreicht die Treuhandstelle durch die Vermittlung der Interessen bei der Auswahl einer Anonymisierungsmethode zwischen Datenehmer und Datengeber. Gleichzeitig agiert die Treuhandstelle als Non-Profit-Organisation. Das bedeutet die Treuhandstelle muss keine Gewinne erzielen und wird von vertrauenswürdigen Institutionen wie beispielsweise Staat oder Hochschulen unterstützt. Gleichzeitig hat sie kein eigenes Interesse an der Nutzung der ausgetauschten Daten. Die Treuhandstelle ist nicht nur in der Anwendung von passenden Anonymisierungsverfahren individuell, sondern auch in der Betreuung der Nutzer durch persönliche Ansprechpartner sowie individuelle Anpassungen der Verträge, die mit der Treuhandstelle eingegangen werden, beispielsweise bei Nutzungszwecken oder Löschfristen. Eine GmbH als Organisationsform ist ebenfalls den Stärken zuzuordnen mit der Gesellschaft von vertrauensvollen Institutionen wie Staat oder Hochschulen. Auf der anderen Seite belasten die Schwächen vorrangig die Datengeber. Die Datengeber bleiben in der Verantwortung für die ausgetauschten Daten. Laut Gesetz müssen sie dafür auch über die Zwecke und Mittel zur Verwendung der Daten entscheiden. Hierzu gehört auch personenbezogene Daten zu annotieren und eine repräsentative Sichtprobe zu erstellen. Insgesamt folgen die Abläufe an der Treuhandstelle zwar vorgegebenen Prozessen, jedoch sind diese wenig automatisiert. Dies liegt unter anderem am hohen Bedarf nach individueller Betreuung der Nutzer der Treuhandstelle. Eine zukünftige Herausforderung kann für die Treuhandstelle die Einstellung qualifizierten Personals sein. Setzt man eine Bezahlung nach im öffentlichen Dienst üblichen Verträgen voraus, schmälert dies die At-

traktivität für Arbeitnehmer. Das benötigte hochqualifizierte Personal für die Aufgaben des Data Scientists oder mit Juraabschluss kann in anderen Branchen deutlich bessere Vergütungen erhalten. Dies verstärkt die Herausforderung, qualifiziertes Personal zu finden. Die Unvorhersehbarkeit der Auftragslage folgt sich aus der Ungewissheit darüber, ob Datengeber tatsächlich bereit sind, Daten zu teilen. Dies beeinflusst direkt die Finanzlage der Treuhandstelle, denn bei einer zu geringen Auftragslast kann die Treuhandstelle auch nicht kostendeckend arbeiten. Dem gegenüber stehen auch einige Chancen. Eine Förderung und Finanzierung der Treuhandstelle ermöglicht einerseits die Umsetzung dieser Treuhandstelle und kann auch beim nachhaltigen Betrieb der Treuhandstelle unterstützen. Verknüpfungen zu weiteren Plattformen, wie beispielsweise dem Mobility Data Space, könnten die Reichweite der Treuhandstelle erweitern und beide Plattformen könnten vom jeweiligen Angebot des anderen profitieren. Beispielsweise könnten Datengeber Angebote über eine Plattform wie den MDS zur Verfügung stellen und die Daten durch den Service der Treuhandstelle einen rechtskonformen Austausch ermöglichen. Einige Initiativen können auch als Konkurrenz zur Treuhandstelle für Mobilitätsdaten gesehen werden. Hierzu könnten beispielsweise Treuhandstellen, die ihr Angebot auf Mobilitätsdaten erweitern, oder kommerzielle Dienstleister mit ähnlichen Anonymisierungsverfahren gezählt werden. Alle weiteren Risiken lassen sich durch den rechtlichen Rahmen bisher nicht reduzieren. Die DSGVO wird beispielsweise durch die Landesdatenschutzbeauftragten der Bundesländer verschieden interpretiert. Eine korrekte Auslegung der DSGVO kann folglich abhängig vom Bundesland sein. Zusätzlich besteht für die Treuhandstelle ein Risiko unbeabsichtigt rechtlich mit dem Datengeber in die Verantwortung gezogen zu werden. Die Treuhandstelle möchte sich im Data Governance Act (DGA) als Datenvermittlungsdienst einordnen. Ungewiss ist hierbei, welche sektoriellen Anforderungen noch folgen werden, da diese gesetzlich noch offen sind. Unklar sind zudem die Ausgestaltung der Kontrollbehörde und die möglichen Folgen bei einem Verstoß gegen den DGA.

Insgesamt überwiegen die Stärken des Konzeptes die Schwächen, da in der Gesamtanalyse zur SWOT noch weitere Aspekte wie beispielsweise das Angebot der Methodenüberwachung, Risikominimierung für Datengebende oder Überprüfungsmöglichkeit der Datenqualität für Datennehmer etc. betrachtet wurden. Auch können sich einige Schwächen durch Chancen abmildern. Zum Beispiel kann eine Finanzierung und Förderung sich positiv auf den Personalbedarf und -bezahlung auswirken oder Verknüpfungen mit anderen Plattformen die Auftragslage beeinflussen.

2.2 Arbeitspaket 2: Technisches Konzept Datenspeicherung und Datenaustausch

2.2.1 AP 2: Die Zielsetzung

Ziel im Arbeitspaket 2 „Technisches Konzept“ war es, das Konzept für eine robuste und effiziente Infrastruktur für den sicheren und vertrauenswürdigen Austausch von Mobilitätsdaten zu schaffen. Dies sollte unter Berücksichtigung der sich aus den anderen Arbeitspaketen ergebenden Anforderungen an Datenschutz, Datensicherheit, Wirtschaftlichkeit und Benutzerfreundlichkeit sowie hinsichtlich der sich im Laufe der Zeit ändernden Anforderungen bei der Datenverarbeitung erfolgen.

Die Hauptziele des Arbeitspakets 2 umfassten:

- Entwicklung einer skalierbaren, erweiterbaren Architektur: Es soll eine Architektur konzipiert werden, die nicht nur den aktuellen Anforderungen gerecht wird, sondern auch zukünftige Erweiterungen und Anpassungen ermöglicht. So ist beispielsweise davon auszugehen, dass die Nutzerzahlen zu Beginn des Projektes noch gering sind, aber im Laufe der Zeit zunehmen werden. Die Architektur muss daher in der Lage sein, mit steigenden Nutzerzahlen umzugehen und hinsichtlich Datenverarbeitung, Datenübertragung und Datenhaltung entsprechend zu skalieren. Weiter ist es wahrscheinlich, dass sich die Anforderungen an die Datenverarbeitung im

Laufe des Projekts ändern werden. Aktuelle Verfahren zur Anonymisierung von Daten werden sich weiterentwickeln oder neu entstehen, die Architektur muss daher flexibel genug sein, um diese Änderungen zu berücksichtigen und die notwendigen Anpassungen zu ermöglichen.

- Sicherstellung der Datensicherheit und des Datenschutzes: Die Architektur muss so konzipiert werden, dass die Sicherheit und der Schutz der Daten gewährleistet sind. Die rechtliche Einordnung der Datentreuhandstelle erfolgt in Arbeitspaket 5, es ergeben sich daraus Anforderungen an die technische Umsetzung der Treuhandstelle. Da davon auszugehen ist, dass personenbezogene Daten verarbeitet werden, müssen durchweg Verfahren eingesetzt werden, die den höchsten Standards zum Schutz der Daten entsprechen. Dies beinhaltet die Implementierung verschlüsselter Übertragungswege, sicherer Speicherlösungen und effektiver Zugriffskontrollen. Es soll dabei auf Verfahren und Protokolle zurückgegriffen werden, die sich in der Praxis bewährt haben und die dem aktuellen Stand der Technik entsprechen.
- Interoperabilität mit bestehenden Systemen: Es soll gewährleistet werden, dass die zu entwickelnde Architektur mit bereits existierenden Plattformen und Protokollen kompatibel ist. Dies sollte eine reibungslose Integration in die bestehende Infrastruktur ermöglichen und gleichzeitig Raum für zukünftige technologische Entwicklungen bieten. Ein Beispiel, das im Rahmen des Projekts als mögliche Erweiterung in Betracht gezogen wird, ist der Mobility Data Space (<https://mobility-dataspace.eu/>).
- Benutzerfreundlichkeit und Zugänglichkeit: Im Rahmen von Arbeitspaket 3 ist die Entwicklung einer Benutzeroberfläche für die Datentreuhandstelle vorgesehen. Ziel von Arbeitspaket 2 ist es, die hierfür nötigen sicheren Schnittstellen anzubieten, sodass die Benutzeroberfläche auf diese aufbauen kann. Der Benutzerclient soll von verschiedenen Nutzergruppen verwendet werden können, ohne dass umfangreiche technische Kenntnisse erforderlich sind. Somit soll das Architektur-Konzept vorsehen, dass Schnittstellen für die Dateneingabe, die Datenverarbeitung und die Datenabfrage implementiert werden können.
- Monitoring und Anpassung: Im Betrieb soll die kontinuierliche Überwachung der Systemleistung der Treuhandstellen-Plattform möglich sein, um ihre Effektivität zu gewährleisten und gegebenenfalls Anpassungen vorzunehmen.

Die erfolgreiche Umsetzung dieser Ziele hat es ermöglicht, eine solide Grundlage für den sicheren und effizienten Austausch von Daten innerhalb des TreuMoDa-Projekts zu schaffen. Dabei stand stets die Balance zwischen Sicherheit, Wirtschaftlichkeit und technologischer Flexibilität im Vordergrund.

2.2.2 AP 2: Die wesentlichen Ergebnisse

Die im vorherigen Kapitel beschriebenen Ziele sollen durch eine geeignete Architektur erreicht werden. Da zu Beginn des Projektes noch kein konkretes Geschäftsmodell oder konkrete Anwendungsfälle feststanden, wurde eine abstrakte Architektur entwickelt, die flexibel genug ist, um auf sich ändernde Anforderungen reagieren zu können. Diese Architektur wurde dann gemäß des Projektplans weiter konkretisiert.

Zu Beginn des Projektes wurden verschiedene Architekturmodelle untersucht und bereits bestehende, ähnliche Projekte recherchiert. So wurde beispielsweise die Architektur von International Data Spaces (IDS) und deren Anforderungen zur Teilnahme analysiert und die Analyseergebnisse bei sämtlichen weiteren Schritten berücksichtigt. Es sollte somit möglich sein, dass eine Integration in die IDS-Architektur möglich ist. Die IDS-Architektur sieht vor, dass Datenanbieter (Data Provider) ihre Daten über einen Connector in den IDS einbringen. TreuMoDa könnte sich in den IDS als so genannten „Data Provider“ einordnen. Im Teilnehmer-Zertifizierungsprozess wäre dies bereits für die niedrigste Stufe (Entry Level) möglich. Das Projektkonsortium sieht aber Herausforderungen in der Implementierung des IDS-Connectors, welcher die technische Komponente zur Verknüpfung zwischen Datenaustauschenden ist. Innerhalb dieses Projektes sieht das TreuMoDa-Konsortium vor, dass das THS-Konzept möglichst leicht mit einem wählbaren Konnektor (IDS-Connector oder dem EDC: Eclipse Dataspace Connector) vereinbar ist. Der EDC wird beispielsweise beim Mobility Data Space verwendet. Der Connector ist allerdings nicht Teil dieses Projektes und müsste dann gegebenenfalls nachträglich in einem Folgeprojekt implementiert werden.

Bereits früh im Projekt zeichnete sich ab, dass sich durch die hohe Varianz bei Größe und Formaten der Daten und häufige Freigabeprozesse Herausforderungen auf infrastruktureller Seite bei der Skalierbarkeit der Architektur, der Wirtschaftlichkeit und der Sicherheit der Daten ergeben. Die Architektur muss daher so konzipiert sein, dass sie flexibel genug ist, um auf diese Herausforderungen reagieren zu können. Dies bedeutet, dass die Architektur skalierbar sein muss, um mit steigenden Nutzerzahlen umgehen zu können, und dass sie so gestaltet sein muss, dass sie verschiedene Arten von Daten verarbeiten kann. Weiterhin muss die Architektur so konzipiert sein, dass sie sicher ist und den Schutz der Daten gewährleistet. Dies beinhaltet die Implementierung von verschlüsselten Übertragungswegen, sicheren Speicherlösungen und effektiven Zugriffskontrollen.

Als erstes Ergebnis wurde somit ein generisches Infrastruktur-Konzept erstellt. Die Architektur in Abbildung 4 zeigt diesen ersten Entwurf angelehnt an gängige ELT-Pipelines (ELT: Extract, Load, Transform): In der ersten Schicht „Production Layer“ befinden sich die Daten-Produzenten, sog. „Datengeber“. Diese erstellen Daten, die verarbeitet werden sollen. Die Daten werden dann an die Treuhandstelle übergeben. Dies erfordert ein Dateneingangs-Gateway, eine Art Frontend-Speicher, mit dem die Datengeber direkt kommunizieren und Daten ablegen. Das Gateway ist somit die Schnittstelle an der Grenze zwischen TreuMoDa-Plattform und den Datengebern und befindet sich im sog. „Edge Layer“. Sobald die Daten in dieser Schicht vom Datengeber übergeben und über einen Freigabeprozess initial validiert wurden, werden die Daten in die Speicherschicht („Storage Layer“) der TreuMoDa-Plattform übergeben. In dieser Schicht werden Daten möglichst effizient hinsichtlich Verarbeitung gespeichert. Diese Daten können nun von verschiedenen Prozessoren des „Processing Layers“ verarbeitet werden. Auch hier sind verschiedene Arten von Prozessoren denkbar, so können beispielsweise Batch- oder Streaming-Pipelines implementiert werden. Sobald die Daten verarbeitet wurden, werden diese über den Edge-Layer und ein zum „Ingress-Gateway“ analog angelegtes Ausgangs-Gateway („Egress-Gateway“) dem Datennehmer („Consumer“) zur Validierung und Abholung bereitgestellt.

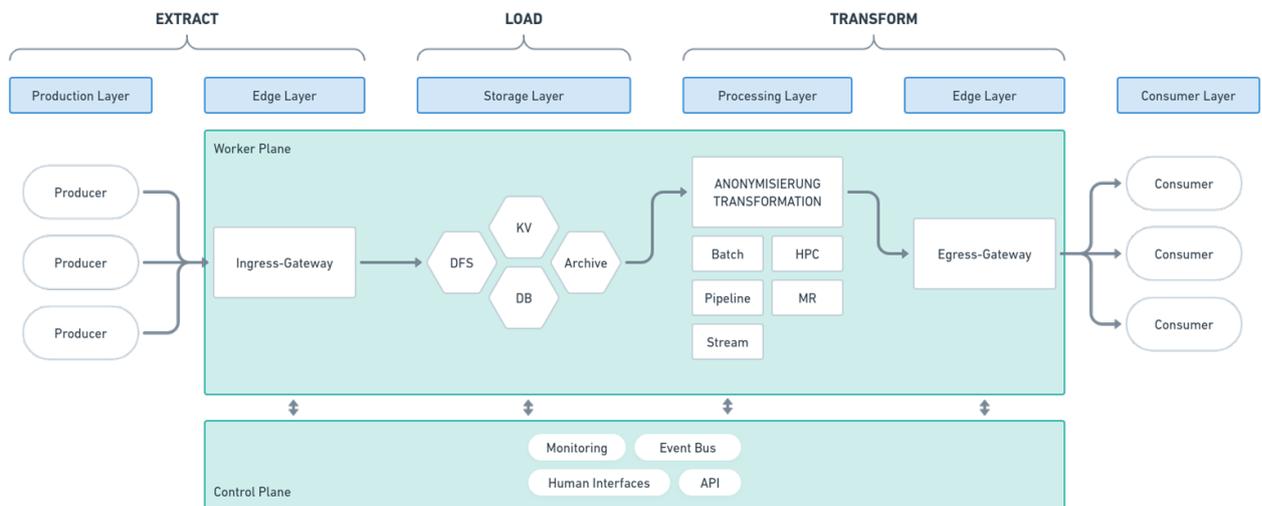


Abbildung 4: Eine abstrakte Struktur der technischen Umsetzung der TreuMoDa-Plattform

Im weiteren Projektverlauf wurden die Anforderungen an die verschiedenen Schichten sukzessive geschärft und Komponentenweise verschiedene Lösungen untersucht. Nachfolgend sollen die final ausgewählten Lösungen im Einzelnen dem Projektplan folgend aufgeführt werden:

- Datenspeicherung:** Ausgehend von den exemplarischen Geschäftsszenarien wurden drei Speicherklassen mit unterschiedlichen Anforderungen identifiziert. Zunächst überträgt ein Datengeber seine Daten an die Treuhandstelle in den sog. Staging Speicher im Ingress-Layer. Hier werden die Daten kurzfristig gespeichert und auf ihre Integrität geprüft. Das Zugriffsmuster ist in erster Linie seriell und die Datenübertragung kann als vorwiegender Flaschenhals angesehen werden. Für diese Speicherklasse wurden somit Speicher untersucht, die skalierbar und kostengünstig betrieben werden können. Geschwindigkeit und parallele Zugriffe sind nicht nötig. Als geeignet wurden hier Objekt-Speicher befunden. Diese zeichnen sich durch eine hohe Skalierbarkeit und Verfügbarkeit aus, allerdings sind Zugriffe auf einzelne Teile von Daten langsamer als bei Block-Speichern. In einem nächsten Schritt werden die Daten zur Verarbeitung auf einen Prozess-Speicher verschoben. Gängige Anonymisierungsverfahren können Daten-parallel arbeiten und benötigen somit schnelle Zugriffe auf die Daten. Hier wurden daher schnelle Block-Speicher als geeignet ausgewählt. Diese sind im Betrieb komplex und aufgrund der hohen Geschwindigkeit teurer als Objekt-Speicher. Diese Speicher sind allerdings nur während der Datenverarbeitung aktiv und können somit nach der Verarbeitung der Daten wieder freigegeben werden. Die dritte Speicherklasse sind Langzeitspeicher für archivierte Daten, auf selten zugegriffen wird. Dieser Speicher ist dafür gedacht, Daten zu speichern, die zur späteren Nachnutzung langfristig gesichert sein müssen. Aufgrund des Zugriffsmusters eignen sich Bandspeicher aufgrund ihrer geringen Betriebskosten sehr gut.
- Datentransfer:** Sämtliche Transfers zu und von der Treuhandstelle sollen selbstverständlich und grundsätzlich nach aktuellem Stand der Technik verschlüsselt sein. Hierfür wurden verschiedene Protokolle und Verfahren untersucht. Für den Datentransfer zwischen Datengeber und Treuhandstelle wurde das HTTPS-Protokoll als geeignet befunden. Dieses Protokoll ist weit verbreitet und wird von den meisten Systemen unterstützt. Im Projekt ist geplant, dass ein Kunde über einen Web-Client mit der Treuhandstelle Daten austauscht. HTTP über TLS

ist hierfür geeignet und ist auch in anderen Bereichen wie Online-Banking oder E-Commerce die Standardlösung.

- **Datenverarbeitung:** Die Datenverarbeitung erfolgt in der Processing-Schicht. Hier werden die Daten verarbeitet, anonymisiert und für den Datenehmer aufbereitet. Die Verarbeitung erfolgt in Batch-Prozessen, die in definierten Container-Umgebungen ablaufen. Die Container-Umgebungen sind so konzipiert, dass sie flexibel und skalierbar sind. Während des Projektes zeigte sich, dass eine Vielzahl unterschiedlicher Programme zur Anonymisierung von Daten zum Einsatz kommen werden. Diese Tools können in unterschiedlichen Programmiersprachen geschrieben sein und beispielsweise unterschiedliche, sich widersprechende Abhängigkeiten an Betriebssystem oder Softwareumgebung haben. Mit Containern kann eine Umgebung geschaffen werden, in der die Programme unabhängig laufen können. Durch die containerbasierte Verarbeitung können auch in Zukunft neue Anonymisierungsverfahren einfach integriert werden. Weiter können Container auch auf speziellen Container-Plattformen betrieben werden, die Datenzugriffe manipulationssicher nachvollziehbar machen (siehe Constellation-Projekt (<https://docs.edgeless.systems/constellation/>) oder Confidential Containers (<https://github.com/confidential-containers/documentation>)).
- **Autorisierung und Authentifizierung:** Um sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können, ist eine sichere Authentifizierung und Autorisierung notwendig. Hierfür wurden verschiedene Verfahren untersucht. Da es sich bei der Treuhandstelle um einen definierten Kundenkreis handelt und gründliche KYC-Prozesse vorgesehen sind, wird ein, im Vergleich zu dem weit verbreiteten Standard-Verfahren mit Benutzername/Password, recht aufwendiges, aber dafür etwas sichereres Verfahren mit Zertifikaten vorgesehen. Hierbei wird jedem Kunden ein Zertifikat ausgestellt, mit dem er sich gegenüber der Treuhandstelle authentifizieren kann. Die Zertifikate werden von einer Zertifizierungsstelle ausgestellt, die von der Treuhandstelle betrieben wird. Die Autorisierung erfolgt dann auf Basis der Zertifikate. Nur Personen, die ein gültiges Zertifikat besitzen, können auf Daten zugreifen, die für die durch das Zertifikat ausgewiesene Person oder Rolle zum Zugriff vorgesehen sind.
- **Metadaten:** Im letzten Schritt des Projektes wurden in den unterschiedlichen Arbeitspaketen Metadaten definiert, um die exemplarischen Szenarien aus den jeweiligen Sichten (organisatorisch, technisch, rechtlich, etc.) möglich zu machen. Aus technischer Sicht sind besonders Checksummen zur Prüfung der Datenintegrität sowie Metadaten zur Beschreibung des Verarbeitungsprozesses relevant. In jedem Fall werden diese Daten in einem strukturierten Datenformat erfasst und zusammen mit den Daten gespeichert. Hier wurden im Projekt verschiedene Varianten untersucht, aber aufgrund der hohen Flexibilität und der einfachen Handhabung wurde JSON-LD (<https://json-ld.org/>) als Kodierungsverfahren als geeignet befunden.

Die hier beschriebenen Komponenten bilden somit die Grundbausteine des oben dargestellten Architekturkonzepts. In einem Folgeprojekt kann nun aufbauend die konkrete Umsetzung der Architektur erfolgen.

2.3 Arbeitspaket 3: Organisatorisches Konzept der Treuhandstelle für Mobilitätsdaten

2.3.1 AP 3: Die Zielsetzung

Ziel des Arbeitspakets war es, die gewünschten Funktionen der Treuhandstelle inklusive der Anforderungen an Kuratierung, Qualitätssicherung, Aufbereitung und Bereitstellung des Datenbestandes zu definieren und sie in organisatorischen Strukturen, Maßnahmen und Prozessen abzubilden. Dabei sollten transparente Prozesse und klare Rollen entsprechend dem gewählten Treuhandmodell in Abstimmung mit AP1 und den regulatorischen Vorgaben in Abstimmung mit AP5 entwickelt werden. Anhand eines Funktionsdemonstrators in Form eines Mockups-UI sollten diese umgesetzt und dann in Zusammenarbeit mit den Stakeholdern aus dem bestehenden Netzwerk in Stakeholderdialoge anhand der definierten Testfälle erprobt werden. Darüber hinaus sollte ein Konzept zur Schaffung einer Geschäftsstelle geschaffen werden, die Datengeber und -nehmer bei allen Verfahrensschritten gezielt unterstützt, das Verfahren koordiniert und Hürden reduziert. Die Stelle würde bei auftretenden rechtlichen Problemen die nötige Expertise vorhalten und Maßnahmen, z. B. zur Anonymisierung, vorgeben.

2.3.2 AP 3: Die wesentlichen Ergebnisse

Literatur, Kontakt und Kommunikation

Um eine erste Bestandsaufnahme zu sich im Aufbau befindlichen Datentreuhandmodellen und insbesondere im Mobilitäts- sowie angrenzenden Bereichen zu machen, wurde Literatur zum Forschungsstand hierzu in Citavi gesammelt. Es wurde Kontakt zu weiteren vom BMBF geförderten Pilotvorhaben aufgenommen, zu denen MobiDataSol (<https://solingen.digital/projekte/mobi-data-sol>), DDTrust (<https://dd-trust.zih.tu-dresden.de/>) und MANDAT (<https://www.ti.rw.fau.de/projects/mandat/>) gehören, um vorhandene Synergien auszuloten.

Darüber hinaus wurde auch Kontakt zu weiteren datentreuhänderischen Anbietern aufgenommen, die nicht zu dem vom BMBF geförderten Pilotvorhaben gehören, aufgrund ihrer Geschäftsmodelle für die weitere Entwicklung von TreuMoDa dennoch interessant sind.

Zur internen und externen Projektkommunikation und Vernetzung wurden eine Website (www.treumoda.de), eine Funktionsmailadresse (treumoda@fast.kit.edu) und weitere Kanäle eingerichtet zu denen Mastodon, Twitter und LinkedIn gehören. Es wurde unterschiedliche Software wie z. B. Miro (<https://miro.com/de/>) genutzt, um Darstellungen und Ideen zum Konzept der Treuhandstelle für Mobilitätsdaten zu veranschaulichen.

TreuMoDa wurde als Data Space bei Data Space Business Alliance (DSBA) registriert und allgemeine Recherchen zur ISO 27001 wurden absolviert. Diese beschreibt das Management der Informationssicherheit, wozu beispielsweise ein Risikomanagementprozess und ein Informationssicherheitsmanagementsystem gehören.

Nutzerportal, WebUI und Vorbereitung Geschäftsstelle

Ein erstes beispielhaftes MockUp für ein Nutzerportal sowohl für Datennehmer als auch Datengeber (<https://gitlab.kit.edu/kit/treumoda/mockups> oder <https://doi.org/10.5281/zenodo.12541246>) wurde

mit der Software Balsamiq (<https://balsamiq.com/>) erstellt und in den Stakeholder-Gesprächen vorgestellt (siehe Abbildung 5). Dieses enthält u. a. Bereiche zur Anmeldung, einen Guide zum Datenaustausch, einem Dokumentenarchiv, einer Auftragshistorie sowie Kontakt- und Stammdaten. Aus den Gesprächen erfolgte das Feedback, dass die Relevanz der einzelnen Schritte hinsichtlich der Verantwortung im Webportal ersichtlich sein muss. Gemeint ist damit, dass Bestätigungen von Kontrollmechanismen nicht zu einfach gestaltet sein sollten, sodass dem Anwender die Bedeutung der Wichtigkeit hinter dem Schritt bewusst ist (keine einfachen Häkchen zum Datencheck). Weitere Resultate aus den Stakeholder-Gesprächen sind die Entscheidung zur Zahlungsmethode „Kauf auf Rechnung“, da damit jeder assoziierte Partner bezahlen kann, und der gewünschte Fokus auf den persönlichen Austausch mit Kunden der Treuhandstelle.

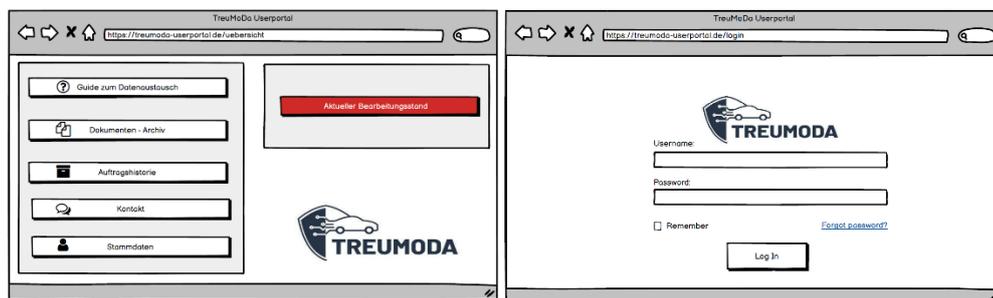


Abbildung 5: Initiales Mockup in Balsamiq

Auf der Grundlage von Stakeholder-Gesprächen konnten sieben Szenarien sowie eine Historien-Anfrage gebildet werden. Szenarien sind die folgenden: Forschung & Entwicklung, Versicherung, Automobilzulieferer, Verkehrsanalyst, Automobilhersteller, Infrastrukturbetreiber und statistische Ämter. Hieraus konnten die Prozesse der Treuhandstelle für Mobilitätsdaten (<https://gitlab.kit.edu/kit/treu-modu/treu-modu-prozesse> oder <https://doi.org/10.5281/zenodo.12541158>) im BPMN-Format (BPMN: Business Process Model and Notation) mit dem Prozessmodellierungstool Camunda erstellt werden (Beispiel siehe Abbildung 6).

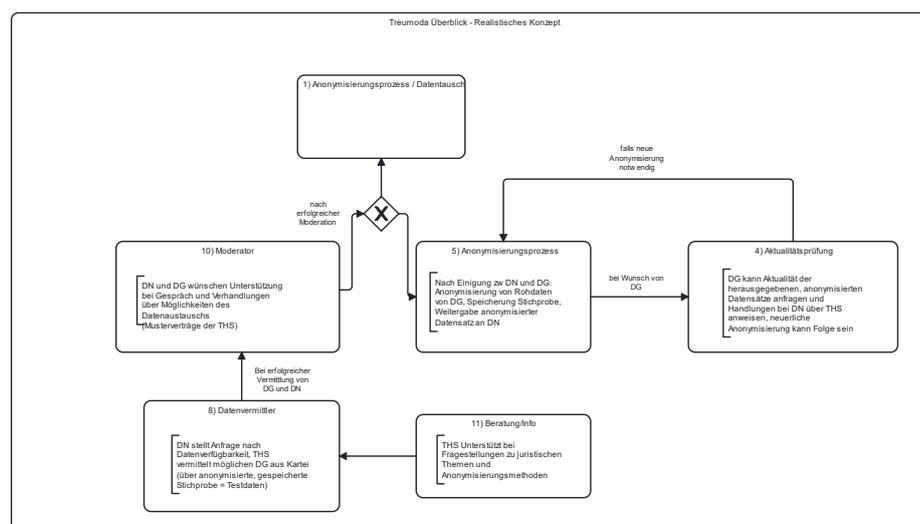


Abbildung 6: Prozessübersicht realistisches Konzept

Dabei wurden die Prozesse für das realistische und das optimistische Konzept modelliert (mehr hierzu siehe AP1). Es wurden im realistischen Fall die Aufgaben „Informieren“, „Beraten“, „Vermittler (von Datengebern)“, „Moderator“, „Anonymisierung“ und „Aktualitätsprüfung“ im Prozess dargestellt. Das optimistische Konzept unterscheidet sich zum realistischen in den Aufgaben durch den Wegfall der Moderationsaufgabe und innerhalb der definierten Prozesse (außer Beratung und Information).

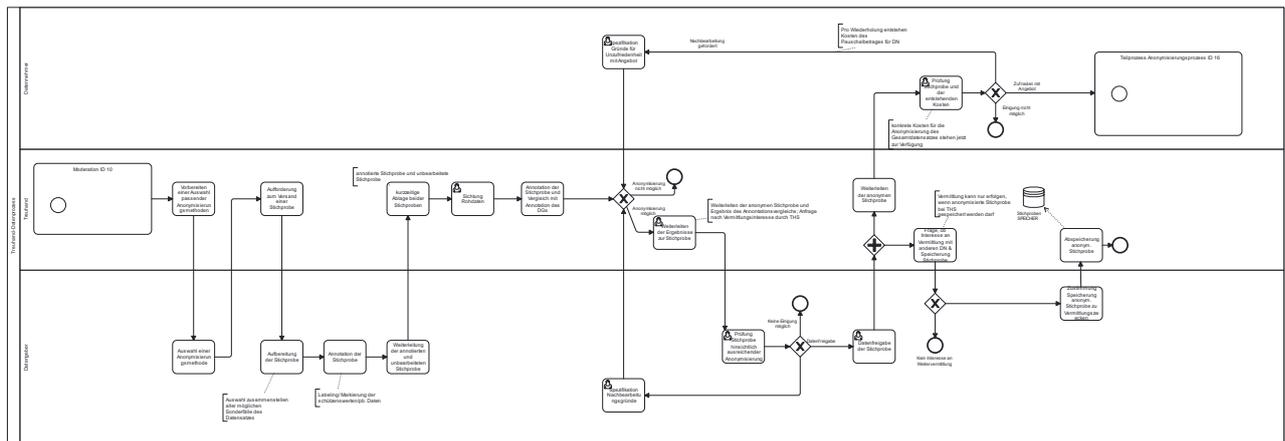


Abbildung 7: Beispielprozess Stichprobenanonymisierung als BPMN

Ein Konzept einer WebUI zum Management von Rollen und Prozessen wurde dargestellt. Dabei wurden die erforderlichen Rollen für die Geschäftsstelle definiert und diese aufgegliedert nach den verschiedenen Entwicklungsstufen, die vom Aufbau bis zur kontinuierlichen Weiterentwicklung der Datentreuhandstelle reichen. Es wurden die Aufgaben des Geschäftsführers, des Verwaltungsmitarbeiters, des Data Scientists/Data Managers, des Mitarbeiters mit juristischer Expertise und des CRM-Managers definiert sowie notwendige Fähigkeiten und Kenntnisse, die sie mitbringen sollten. So ist der Geschäftsführer nicht nur für den reibungslosen Ablauf der betrieblichen Unternehmensprozesse verantwortlich, sondern auch für die Mitarbeiterführung und -bindung, die Überwachung der Finanzen sowie die strategische Gesamtkonzeption. Er sollte Kenntnisse zum agilen Projektmanagement, zum Wissensmanagement sowie bestmöglich auch in Bezug auf Datenschutz mitbringen. Hier zeigt sich, dass das Anforderungsprofil eine gewisse Spezialisierung mitbringt, die etwa ein Jurist mit Schwerpunkt Datenschutz und entsprechender Berufserfahrung in einem Unternehmen mitbringen könnte. Die Aufgaben des Data Scientists/Data Managers wurden in den verschiedenen Entwicklungsstufen der Datentreuhandstelle detaillierter dargestellt, da hier differenzierte Rollen erforderlich sind. So könnte während des Aufbaus der Datentreuhandstelle ein Solution Architect Authentifizierungsfragen und solche in Bezug auf Datenschutz beantworten, während der Instandhaltung bzw. dem operativen Geschäft ist ein Administrator etwa in Form eines Fachinformatikers notwendig, der hier primär technischer Ansprechpartner und Support ist. Während der Weiterentwicklung der Datentreuhandstelle ist dann wieder ein Architect notwendig, der u. a. Kenntnisse zu KI-Methoden mitbringen sollte. Die Hauptaufgabe des Data Scientist/Data Manager besteht in der Selektion & Anonymisierung sowie der Weiterleitung der durch den Datengeber bereitgestellten Rohdaten an den Datennehmer. Dem Geschäftsführer und dem Verwaltungsmitarbeiter wurden bereits in der ersten Entwicklungsstufe Vollzeitstellen zugeordnet. Aufgrund des diversen Anforderungsprofils des Data Scientists/Data Managers könnte auch ein externer Berater in Erwägung gezogen werden, etwa jemand der im Bereich Data Science an einer Hochschule tätig ist, hier jedoch nicht in Vollzeit arbeitet und sein Profil durch die Mitarbeit am Aufbau und der Weiterentwicklung der Datentreuhandstelle schärfen will. Für den

CRM-Manager wurde ein Kundenbindungskonzept ausgearbeitet, das die Punkte Zufriedenheit des Kunden, Interaktion mit dem Kunden sowie finanzielle Anreize enthält. Geplant wurde, die Aufgaben der jeweiligen Mitarbeiter mit steigender Entwicklungsstufe der Treuhandstelle entsprechend zu erweitern und hierbei auch den Stellenumfang nach Möglichkeit zu erhöhen.

Einflussfaktoren, die den Aufbau der Geschäftsstelle betreffen, wurden näher dargestellt. Diese sind das bereits näher beschriebene Personal, eine nachhaltige Finanzierung und eine passende Organisationsstruktur. Hierbei wurde eine Übersicht zu den Personalkosten erstellt. Die Stelle des Mitarbeiters mit juristischer Expertise ist mit einem Stellenumfang von maximal 50 % vorgesehen, die des CRM-Managers mit zunächst 25 %. So könnte hier auch ein Werkstudent angestellt werden. Es wurden Vorschläge zur möglichen Organisationsstruktur der Treuhandstelle gemacht, d. h. etwa hierarchisch, funktional oder horizontal-flach organisiert, wobei die beiden letzteren favorisiert werden. Die funktionale Organisationsstruktur zeichnet sich dadurch aus, dass hier die Mitarbeiter nach ihren spezifischen Fähigkeiten und ihrer entsprechenden Funktion im Unternehmen organisiert sind und sich so auf ihre eigene Rolle konzentrieren können. Diese Organisationsstruktur ist in jeder Unternehmensgröße leicht skalierbar und ist gerade in der Aufbauphase eines Unternehmens von Vorteil, da sich die Mitarbeiter auf die Durchführung ihrer eigenen Aufgaben konzentrieren können. Die horizontal-flache Organisationsstruktur zeichnet sich dadurch aus, dass sie vor allem von Start-up-Unternehmen genutzt wird, um neue Abteilungen aufzubauen. Sie fördert eine offene Kommunikation im Unternehmen und verbessert die Koordination und Geschwindigkeit bei der Implementierung neuer Ideen.

Hinsichtlich der Wahl einer Rechtsform für die Datentreuhandstelle wird eine GmbH empfohlen. Aus den Stakeholder-Gesprächen kommt hervor, dass eine Angliederung an das KIT aus Gründen des Vertrauens und der Neutralität für potentielle Nutzende durchaus sinnvoll ist. So bittet sich eine Geschäftsstelle an der KIT-BIB mit einer eigenständigen Datentreuhandstelle an.

Erprobung Organisatorisches Konzept - Ergebnisse aus den Stakeholder-Workshops

Die Stakeholder-Gespräche bzw. Workshops wurden im Juni und November 2023 über Zoom organisiert, mit insgesamt 18 Stakeholdern, aufgeteilt in zwei Gruppen potenzieller Datenanbieter und Datenkonsumenten. Jeder Workshop bestand aus zwei Teilen: einem individuellen Interview, das durch die Mockups des TreuMoDa-Nutzerportal führte, und einer anschließenden halbstrukturierten Diskussion unter den eingeladenen Stakeholdern.

Insgesamt boten die Mockups in den Workshops (Beispiele siehe Abbildung 8 und Abbildung 9) eine positive Benutzererfahrung mit minimalem geistigem Aufwand für das Durchlaufen komplexer Datenfreigabeprozesse durch Dritte. Durch die Integration von Vertrauenselementen konnten die Mockups auch das Gefühl von Handlungsfähigkeit und Kontrolle bei den Nutzern in Entscheidungsprozessen im Datenraum stärken.



Abbildung 8: Beispiel Mockup für Datensatz

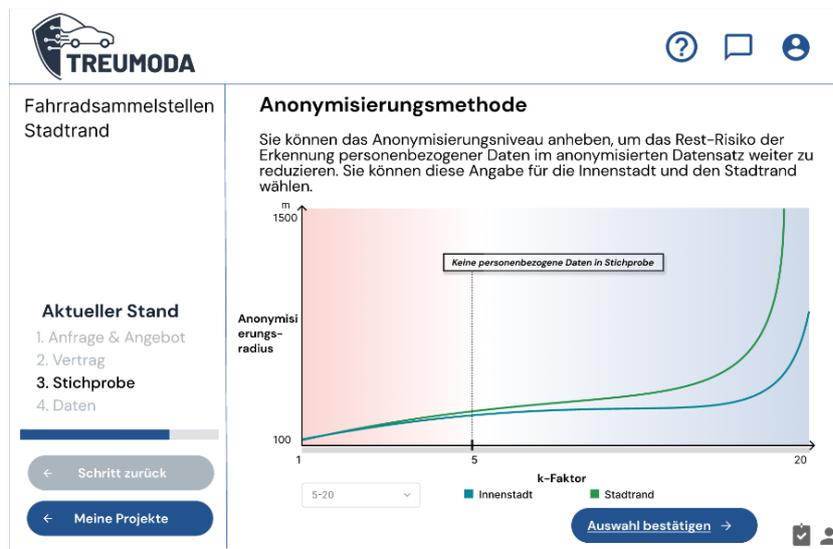


Abbildung 9: Beispiel Mockup zur Kontrolle des Anonymisierungsniveaus

Infolgedessen wurden mehrere wichtige Erkenntnisse deutlich. Die Betonung von TreuMoDa auf die Bereitstellung erschöpfender Metadaten wurde durch den Ruf der Teilnehmer nach detaillierteren Informationen während der Mockup-Interviews bestätigt. Die dichotomen Reaktionen zwischen technischen Experten und einem breiteren Publikum in Bezug auf Datenanonymisierung und KI-Methoden deuten auf die Notwendigkeit eines flexiblen Ansatzes hin. Darüber hinaus definierten die Umfrageergebnisse zu Metadatenanforderungen mehrere Metadatentypen, die potenzielle Nutzer als besonders wichtig erachten würden. Die Diskussionsergebnisse sprachen weitere Verbesserungsmöglichkeiten des TreuMoDa-Service an, z. B. durch die Integration einer Wissensbasis in das Benutzerportal und die Kombination des Datenraums mit Beratungsdiensten.

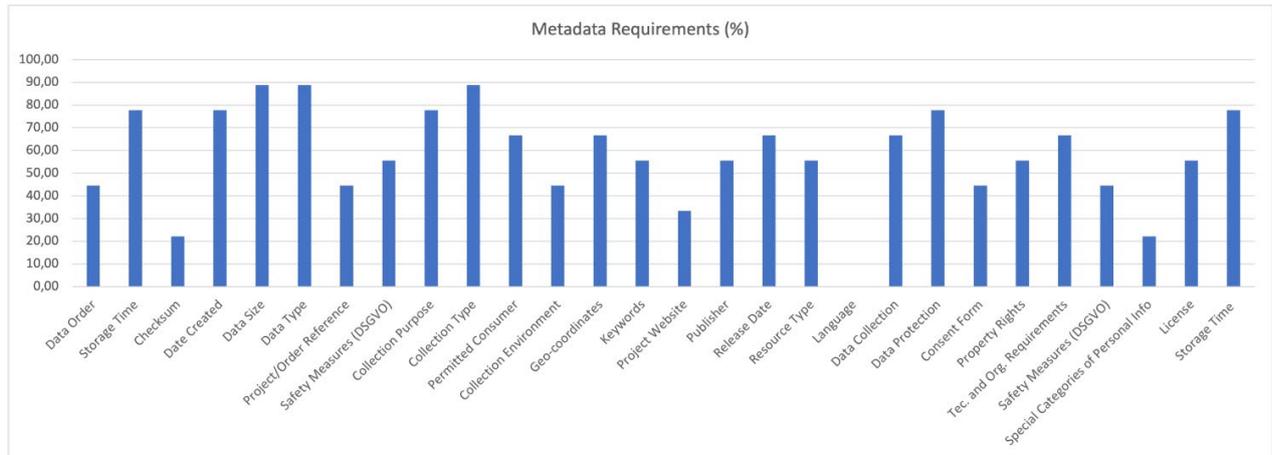
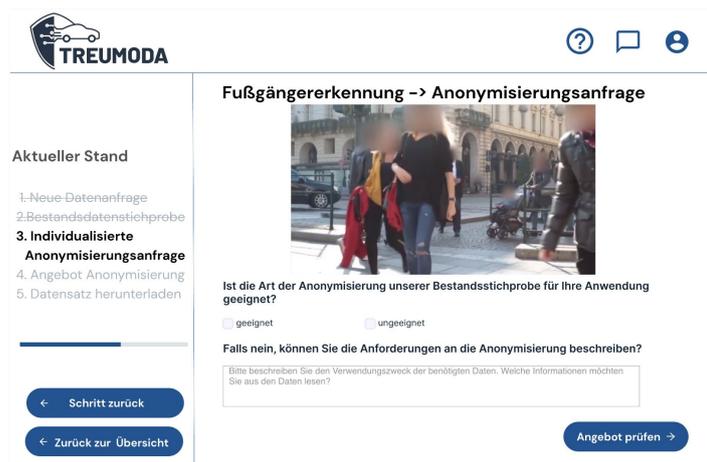


Abbildung 10: Auswertung des Bedarfs an Metadaten aus Erprobung

Abschließend dienten die Stakeholder-Workshops als Teil der formativen Studien für die Softwareentwicklung und die Konzeption des Geschäftsmodells. Durch diese Workshops wurde ein besseres Verständnis für die Anforderungen potenzieller Nutzer gewonnen und die Grundlage für das Treuhandstellen-Service-Modell gelegt. Zusätzlich wurden Prototypen der Web-Benutzeroberfläche für nachfolgende formative Studien und die Realisierung des Projekts zur Verfügung gestellt. Abschließend bestätigt das Feedback zur Vision von TreuMoDa das Potenzial der Plattform.

2.4 Beteiligung des KITs an weiteren Arbeitspaketen

Zusätzlich zu den obengenannten Arbeitspaketen war das KIT maßgeblich auch an dem Arbeitspaket zur Anonymisierung beteiligt, welches vom Forschungszentrum Informatik (FZI) geleitet wurden und im entsprechenden Bericht zum Teilvorhaben ausführlich beschrieben wird.



TREUMODA

Fußgängererkennung -> Anonymisierungsanfrage

Aktueller Stand

1. Neue Datenanfrage
2. Bestandsdatenstichprobe
- 3. Individualisierte Anonymisierungsanfrage**
4. Angebot Anonymisierung
5. Datensatz herunterladen

Ist die Art der Anonymisierung unserer Bestandsstichprobe für Ihre Anwendung geeignet?

geeignet ungeeignet

Falls nein, können Sie die Anforderungen an die Anonymisierung beschreiben?

Bitte beschreiben Sie den Verwendungszweck der benötigten Daten. Welche Informationen möchten Sie aus den Daten lesen?

[← Schritt zurück](#) [← Zurück zur Übersicht](#) [Angebot prüfen →](#)

Abbildung 11: Einbindung der am FZI entwickelten Verfahren in Mockup

Die relevanten Ergebnisse des KITs hier beziehen sich insbesondere auf die Erprobung und prototypischen Umsetzung der Ergebnisse in AP3 (siehe Abschnitt zur Erprobung). Insbesondere hat das

KIT hierzu einen prototypischen Anwendungsfall zur Anonymisierung von GPS-Traces implementiert der innerhalb der Workshops erprobt wurde.

Hierzu hat das KIT (teilweise im Rahmen einer Bachelorarbeit) aus offenen anonymisierten Daten auf Basis hypothetischer Personen synthetisch einen personenbezogenen Datensatz erstellt, der wiederum unter Nutzung der vorgegebene Anonymisierung auf den anonymisierten Datensatz deterministisch abbildbar ist. Hierdurch konnte ein Vergleich von Anonymisierungen durchgeführt werden ohne Datensubjekte zu gefährden.

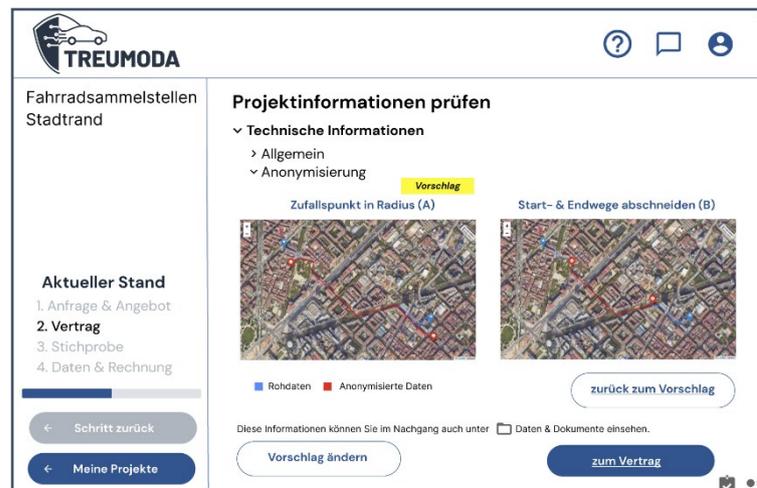


Abbildung 12: Anonymisierung tracebasierter Daten

Für die Mockups wurden hier mehrere bekannte Anonymisierungsmethoden umgesetzt und mit der Zielgruppe innerhalb eines Szenarios in Bezug auf den verbleibenden Wert der Daten evaluiert.

Innerhalb von AP5, welches vom Leibniz Institut für Informationsinfrastruktur (FIZ Karlsruhe) geleitet wurde hat sich KIT mit den technischen Ergebnissen aus AP1-4 eingebracht, um eine rechtliche Folgenabschätzung zu begleiten. Gerade im Bereich der Governance fand die Abstimmung in engen Iterationsschritten mit den Rechtsexperten von FIZ und FZI statt. Insbesondere mit dem FIZ fanden hierzu wöchentliche Abstimmungstreffen statt, die insbesondere sich in den bereits dargestellten Ergebnissen zu AP1 widerspiegeln.

3 Die wichtigsten Positionen des zahlenmäßigen Nachweises

Die finanziellen Mittel im Umfang von ca. 474 T€ wurden wie beantragt im Projektzeitraum für Personal zur Bearbeitung der obengenannten Arbeiten am KIT innerhalb des Förderprojektes ausgegeben.

Es wurde für keine weiteren Kostenpositionen Förderung beantragt.

4 Die Notwendigkeit und Angemessenheit der geleisteten Projektarbeit

Die geleisteten Arbeiten waren zur Erreichung der Projektziele, d. h. zur Konzeptionierung der Treuhandstelle, notwendig. Der Bedarf für einer Treuhandstelle wurde während Projektlaufzeit bestätigt.

Anwender der Treuhandstelle kommen aus dem Bereichen Forschung, Wirtschaft und öffentlichen Behörden und sind schon Teil der Interessensgruppe (assoziierte Partner). Eine Treuhandstelle, wie sie in diesem Projekt entworfen wird, entlastet die Kunden in der Herausforderung der Anonymisierung bei gleichzeitigem Informationserhalt.

5 Nutzen und Verwertbarkeit des Ergebnisses

Innerhalb des Projektes wurde für die Treuhandstelle für Mobilitätsdaten ein Gesamtkonzept entworfen, welches darauf abzielt, das Projektergebnis in Form eines Konzeptes tatsächlich umzusetzen. Das entstandene Geschäftsmodell kann für eine Etablierung der Treuhandstelle genutzt werden. Zu jedem Angebot der Treuhandstelle wurde ein Prozess modelliert, welcher die genaue Reihenfolge in der Abwicklung des Angebots aus organisatorischen, rechtlichen und technischen Aspekten definiert.

Für die Errichtung einer Treuhandstelle für Mobilitätsdaten sind nach diesem Konzept noch weitere Arbeiten nötig, wie beispielsweise die Ausgestaltung der Verträge und die Implementation der technischen Infrastruktur.

Das KIT ist an der Einrichtung einer Treuhandstelle interessiert. Es hat sich während des Projektes gezeigt, dass ein breiterer Fokus (z. B. Technikdaten allgemein) wahrscheinlich notwendig ist, um eine wirtschaftliche Umsetzung zu ermöglichen. Gerade durch den Data Governance Act (DGA) kann hierzu die Gründung einer neuen vom KIT rechtlich abgegrenzten Stelle notwendig sein, die angemeldet werden müsste. Hierzu sind jedoch momentan in Deutschland noch nicht alle Rahmenbedingungen klar.

Das KIT verfolgt die im Projekt verfolgten Ziele werden in anderen Vorhaben (z. B. der Datenplattform der KI-Allianz Baden-Württemberg) abgewandelt weiterverfolgt. Weiterhin bemüht sich das KIT um weitere Fördermittel, die zu einer Umsetzung der Konzepte durch das KIT notwendig wären.

Insgesamt sehen wir auf Basis der Ergebnisse des Projektes und des Feedbacks der befragten Stakeholder ein hohes Verwertungspotential für die entwickelten Angebote.

6 Fortschritte auf dem Gebiet des Vorhabens

Der obengenannte europäische Data Governance Act (DGA) erlangte im Juni 22 Gesetzeskraft und ist seit September 23 gültig. Damit kann das Projektkonsortium den DGA als gültige Rechtsgrundlage in der Bearbeitung des Projektes betrachten.

7 Veröffentlichungen der Ergebnisse

Czech, A. Data Trust Model in Research and Economy: Conceptual Design of a Mobility Data Trustee (TMD). Presentation at the Improving Discovery and Collaboration in Open Science Final TRIPLE Conference. 1-3 February 2023 in Bonn. <https://doi.org/10.5445/IR/1000155828>.

Czech, Andreas, Vivien Geenen, Constantin Breß, Marija Turkovic Popovski, Peter Krauß, Till Riedel, und Frank Gauterin. „Designing a Mobility Data Trustee (MDT): Findings From a Multi-Disciplinary Analysis of Requirements of an MDT“. *Proceedings of the Conference on Research Data Infrastructure* 1 (7. September 2023). <https://doi.org/10.52825/cordi.v1i.370>.

Geenen, Vivien, und Till Riedel. „Consensual videos of potentially re-identifiable individuals recorded at the Autonomous Driving Test Area Baden-Württemberg (raw images with location and IMU data)“. Zenodo, 6. April 2023. <https://doi.org/10.5281/ZENODO.7805961>.

Vivien Geenen, und Till Riedel. „Consensual videos of potentially re-identifiable individuals recorded at the Autonomous Driving Test Area Baden-Württemberg (raw images recorded daytime)“. Zenodo, 19. Oktober 2023. <https://doi.org/10.5281/ZENODO.10020644>.

Geenen, Vivien. „TreuMoDa – Treuhandstelle für Mobilitätsdaten : Projekt und Konzeptvorstellung“. Vortrag. Berlin, 30. Juni 2023. https://stiftungdatenschutz.org/fileadmin/Redaktion/DatenTag/Daten-Tag_Datentreuhand_30062023/Praesentationen/Vivien%20Geenen_ChancenDatentreuhaender_TreuMoDa_v02.pdf.

Gitlab-Repository der im Projekt entwickelten BPMN-Prozesse:
<https://gitlab.kit.edu/kit/treumoda/treumoda-prozesse>
<https://doi.org/10.5281/zenodo.12541158>

Gitlab-Repository der im Projekt entworfenen Mockups:
<https://gitlab.kit.edu/kit/treumoda/mockups>
<https://doi.org/10.5281/zenodo.12541246>

Literaturverzeichnis

Wohllebe, Atilla (Hg.) (2022): Geschäftsmodelle systematisch analysieren. Wiesbaden: Springer Fachmedien Wiesbaden.