Bundesministerium
für Bildung
und Forschung

TRANSIT
DATA TRUSTS FOR LOGISTICS

Schlussbericht zum Verbundprojekt TRANSIT

Teil 1 – Kurzbericht

Zuwendungsempfänger:	Förderkennzeichen:
Universität Leipzig, Institut für Wirtschaftsinformatik **Grimmaische Straße 12, 04109 Leipzig**	**16DTM109A**
Vorhabenbezeichnung: **TRANSIT - Data Trusts for Enhancing Logistics Collaboration** **Teilvorhaben:** Entwicklung eines Konzepts zur Umsetzung eines Datentreuhandmodells	
Laufzeit des Vorhabens: **01.01.2022 bis 30.06.2024**	
Berichtszeitraum: **01.01.2022 bis 30.06.2024**	

UNIVERSITÄT
LEIPZIG

1 Ursprüngliche Aufgabenstellung

Im Verbundprojekt TRANSIT sollten Konzepte für den Einsatz von Datentreuhandmodellen in der Logistik entwickelt und evaluiert werden, um die Effizienz der Branche zu steigern. Ziel sollte es sein, den Akquisitionsprozess von Transportaufträgen zu optimieren, Leerfahrten zu reduzieren und Synergien zwischen Logistikunternehmen (insbesondere KMU) durch stärkere Kollaborationen zu fördern. TRANSIT verfolgte dabei fünf Ziele:

Ziel 1 - Entwicklung eines Konzepts zur Umsetzung eines Datentreuhandmodells für den Datenaustausch zwischen Logistikdienstleistern

Ziel 2 - Erstellung, Erprobung und Evaluierung von Anwendungsszenarien

Ziel 3 - Aufbau einer prototypischen Datentreuhand-Plattform

Ziel 4 - Erarbeitung von Geschäftsmodellen für die TRANSIT Plattform

Ziel 5 - Beschreibung vertrauensaufbauender Maßnahmen

Zur Erreichung der angestrebten wissenschaftlich-technischen Arbeitsziele wurden dem Gesamtvorhaben die folgenden Teilvorhaben zugeordnet:

Teilvorhaben	Partner
Entwicklung eines Konzepts zur Umsetzung eines Datentreuhandmodells	Universität Leipzig - Institut für Wirtschaftsinformatik
Konzeption und Entwicklung der TRANSIT-Plattform	Institut für Angewandte Informatik e.V.
Anforderungsszenarien und praktische Erprobung (TRUSTFOX)	fox-COURIER GmbH

Es erfolgte eine Zusammenarbeit mit dem Netzwerk Logistik Mitteldeutschland e.V. als assoziierter Partner.

2 Ursprünglicher Wissenschaftlicher / Technischer Stand

Es existieren zahlreiche Kollaborationsplattformen, die Logistikunternehmen bei der Digitalisierung und Optimierung ihrer Prozesse unterstützen. Der Schwerpunkt dieser Plattformen liegt häufig auf der technischen Integration des Datenaustauschs und der Verbesserung logistischer Abläufe. Neben diesen grundlegenden Funktionen bieten einige Plattformbetreiber erweiterte Dienste an, wie die Abwicklung des gesamten Transportprozesses im Rahmen eines sogenannten Fourth-Party-Logistics-Providers (4PL). Diese Anbieter übernehmen nicht nur die Koordination, sondern auch die operative Umsetzung von Transportdienstleistungen, was insbesondere für kleinere Logistikunternehmen von Vorteil sein kann. Unabhängig von den angebotenen Funktionen bleibt jedoch eine zentrale Herausforderung bestehen: Die Teilnahme an solchen Plattformen erfordert die Weitergabe sensibler Geschäfts- und Prozessdaten an Dritte. Diese Dritten sind in der Regel private, gewinnorientierte Anbieter, die die Plattformen betreiben. Dadurch entsteht ein Spannungsfeld zwischen der Notwendigkeit zur Kooperation und den Risiken durch die Preisgabe unternehmenskritischer Informationen. Zudem spielt der Schutz dieser Daten häufig eine untergeordnete Rolle. Datenschutzgrundsätze wie die Wahrung der Datenhoheit, die Minimierung der erhobenen und verarbeiteten Datenmengen oder transparente Regelungen zum Datenzugriff und -gebrauch werden selten konsequent umgesetzt. Solche Hemmnisse erschweren es vielen Unternehmen, den vollen Nutzen aus der Kollaboration über diese Plattformen zu ziehen.

3 Planung und Ablauf des Vorhabens

Für die Erarbeitung der Projektergebnisse folgte TRANSIT dem Spiralmodell. Der Arbeitsplan gliederte sich in sechs Arbeitspakete mit den jeweiligen Meilensteinen (M), die sich über die Projektlaufzeit von **01.01.2022 – 30.06.2024** wie folgt erstreckten:

Arbeitspakete (AP)		**1. Jahr**				**2. Jahr**				**3. Jahr**	
		I	II	III	IV	I	II	III	IV	I	II
AP1	Anforderungsanalyse und Evaluation		M 1.1				M 1.2				M 1.3
AP2	Rechte- und Datenmanagement			M 2.1				M 2.2			M 2.3
AP3	Datentreuhandmodelle					M 3.1				M 3.2	
AP4	Plattformentwicklung					M 4.1				M 4.2	
AP5	Datengetriebene Dienstleistungen & Geschäftsmodelle									M 5.1	
AP6	Verbreitung / Verwertung										

4 Wesentliche Ergebnisse

Im Vorhaben TRANSIT wurde ein umfassendes Kooperationsmodell für Logistikunternehmen erarbeitet, das die Potenziale einer datentreuhandgestützten Datenverarbeitung ausschöpft. Im Mittelpunkt steht ein innovativer Ansatz, bei dem ein Datentreuhänder als neutraler Vermittler zwischen den Unternehmen agiert. Dieser B2B-Intermediär schafft die Grundlage für einen sicheren und vertrauenswürdigen Austausch sensibler Geschäftsprozessdaten, die bisher aus Sorge vor Datenmissbrauch oder Wettbewerbsnachteilen nur selten geteilt werden. Ein entscheidender Vorteil des TRANSIT-Datentreuhandmodells ist die Möglichkeit, Daten wie Ladekapazitäten, Lieferbeziehungen oder Transportdetails unter Wahrung der Datenhoheit der beteiligten Unternehmen auszutauschen. Der Datentreuhänder fungiert hierbei als neutrale Instanz, die sicherstellt, dass Daten nur für die vorgesehenen Zwecke genutzt werden und dabei die Interessen aller Beteiligten geschützt bleiben. Dies schafft die Voraussetzung für eine intensivere und effizientere Zusammenarbeit zwischen den Akteuren der Logistikbranche, insbesondere in einem dynamischen Marktumfeld mit häufig wechselnden Partnern und hohen Anforderungen an Flexibilität und Transparenz. Im Rahmen von TRANSIT wurden nicht nur die technischen Grundlagen für dieses Modell entwickelt, sondern auch umfangreiche Geschäfts- und Betriebsmodelle, die die praktische Umsetzung eines solchen Datentreuhandansatzes ermöglichen. Zentrales Ergebnis ist die TRANSIT-Plattform, die prototypisch umgesetzt wurde und bereits eine konkrete Anwendung des Modells darstellt. Diese Plattform wurde in enger Zusammenarbeit mit Anwendern aus der Logistikbranche entwickelt, um sicherzustellen, dass sie den realen Anforderungen und Bedürfnissen gerecht wird. Die TRANSIT-Plattform bietet Logistikdienstleistern die Möglichkeit, Lieferaufträge mit anderen Partnern zu teilen und dabei die Kontrolle über ihre Daten zu behalten. Die Plattform verbindet technologische Innovation mit einem hohen Maß an Datensicherheit und ermöglicht so eine neue Qualität der Kooperation. Durch die Kombination von Vertrauen, Sicherheit und Effizienz adressiert das TRANSIT-Datentreuhandmodell zentrale Herausforderungen der Logistikbranche und zeigt auf, wie digitale Technologien und innovative Geschäftsmodelle zur Verbesserung der gesamten Wertschöpfungskette beitragen können. Die Plattform bietet nicht nur eine praktische Lösung für aktuelle Probleme, sondern auch ein zukunftsweisendes Konzept für die weitergehende Digitalisierung und Vernetzung der Logistik.

Bundesministerium
für Bildung
und Forschung

TRANSIT
DATA TRUSTS FOR LOGISTICS

Schlussbericht zum Verbundprojekt TRANSIT

Teil 2 – Ausführlicher Bericht

Zuwendungsempfänger: **Universität Leipzig, Institut für Wirtschaftsinformatik** **Grimmaische Straße 12, 04109 Leipzig**	Förderkennzeichen: **16DTM109A**
Autoren Sascha Kober, Silvia Torres Landaverde, Benjamin Gaunitz	
Vorhabenbezeichnung: *Verbundvorhaben:* **TRANSIT - Data Trusts for Enhancing Logistics Collaboration** Teilvorhaben: Entwicklung eines Konzepts zur Umsetzung eines Datentreuhandmodells	
Laufzeit des Vorhabens: **01.01.2022 bis 30.06.2024**	
Berichtszeitraum: **01.01.2022 bis 30.06.2024**	

UNIVERSITÄT LEIPZIG

InfAI
Institut für Angewandte Informatik

FOX COURIER

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Ergebnisse

1.1 Rechte- und Datenmanagement

In enger Zusammenarbeit mit dem Praxispartner FOX und durch umfassende Literatur- und Studienrecherchen wurden verschiedene rechtliche Gesetze und Verpflichtungen identifiziert, die für Betreiber von Webplattformen und insbesondere für Datentreuhänder von entscheidender Bedeutung sind. Basierend auf diesen Anforderungen wurde ein Datenmanagement-System entwickelt, das in einem iterativen Prozess gemeinsam mit der Rechtsabteilung des InfAI erstellt und unter Berücksichtigung weiterer Recherchen jährlich aktualisiert wird. Diese Kooperation und das systematische Vorgehen tragen dazu bei, die Einhaltung relevanter rechtlicher Rahmenbedingungen sicherzustellen und gleichzeitig die Datenintegrität und -sicherheit zu gewährleisten.

1.1.1 Relevante Gesetzgebungen

Die Identifizierung relevanter Gesetzgebungen erfolgte durch eine systematische Analyse der rechtlichen Anforderungen, die an Betreiber von Datenplattformen gestellt werden. Hierbei wurden insbesondere folgende Gesetze als besonders relevant eingestuft:

Datenschutz-Grundverordnung (DSGVO): Die DSGVO ist das zentrale rechtliche Rahmenwerk in der Europäischen Union, das die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen regelt. Sie zielt darauf ab, die Grundrechte und Freiheiten natürlicher Personen zu schützen und den freien Datenverkehr innerhalb des Europäischen Wirtschaftsraums zu gewährleisten.

Bundesdatenschutzgesetz (BDSG-neu): Das BDSG-neu dient der Anpassung des nationalen Datenschutzrechts an die Vorgaben der DSGVO und ergänzt diese um spezifische nationale Regelungen, wie beispielsweise die Datenverarbeitung im Beschäftigungsverhältnis und die Bestellung von Datenschutzbeauftragten.

Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG): Dieses Gesetz regelt spezifische Datenschutzfragen in den Bereichen Telekommunikation und Telemedien. Es adressiert insbesondere die Anforderungen an die Einwilligung zur Nutzung von Cookies und ähnlichen Technologien sowie den Datenschutz bei der Nutzung von elektronischen Kommunikationsdiensten.

Geschäftsgeheimnisgesetz (GeschGehG): Das GeschGehG schützt Informationen, die als Geschäftsgeheimnisse klassifiziert sind, vor unerlaubter Erlangung, Nutzung und Offenlegung. Es setzt die EU-Richtlinie über den Schutz vertraulicher Geschäftsinformationen um.

Data Governance Act (DGA): Der DGA ist ein relativ neues Gesetz, das darauf abzielt, die Bedingungen für den Zugang zu und die Wiederverwendung von Daten innerhalb der EU zu regeln. Er ist besonders relevant für Datentreuhänder, da er Rahmenbedingungen für die datengetriebene Wirtschaft und die Nutzung von Daten für gesellschaftliche und wirtschaftliche Zwecke festlegt.

1.1.2 Umsetzung der gesetzlichen Anforderungen

Die Umsetzung der gesetzlichen Anforderungen erfordert ein robustes Datenmanagement-System, das nicht nur die Einhaltung dieser Gesetze gewährleistet, sondern auch die Sicherheit, Integrität und Vertraulichkeit der verarbeiteten Daten sichert. Folgende Prinzipien wurden dabei besonders berücksichtigt:

Datenschutz: Einhaltung aller relevanten Datenschutzgesetze und -verordnungen, insbesondere der DSGVO. Dies beinhaltet Maßnahmen zur Datensicherheit, Transparenz der Datenverarbeitung und Sicherstellung der Vertraulichkeit der Daten.

Datensicherheit: Implementierung geeigneter technischer und organisatorischer Maßnahmen, um Daten vor unbefugtem Zugriff und Missbrauch zu schützen.

Vertraulichkeit und Transparenz: Gewährleistung, dass Daten nur für die festgelegten Zwecke verwendet und dass die Verarbeitungsaktivitäten klar und verständlich für die betroffenen Personen kommuniziert werden.

Zweckbindung und Minimierung: Verarbeitung der Daten ausschließlich für explizit definierte und legitime Zwecke sowie Reduzierung der verarbeiteten Daten auf das für die jeweiligen Zwecke notwendige Minimum.

Trotz der umfassenden Initialanalyse und der Etablierung eines fundierten rechtlichen Rahmens bleiben Herausforderungen bestehen, insbesondere im Hinblick auf die dynamische Natur der digitalen Datenwirtschaft und die kontinuierliche Weiterentwicklung der rechtlichen Landschaft. Aus diesem Grund ist die regelmäßige Überprüfung und Anpassung des Datenmanagement-Systems unerlässlich. Die jährliche Überarbeitung des Systems erfolgt in Zusammenarbeit mit der Rechtsabteilung des InfAI und unter Einbeziehung der neuesten rechtlichen Entwicklungen und technologischen Fortschritte. Diese iterative Vorgehensweise ermöglicht eine flexible Reaktion auf neue Anforderungen und Herausforderungen, die sich aus der praktischen Anwendung des Datenmanagements und aus Veränderungen im rechtlichen Umfeld ergeben. Die kooperative und proaktive Herangehensweise bei der Entwicklung und Pflege des Datenmanagement-Systems stellt sicher, dass nicht nur aktuelle rechtliche Anforderungen erfüllt werden, sondern auch eine solide Grundlage für zukünftige Entwicklungen und Herausforderungen geschaffen wird. Die Einbindung von Expertenwissen und die regelmäßige Aktualisierung sind entscheidend, um die Integrität und Sicherheit der Datenplattformen im Einklang mit den rechtlichen Vorgaben zu gewährleisten.

Erstellung Erstversion Datenmanagementkonzept

Als Datentreuhänder ist es wichtig, sensible Daten sicher zu verwalten und zu schützen. Um dies umzusetzen bedarf es folgender Schritte:

Nr.	Schritte der Datenverwaltung	Kurzbeschreibung
1	Identifikation der Daten	Alle zu verwaltenden Daten identifizieren, z.B. Name, Adresse, Telefonnummer, E-Mail-Adresse, Sozialversicherungsnummer etc.
2	Klassifizierung der Daten	Daten je nach Art und Sensibilität in verschiedene Kategorien einteilen, um Sicherheitsstufe anzuwenden.
3	Speicherung der Daten	Entscheiden, wo die Daten gespeichert werden sollen, z.B. eigene IT-Infrastruktur oder Cloud.
4	Zugriffsverwaltung	Nur autorisierte Personen Zugriff auf gespeicherte Daten gewähren, z.B. mit Passwörtern, Multi-Faktor-Authentifizierung oder Rollenbasierte Zugriffssteuerung.
5	Datenweitergabe	Bedingungen für Datenweitergabe in einem Vertrag regeln, z.B. Zweck, Art der Daten, Sicherheitsvorkehrungen, Haftungsfragen.
6	Überwachung und Wartung	Regelmäßige Prüfung, ob Datenverwaltung den gesetzlichen Anforderungen entspricht und Überwachung der Datenintegrität, -verfügbarkeit und -sicherheit.
7	Datenvernichtung	Daten ordnungsgemäß vernichten, z.B. alle Kopien und Backups löschen und Daten unlesbar machen, um Wiederherstellung zu verhindern.

Tabelle 1: Schritte eines effektiven Datenmanagementkonzepts

Es sollen im Rahmen des Datentreuhänders Geschäftsprozessdaten des Logistikers verwaltet werden wozu Auftragsdaten, Fahrzeugdaten und Personen/Mitarbeiterdaten gehören, Firmendaten. Da für die Kollaboration zwischen Unternehmen primär Auftragsdaten erforderlich sind, werden diese in der Datentreuhandplattform einen großen Stellenwert haben. Dazu gehören Adressen, Wareneigenschaften, Abhol- /Anlieferungszeiten, Beträge für die Aufträge, Infos zu Lagerhäusern und Fahrzeugen (Zuordnung). Des Weiteren müssen auch einige Personendaten gespeichert werden, welche für den reibungslosen Ablauf der Plattform erforderlich sind. Dazu werden für die Anmeldung Vor und Zuname, Email sowie die Zugehörigkeit zu einer Firma erfasst. Weiter sind bestimmte Firmendaten erforderlich, welche für alle Teilnehmer der Plattform einsehbar sind, wie Hauptanschrift, Name der Firma, Ansprechpartner, teilweise das Liefergebiet. Zu den sensibelsten Daten, den personenbezogenen, gehören alle direkt mit einer Person in Beziehung stehenden Werte wie Namen und Email, sowie die Rolle in der Firma, sowie welche Firma. Die gesamten Auftragsdaten fallen unter das Geschäftsgeheimnisgesetz, sind somit auch sensibel. Dazu gehören zum Beispiel Preis, Paketdaten, verantwortlicher Fahrer, Strecke. Die dritte Kategorie der Firmendaten ist am unsensibelsten, da dadurch erst eine Firma aufgefunden werden kann, also Firmenname, Hauptanschrift oder auch das Liefergebiet. Die Speicherung der Daten soll auf der eigenen IT-Infrastruktur der Universität Leipzig stattfinden, was auch eine vertrauensfördernde Maßnahme ist. Des Weiteren muss ein regelmäßiges Backup der Daten eingerichtet werden, um gegen Ausfälle vorzubeugen. Auch soll ein containerisierter Ansatz gewählt werden, da somit auch eine Skalierung der Anwendungen und der Datenbank einfach möglich sind. Ein weiterer Vorteil der zentralen Speicherung sind die hohe Verfügbarkeit und der große Durchsatz der Daten, wenn dies an einer Universität gehostet wird. Um die Datenspeicherung von Geo-Daten zu ermöglichen wird einerseits auf die Datenbank PostGIS gesetzt, sowie die Möglichkeit diese in einen Clusterverbund zu skalieren in Betracht gezogen.

Der Zugriff auf die Daten soll in erster Linie nur auf die eigenen Firmendaten möglich sein, indem diese virtuell getrennt werden. Um auf eine Entität zuzugreifen, muss für einen Nutzer die Rolle innerhalb der Firma, sowie die Firmen-ID als Zugriffentscheidung genutzt werden. Also eine Kombination aus ABAC und RBAC. Das Datenteilen sollen dann nur speziell autorisierte Nutzer einer Firma mit entsprechender Rolle durchführen können. Anschließend werden nur die freigegeben Daten einer Entität, im Weiteren die Eigenschaften einer Entität, freigegeben, sodass diese Daten innerhalb der zweiten Firma lesbar sind, wenn die entsprechende Person die richtige Rolle innehat. Für die Anmeldung soll eine Passwortrichtlinie erstellt werden, sowie der Zugriff auf die Plattform erst gewährt werden, wenn die E-Mail-Adresse verifiziert wurde. Bisher ist es nicht erforderlich und gewünscht die Daten an Dritte weiterzugeben. Ansätze mit Anonymisierung oder Pseudonymisierung könnten weiter betrachtet werden.

Ehe eine neue Version in das produktive System überführt wird, müssen Überprüfungen stattfinden, inwiefern der entsprechend programmierte Code auch die richtigen Funktionalitäten aufweist, was z.B. mit Unit-Tests oder Integration-Tests durchgeführt wird. Des Weiteren ist es erforderlich die Funktionalität regelmäßig im Livesystem auszutesten, inwiefern an einer Stelle unvorhersehbare Lücken oder Funktionsfehler auftreten. Zudem soll ein gesetzeskonformes Zugriffsprotokoll angelegt werden, mit welchen in zukünftigen Arbeiten Kompromittierungen durch Intrusion-Detection erkannt und eliminiert werden können.

An dieser Stelle ist es im Rahmen des Rechteworkshops zu klären ob die Daten komplett vernichtet oder eine vollständige Anonymisierung der Daten ausreicht. Im ersten Schritt soll es ermöglicht werden, dass der Nutzer seinen Account komplett löschen kann. Hierbei ist zu prüfen, welche abhängigen Daten mit gelöscht werden können und dürfen und welche z.B. erstellte Aufträge einer Firma umfassen.

1.1.3 Analyse / Evaluation / Anpassung rechtlicher Anforderungen

Im Abschnitt AP 2.3 wird die Analyse und Evaluation der rechtlichen Anforderungen sowie die Anpassung dieser Anforderungen für die Umsetzung eines Datentreuhänders behandelt. Hierbei steht die Einhaltung der rechtlichen Vorgaben im Vordergrund, insbesondere die der Datenschutz-Grundverordnung (DSGVO), die spezifischen Anforderungen an die Verarbeitung personenbezogener Daten durch Datentreuhänder stellt.

Hauptpunkte der rechtlichen Anforderungen

Auftragsverarbeitungsvertrag (AVV): Gemäß Artikel 28 DSGVO muss zwischen dem Datenverantwortlichen und dem Datentreuhänder ein schriftlicher Vertrag existieren, der detailliert die Verarbeitungszwecke, Datentypen sowie die Rechte und Pflichten beider Parteien beschreibt.

Datensicherheit: Der Datentreuhänder ist verpflichtet, angemessene technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit der Daten zu gewährleisten, einschließlich der Verschlüsselung sensibler Daten.

Datenschutz durch Technikgestaltung: Artikel 25 DSGVO fordert, dass Datenschutz von Anfang an in die Technikgestaltung einfließt und dass Systeme standardmäßig auf Datensparsamkeit und Transparenz ausgerichtet sind.

Meldepflicht bei Datenschutzverletzungen: Der Datentreuhänder muss Datenschutzverletzungen umgehend nach Kenntnisnahme melden.

Zusammenarbeit mit Aufsichtsbehörden: Bei Anfragen oder Untersuchungen muss der Datentreuhänder kooperativ mit den Datenschutzbehörden zusammenarbeiten.

Datenweitergabe an Dritte: Jegliche Weitergabe von Daten muss im Einklang mit den Anweisungen des Verantwortlichen und den Bestimmungen der DSGVO stehen.

Datenübertragung in Drittländer: Bei einer Übertragung in Drittländer muss ein angemessenes Datenschutzniveau sichergestellt sein.

Zusätzliche rechtliche Regelungen

DATA Act (USA): Dieses Gesetz verbessert die Transparenz und Rechenschaftspflicht der US-Bundesregierung bezüglich Finanzdaten. Obwohl es die Verwaltung von Finanzdaten in den USA regelt, ist es nicht direkt auf Datentreuhänder in der EU anwendbar.

EU Data Act: Diese Verordnung regelt den fairen Datenzugang und die Datennutzung in der EU und umfasst Vorschriften zur Datenweitergabe zwischen Unternehmen und Verbrauchern, die Pflichten der Dateninhaber und das Verbot missbräuchlicher Vertragsklauseln.

Evaluation und Anpassung der rechtlichen Anforderungen

Die Evaluation der rechtlichen Anforderungen konzentriert sich auf die Analyse, wie die TRANSIT-Plattform die Vorschriften der DSGVO umsetzt, insbesondere im Hinblick auf die Verarbeitung von Geschäftsprozessdaten und personenbezogenen Daten. Wesentliche Aspekte sind:

Art der verarbeiteten Daten: Es werden Geschäftsprozessdaten und personenbezogene Informationen wie Kontaktdaten verarbeitet.

Datensparsamkeit und Transparenz: Es muss sichergestellt sein, dass nur notwendige Daten gesammelt und die Nutzer über die Datenverarbeitung informiert werden.

Sicherheitsmaßnahmen: Angemessene Maßnahmen müssen implementiert werden, um Daten vor unbefugtem Zugriff und Missbrauch zu schützen.

Rechte der betroffenen Personen: Mechanismen zur Ausübung der DSGVO-Rechte müssen vorhanden sein.

Auftragsverarbeitungsvertrag: Notwendigkeit eines AVVs, falls die Plattform als Auftragsverarbeiter fungiert.

Die Einhaltung der rechtlichen Anforderungen wird durch regelmäßige Überprüfungen und Anpassungen gewährleistet, um die Datenschutzkonformität stets nach dem neuesten Stand der Technik zu halten. Zusätzlich wird die Relevanz weiterer Gesetzgebungen wie des AI Acts in Bezug auf die Nutzung künstlicher Intelligenz evaluiert, um zukünftige Anforderungen proaktiv zu integrieren.

Definition von Freigabestufen und Zugriffspolicies für Geschäftsprozessdaten

Die TRANSIT-Plattform implementiert umfassende Freigabe- und Vertraulichkeitsstufen, um den Anforderungen verschiedener Nutzergruppen gerecht zu werden und die Sicherheit und Integrität der Daten zu gewährleisten. Die Plattform nutzt eine grafische Oberfläche für die Dateneingabe, und Daten werden über eine öffentlich zugängliche Schnittstelle in eine zentrale Datenbank übertragen. Der Zugang zu diesen Daten ist rollenbasiert, wobei jede Rolle spezifische Zugriffsrechte hat, von der globalen Admin-Rolle, die nur eingeschränkte administrative Zugriffe besitzt, bis hin zu spezifischen Rollen wie Fahrern und Lagerarbeitern, die nur eingeschränkten Zugang zu bestimmten Datensätzen haben. Die Rollenvergabe ist klar strukturiert, der Firmenbesitzer kann weitere Besitzer ernennen und besitzt die umfassendsten Rechte zur Rollenvergabe. Ein zugewiesener Firmenadmin kann die übrigen Rollen vergeben und entziehen. Die Plattform beinhaltet auch ein Konzept für Nutzerentitäten, das den firmenübergreifenden Zugriff regelt, indem es bestimmte Paketklassen definiert, die nur vom Betreiber der Plattform bearbeitet werden können, während andere Nutzer diese nur lesen können.

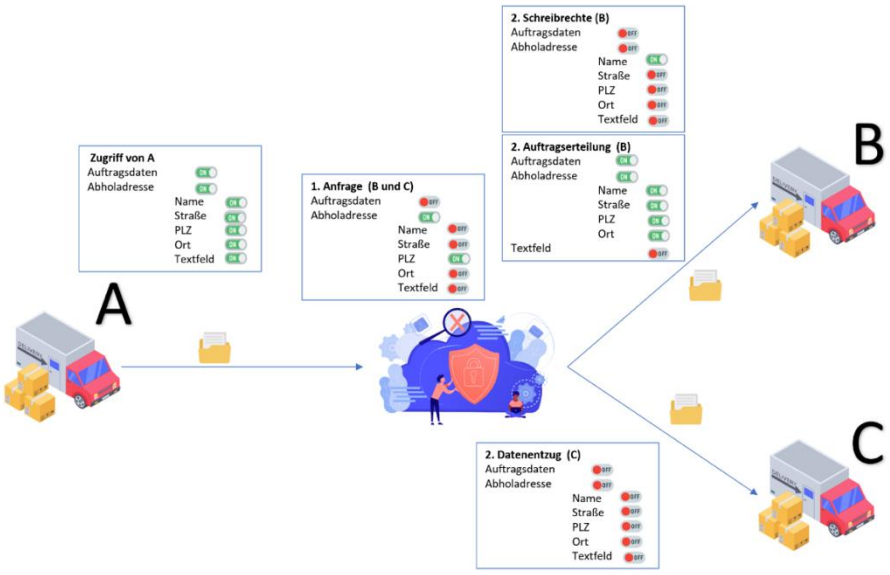

Abbildung 1: Vorgang des Datenteilens und Rechteentzug

Die Datenzugriffsrechte innerhalb einer Firma sind klar definiert, um sicherzustellen, dass nur autorisierte Nutzer die notwendigen Daten bearbeiten oder einsehen können. Ein Beispiel hierfür sind Paketeigenschaften, die nur von bestimmten definierten Nutzern bearbeitet werden dürfen. Dies trägt dazu bei, dass sensitive Informationen innerhalb der Plattform sicher gehandhabt werden und die Datensicherheit durch eine präzise Rollen- und Rechteverwaltung unterstützt wird.

Die TRANSIT-Plattform entwickelt weiterhin ihre Zugriffsregelungen, um neuen Gegebenheiten und Anforderungen gerecht zu werden, wobei der Fokus stets auf der Sicherheit der Daten und der Einfachheit der Nutzung für die Logistiker liegt, ohne dass diese den komplexen technischen Unterbau verstehen müssen. Eine mögliche zukünftige Erweiterung des Freigabekonzeptes könnte die Speicherung und Verwaltung der Lese- und Schreibrechte umfassen, die eine Firma an eine von ihrer beauftragten Firma weitergeben kann (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Analyse / Evaluation rechtlicher Anforderungen und Anpassung der Anforderungen

Im Rahmen der erneuten Analyse und Evaluation gesetzlicher Anforderungen wurden keine neuen Gesetze oder in naher Zukunft gültigen Gesetze gefunden, welche für die Datentreuhandplattform Transit relevant sein könnten. Bezüglich des Datenmanagementkonzeptes wurden weitere Datenfelder dynamisch nach mehreren Evaluationen mit den Praxisanwendern ergänzt, welche unter die Geschäftsgeheimnisse zählen. Zu den Personen bezogenen Daten gibt es keine weiteren welche im Laufe der letzten Evaluation hinzugekommen sind.

Die Compliance mit rechtlichen Vorgaben ist ein fundamentaler Aspekt der Datennutzung und -verarbeitung auf jeder Plattform, die personenbezogene Daten verarbeitet. Für die TRANSIT-Plattform, ist die Einhaltung dieser Vorgaben besonders kritisch, da sie direkt mit sensiblen Transport- und Logistikdaten arbeitet. AP 2.5 fokussiert sich auf die Überprüfung und Anpassung der Plattform an die rechtlichen Anforderungen, die sich aus den Datenschutzgesetzen, insbesondere der DSGVO, sowie anderen relevanten nationalen und internationalen Gesetzen ergeben.

Rechtlicher Rahmen

Die primäre rechtliche Grundlage für die Datenverarbeitung innerhalb der EU ist die Datenschutz-Grundverordnung (DSGVO), die strengen Richtlinien für den Umgang mit personenbezogenen Daten vorschreibt. Zusätzlich gibt es länderspezifische Datenschutzgesetze, die in bestimmten Aspekten von der DSGVO abweichen können. Für die TRANSIT-Plattform ist es essenziell, nicht nur die DSGVO, sondern auch solche spezifischen nationalen Anforderungen zu berücksichtigen. So ist der europäische Data Act auch von großer Wichtigkeit.

Die erneute Analyse umfasste eine detaillierte Prüfung der Plattform hinsichtlich der Einhaltung dieser Datenschutzstandards. Dazu gehörten Aspekte wie die Rechtmäßigkeit der Datenverarbeitung, die Transparenz der Verarbeitungsprozesse, die Datenminimierung, die Sicherstellung der Datenqualität, die Sicherheit der Verarbeitung sowie die Rechte der betroffenen Personen. Weiterhin wurde evaluiert, inwiefern bestehende technische und organisatorische Maßnahmen (TOMs) der Plattform den aktuellen rechtlichen Anforderungen entsprechen. Dazu zählen Verschlüsselungsverfahren, Zugriffskontrollen, Protokollierungsmechanismen und die Schulung der Mitarbeiter in datenschutzrelevanten Themen.

Eine vollständige Analyse des Datenflusses auf der Plattform wurde durchgeführt, um sicherzustellen, dass alle Datentransfers, sowohl intern als auch extern, den rechtlichen Vorgaben entsprechen. Besonderes Augenmerk wurde auf grenzüberschreitende Datenübertragungen gelegt, die zusätzliche rechtliche Herausforderungen darstellen können.

Anpassung des Datenmanagementkonzeptes

Auf Basis der Rückmeldungen der Nutzer wurden zusätzliche Datenfelder, die als Geschäftsgeheimnisse klassifiziert sind, in das Datenmodell aufgenommen. Diese neuen Felder erfordern spezielle Schutzmaßnahmen, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Obwohl keine neuen relevanten Gesetze identifiziert wurden, bleibt die

Plattform vorbereitet, schnell auf zukünftige gesetzliche Änderungen reagieren zu können. Dies beinhaltet die Implementierung eines agilen Datenmanagementkonzepts, das eine schnelle Anpassung an neue rechtliche Anforderungen ermöglicht.

Die Evaluation hat gezeigt, dass die TRANSIT-Plattform größtenteils den aktuellen rechtlichen Anforderungen entspricht. Empfohlen wird jedoch die fortlaufende Überwachung der rechtlichen Landschaft und die regelmäßige Schulung der Mitarbeiter, um das Bewusstsein für Datenschutzfragen kontinuierlich zu stärken. Die in AP 2.5 vorgenommenen rechtlichen Bewertungen und Anpassungen haben direkte Auswirkungen auf AP 2.6. Die Einhaltung der Datenschutzstandards muss sich auch in den Methoden und Prozessen des Datenqualitätsmanagements widerspiegeln. Protokolle zur Datenbereinigung, Validierung und Fehlerbehebung müssen datenschutzkonform gestaltet sein, was eine enge Abstimmung zwischen diesen beiden APs erfordert.

Implementierung Datenqualitätsmanagement

Um die Implementierung des Datenqualitätsmanagements zu dokumentieren, werden die einzelnen Datenbankentitäten betrachtet, sowie wie die Vorgaben des Managements umgesetzt wurden. Um eine gute Qualität von vornherein zu gewährleisten wurde mit FOX in mehreren Workshops als Grundlage ein einheitliches Datenmodell für die Logistik geschaffen, welche die wichtigsten Daten zur Auftragsverwaltung erfasst.

Im Folgenden werden die umgesetzten Anforderungen an die Datenqualität dokumentiert, welche einzelnen Datentypen, bestimmte Entitäten oder auch logische Zusammenhänge innerhalb der Daten umfasst.

Im Allgemeinen wurde sich darauf geeinigt das Kommazahlen in englischer Notation mit Punkt als Kommastelle abgespeichert werden, wobei die Transformation von der API vorgenommen, falls entsprechende Datenfelder abgelegt werden sollen. Hierbei gibt es z.B. auch für die Länge, Breite, Höhe gewisse Mindest- und Maximalvorgaben, um eine Unaufmerksamkeit der Mitarbeiter auszuschließen.

Zahlenfelder dürfen auch im Allgemeinen keine Buchstaben enthalten, somit ist auch keine verkürzte Notation mit „e“ möglich.

Emailadressen, müssen auch ein gewissen Schema folgen um im Frontend bzw. Backend eingebbar zu sein, welches on-the-fly geprüft wird.

In Textfeldern gibt es keine Einschränkungen der Länge da somit gewährleistet ist das beliebig lange Ortsnamen oder Nachrichten eingebeben bzw. zum Informationsfesthaltung bzw. -austauscht verwendbar sind. Sodass aber auch geprüft wird, dass diese nicht leer sind, wurde sich auf eine Mindestlänge von drei Zeichen geeinigt.

Datumsangaben werden Plattform-übergreifend im ISO-8601 Format abgespeichert, um intern sowie mit anderen Systemen um die Interoperabilität zu fördern und Datenverarbeitung zu erleichtern.

Die Entität der Adressen wird für eine Firma über alle Aufträge geteilt, um die Konsistenz dieses Stammdatenteils zu erhalten. In bestimmten Fällen der Auftragsdatenteilung mit unterschiedlichen Freigabenrechten über mehrere Aufträge hinweg, ist es in manchen Fällen erforderlich die Adressen zu kopieren und dem Auftrag zuzuordnen. Diese kopierten Adressen werden nur für die interne Verwaltung der Daten genutzt und bei direktem Abruf gesendet und keinesfalls im Adressverzeichnis doppelt angezeigt.

Für diverse Entitäten wurden auch Pflichtfelder eigeführt, welche minimal ausgefüllt werden müssen, sodass ein Anlegen dieser in der Datenbank möglich ist. Zum Beispiel muss für einen Ansprechpartner einer Firma immer ein Name, Email und eine Telefonnummer erfasst werden.

Um auch die Qualität während der Verarbeitung und Bearbeitung zu gewährleisten wurden auch bestimmte Einschränkungen für deren Bearbeitung getroffen. Dazu zählt zum Bespiel die Änderung des Auftragsstatus. Dieser darf nur auf abgeschlossen gesetzt werden, falls hinterlegt wurde wann und wo die Ware abgeholt und wann und wo die Ware abgegeben wurde.

Des Weiteren gibt es bzgl. der Datenqualität und Übereinstimmung für die Firmen und Pakete spezifische Eigenschaften, welche firmenübergreifend oder plattformübergreifend zum Einsatz kommen, um die Konsistenz der Daten zu erhöhen. Dazu zählen firmenspezifische Daten wie Sendungseigenschaften (z.B. zerbrechlich, Kühlware), welche dann in einer Liste für alle Firmenmitarbeiter beim Anlegen eines Auftrages gleich sind. Plattformübergreifend gibt es Werte wie Sendungsklassen, wozu Palette oder IBC zählen sowie Firmen-Eigenschaften, welche eine Firma charakterisieren, wie Email-Adresse, Telefonnummer.

Basierend auf diesen Definitionen wurden sich die Aufgaben des Qualitätsmanagements genauer betrachtet:

Datenbereinigung: Überprüfung von Dateneingaben mit regulären Ausdrücken und automatisches Abändern von Eingabefehlern, wie Änderung von Komma zu Punkt bei Gleitkommazahlen.

Datenintegration: Durch die Bereitstellung einer API ist es möglich verschiedene Datenquellen an die Datentreuhandplattform anzubinden.

Datenvalidierung: Einmal übermittelte Daten werden zuerst gepaart und dann geprüft, ob sie zu Konsistenzverletzungen in den Daten führen könnten, ehe diese abgespeichert werden (wie am Beispiel des Auftragsstatus beschrieben).

Datenüberwachung: Es werden in regelmäßigen Abstand automatische Prozesse ausgeführt, welche bestimmte Konsistenzprobleme frühzeitig erkennen können. Dazu zählt zum Beispiel, dass eine Adresse nicht gleichzeitig eine Firmen-, Kunden- und Auftragsadresse sein kann, oder eine Adresse mit unterschiedlichen Freigaberegeln an die gleiche Firma zwei verschiedene Adressen sein müssen. Diese Jobs aktualisieren automatisch die gespeicherten Daten sowie die gespeicherten Zugriffsrechte, um die Konsistenz der Daten zu erhalten.

Datenpflege: Die zugänglichen Dashboards und Auswertungen, werden regelmäßig in bestimmten Zeitabständen automatisch aktualisiert, um ein aktuelles Bild der Auftragslage für weitere Entscheidungen einsehbar zu haben.

1.2 Datentreuhandmodelle

1.2.1 Identifikation benötigter Datenquellen und -formate

Im Zuge der Ist-Zustandsanalyse in AP1 wurden die aktuellen Datenquellen und -formate identifiziert und dokumentiert. Auf Basis dieser Ergebnisse wird nun ein Vorgehensmodell zur Bestimmung und Erfassung der Datenquellen und -formate entwickelt. Das Vorgehen umfasst die Analyse des internen Vorgehens sowie nutzbare Plattformen und Programme, die für die Datenverwaltung des Logistikers genutzt werden. Zudem erfolgt eine Analyse der einzelnen Daten, um eine Vereinheitlichung der Metadaten zu ermöglichen. Iterative Anpassungen des Datenmodells sollen eine allgemeingültige Abbildung der erforderlichen Daten liefern.

Im Hinblick auf Weiterentwicklungen und spezielle Spezifikationen können auch externe Quellen und Veröffentlichungen zurate gezogen werden, wie zum Beispiel (Schulz et al. 2020; Bernhard et al. 2007).

Es gibt verschiedene Vorgehensmodelle zur Bestimmung und Erfassung von Datenquellen und -formaten. Hier sind einige Beispiele:

- CRISP-DM (Cross Industry Standard Process for Data Mining)
- KDD (Knowledge Discovery in Databases)
- SEMMA (Sample, Explore, Modify, Model, Assess)
- ASUM-DM (Adaptive System for Unified Mining - Data Mining)

CRISP-DM: CRISP-DM (Cross Industry Standard Process for Data Mining) ist ein weit verbreitetes Vorgehensmodell für Data-Mining-Projekte, das auch für die Bestimmung und Erfassung von Datenquellen und -formaten eingesetzt werden kann. CRISP-DM umfasst sechs Phasen: Verständnis des Problems, Verständnis der Daten, Datenvorbereitung, Modellierung, Bewertung und Bereitstellung.

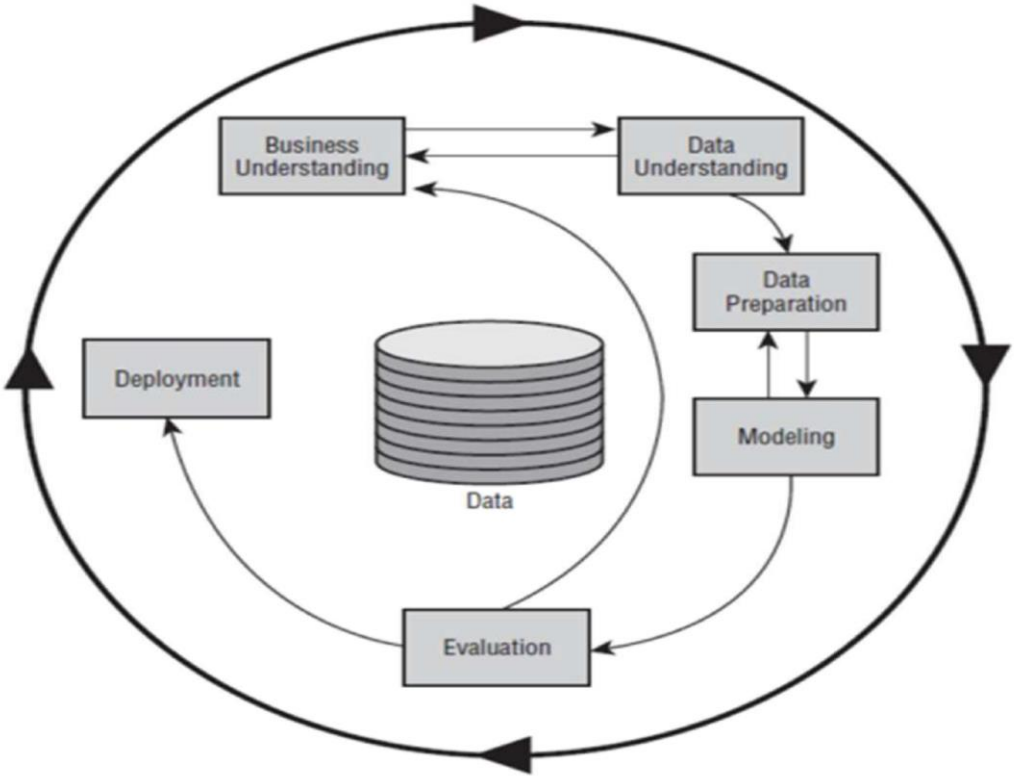

Abbildung 2: CRISPDM Model (Shafique und Qaiser 2014)

KDD ist ein Prozess zur Identifikation von nützlichen Informationen aus Daten. Es umfasst die Phasen Auswahl, Vorverarbeitung, Transformation, Data Mining, Interpretation und Evaluation.

SEMMA ist ein weiteres Vorgehensmodell für Data-Mining-Projekte. Es umfasst fünf Phasen: Stichprobe, Exploration, Modifikation, Modellierung und Bewertung.

Diese Vorgehensmodelle haben unterschiedliche Schwerpunkte und können je nach Anforderungen und Rahmenbedingungen eingesetzt werden. Es ist wichtig, das passende Vorgehensmodell auszuwählen und gegebenenfalls anzupassen, um die gewünschten Ergebnisse zu erzielen.

Data Mining Process Models	KDD	CRISP-DM	SEMMA
No. of Steps	9	6	5
Name of Steps	Developing and Understanding the Application	Business Understanding	----------
	Creating a Target Data Set	Data Understanding	Sample

	Data Cleaning and Pre-processing		Explore
	Data Transformation	Data Preparation	Modify
	Choosing the suitable Data Mining Task	Modeling	Model
	Choosing the suitable Data Mining Algorithm		
	Employing Data Mining Algorithm		
	Interpreting Mining Patterns	Evaluation	Assessment
	Using Discovered Knowledge	Deployment	----------

Abbildung 3: Summary of KDD, CRISP-DM and SEMMA Processes (Shafique und Qaiser 2014)

ASUM-DM (IBM Analytics 2016), ist ein adaptives Data-Mining-System, das verschiedene Data-Mining-Techniken in einem integrierten Framework vereint. Es umfasst fünf Phasen: Analyse, Design, Konfiguration und Herstellung, Inbetriebnahme, Betrieb und Optimierung.

Ein möglicher Vorgehensablauf gemäß ASUM-DM besteht aus den Phasen Analyse, Design, Konfiguration und Herstellung, Inbetriebnahme sowie Betrieb und Optimierung. Durch eine systematische Erfassung und Verwaltung der Datenquellen und -formate können Logistikprozesse optimiert und die Datenauswertung verbessert werden.

Das konkrete Vorgehensmodell zur Bestimmung und Erfassung der Datenquellen und -formate kann je nach Anforderungen und Rahmenbedingungen unterschiedlich aussehen. Ein beispielhafter Ablauf könnte wie folgt aussehen:

Bestandsaufnahme: Eine Bestandsaufnahme der vorhandenen Datenquellen und -formate wird durchgeführt, um einen Überblick über die vorhandenen Daten zu erhalten.

Analyse: Eine Analyse der Datenquellen und -formate wird durchgeführt, um ihre Qualität, Vollständigkeit und Aktualität zu bewerten. Dabei können auch Aspekte wie die Herkunft der Daten, ihre Struktur und ihre Relevanz für die Logistikprozesse berücksichtigt werden.

Auswahl und Bewertung: Auf Basis der Analyseergebnisse werden die relevanten Datenquellen und -formate ausgewählt und bewertet. Hierbei können auch externe Datenquellen wie beispielsweise Marktdaten einbezogen werden.

Vereinheitlichung: Die ausgewählten Datenquellen und -formate werden standardisiert und vereinheitlicht, um eine einheitliche Datengrundlage zu schaffen.

Integration: Die standardisierten Datenquellen und -formate werden in die Datenarchitektur des Unternehmens integriert. Hierbei können auch technische Aspekte wie die Anbindung der Datenquellen an das Datenmanagementsystem berücksichtigt werden.

Test und Validierung: Die integrierten Datenquellen und -formate werden getestet und validiert, um ihre Funktionsfähigkeit und ihre Qualität zu überprüfen.

Dokumentation: Eine Dokumentation der Datenquellen und -formate wird erstellt, um eine Transparenz über die vorhandenen Daten zu schaffen. Hierbei können auch Metadaten wie beispielsweise Beschreibungen der Datenquellen oder ihre Verwendungszwecke erfasst werden.

Wartung und Pflege: Die Datenquellen und -formate werden regelmäßig gewartet und gepflegt, um ihre Aktualität und Qualität sicherzustellen. Hierbei können auch Aspekte wie die Überwachung von Datenqualität oder die Aktualisierung von Datenquellen berücksichtigt werden.

Das Vorgehensmodell kann iterativ gestaltet werden, sodass eine kontinuierliche Verbesserung und Anpassung der Datenquellen und -formate möglich sind. Dabei kann auch eine Zusammenarbeit mit internen und externen Stakeholdern, wie beispielsweise Fachabteilungen oder externen Dienstleistern, erfolgen (Shafique und Qaiser 2014). Ein wichtiger Aspekt des

Vorgehens ist das Forschungsdatenmanagement sowie die Einhaltung von FAIR Data Prinzipien (Findable, Accessible, Interoperable, Reusable).

Ein weiterer Aspekt des Projekts ist das Forschungsdatenmanagement und die Einhaltung der FAIR-Prinzipien. Dies beinhalten beispielsweise die Dokumentation und Archivierung der Daten sowie die Gewährleistung der Nachvollziehbarkeit und Reproduzierbarkeit der Ergebnisse.

Durch die Umsetzung des Vorgehensmodells und die Einhaltung der FAIR-Prinzipien soll eine effiziente und transparente Verwaltung der Daten erreicht werden. Insgesamt ist ASUM-DM eher geeignet, wenn der Benutzer einen maßgeschneiderten Ansatz für Data Mining benötigt, während KDD eher für Situationen geeignet ist, in denen ein systematischer Ansatz erforderlich ist. Beide Modelle haben jedoch ihre Stärken und Schwächen, und die Wahl des Modells hängt von den spezifischen Anforderungen des Projekts ab.

Modell	ASUM-DM	KDD
Definition	ASUM-DM ist ein adaptives und vereinheitlichtes Data Mining-System, das die Erstellung von benutzerdefinierten Mining-Algorithmen durch die Verwendung einer Reihe von grundlegenden Operatoren ermöglicht.	KDD ist ein Prozess zur Entdeckung nützlicher Kenntnisse aus Daten, der verschiedene Schritte wie Datenvorbereitung, Data Mining und Interpretation der Ergebnisse umfasst.
Schritte	8	9
Fokus	ASUM-DM konzentriert sich auf Anpassungsfähigkeit und Anpassung von Mining-Algorithmen.	KDD konzentriert sich auf einen systematischen Prozess zur Wissensentdeckung aus Daten.
Ansatz	Der Ansatz von ASUM-DM ist bottom-up, d.h. er beginnt mit den grundlegendsten Operatoren, um komplexere Algorithmen aufzubauen.	Der Ansatz von KDD ist top-down, d.h. er beginnt mit dem Gesamtziel der Wissensentdeckung und geht dann zu spezifischen Data-Mining-Techniken über.
Vorteile	ASUM-DM bietet einen flexiblen und anpassungsfähigen Ansatz für Data Mining. Es ermöglicht die Erstellung benutzerdefinierter Mining-Algorithmen auf der Grundlage der Bedürfnisse des Benutzers.	KDD bietet einen systematischen Ansatz zur Wissensentdeckung und stellt sicher, dass alle notwendigen Schritte durchgeführt werden. Es wird weit verbreitet eingesetzt und wurde in verschiedenen Bereichen erfolgreich angewendet.
Nachteile	ASUM-DM erfordert ein gewisses Maß an Expertise im Bereich Data Mining, um effektiv genutzt zu werden. Die Erstellung benutzerdefinierter Algorithmen kann zeitaufwändig sein.	KDD ist möglicherweise aufgrund der Rechenkomplexität nicht für sehr große Datensätze geeignet. Es liefert möglicherweise nicht immer nützliche Ergebnisse, da die Qualität des entdeckten Wissens von der Qualität der verwendeten Daten abhängt.

Tabelle 2: Vergleich ASUM-DM und KDD

1.2.2 Aufgaben- und Funktionsdefinition des Datentreuhänders

Die Rolle des Datentreuhänders wird immer wichtiger in einer digitalisierten Welt, in der Daten eine zentrale Rolle spielen. Der Datentreuhänder ist dafür verantwortlich, einen sicheren Datenraum zu schaffen, in dem die Daten von Datengebern sicher gespeichert und verwaltet werden können. Hierbei ist es wichtig, dass der Datentreuhänder den rechtlichen Rahmen einhält und vertrauensfördernde Maßnahmen ergreift, um das Vertrauen der Datengeber zu gewinnen. Er ist eine zentrale Figur bei der Einrichtung und Verwaltung einer Datentreuhandplattform. Seine Kernfunktionalitäten und Aufgaben sind vielfältig und umfassen organisatorische, rechtliche und technische Aspekte.

Eine der wichtigsten Funktionen des Datentreuhänders ist die Bereitstellung von Infrastruktur und Software für die Datenablage und -teilung. Hierbei müssen technische Maßnahmen ergriffen werden, um die Daten sicher abzulegen und vor unbefugtem Zugriff zu schützen. Dazu zählen regelmäßige Backups der Daten, verschlüsseltes Datenmanagement,

Zugriffskontrollen für Datengeber und -nutzer sowie Logging von Datenzugriffen, um mögliche Fehler im Zugriff zu erkennen.

Der Datentreuhänder muss auch sicherstellen, dass alle rechtlichen Bestimmungen eingehalten werden, insbesondere in Bezug auf den Datenschutz. Hierbei ist es wichtig, eine feingranulare Zugriffsregelung für Datengeber und -nutzer bereitzustellen, um sicherzustellen, dass jeder Benutzer nur auf die Daten zugreifen kann, für die er die Berechtigung besitzt.

Der Datentreuhänder kann auch Mehrwertdienstleistungen anbieten, wie beispielsweise Datenanalysen und -auswertungen für Datengeber und -nutzer sowie Datenaufbereitung wie Pseudonymisierung und Anonymisierung, um noch mehr Datennutzer zu finden.

Ein weiterer wichtiger Aspekt ist die Bereitstellung von leicht nutzbaren Datenschnittstellen für den Import und Export von Daten. Hierbei ist es wichtig, dass die Datenschnittstellen standardisiert sind, um die Interoperabilität zu gewährleisten und den Datenaustausch zwischen verschiedenen Plattformen zu erleichtern.

Insgesamt ist die Rolle des Datentreuhänders von großer Bedeutung, um sicherzustellen, dass Daten sicher und rechtskonform verwaltet werden. Der Datentreuhänder muss sicherstellen, dass Datengeber jederzeit die vollständige Kontrolle und Einsicht über ihre Daten haben und dass Daten nur von berechtigten Personen genutzt werden können.

Die Aufgaben des Datentreuhänders für den Betrieb einer Datentreuhandplattform sind vielfältig und umfassen organisatorische, rechtliche sowie technische Aspekte. Der Datentreuhänder muss einen sicheren Datenraum schaffen, der den geltenden Gesetzen entspricht und es dem Datengeber ermöglicht, seine Daten zu verwalten und weiterzugeben. Hierbei muss der Datengeber jederzeit die vollständige Kontrolle und Einsicht über seine Daten behalten. Dazu gehören Maßnahmen wie die Wahl einer vertrauenswürdigen Betreibergesellschaft, die Bereitstellung von Infrastruktur und Software, die Speicherung und Verwaltung von Daten, regelmäßige Backups und Verschlüsselung der Daten sowie die Einhaltung aller rechtlichen Bestimmungen.

Weitere Aufgaben umfassen die regelmäßige Überprüfung und Anpassung der Plattform an geltende gesetzliche Bestimmungen, wobei dies Software, Datenmanagement und das Betriebskonzept beinhaltet. Dazu kommen die Durchführung und die Umsetzung von Maßnahmen für die Vertrauensförderung, wie Gespräche mit potentiellen Kunden, Aktualisierungen der Plattform in Zustimmung mit den Plattformbeteiligten oder Schulungen und ausführliche, immer aktuelle und nutzerfreundliche Dokumentation bzgl. der Nutzung der Plattform.

Auf der Seite der technischen Aufgaben erfolgt die Überprüfung der Hardware und Software ob diese State-of-the-Art ist sowie daraus resultierender Aktualisierung und das Testen, ob alle technischen Kernfunktionalitäten technisch einwandfrei ablaufen. Des Weiteren das Kontrollieren der Software auf mögliche Datenverarbeitungsfehler, sowie der Zugriffsregelung. Ergänzend muss eine Erweiterung des Angebotes an Mehrwertdienstleitungen und Umwandlung in Geschäftsmodelle für die Kostendeckung der Plattform und Schnittstellenerweiterung und -ausbau, um mehr potentiellen Kunden den Einstieg in die Plattform zu erleichtern, erfolgen. Diese technischen Aufgaben können auch als Bereitstellung eines Minimum Viable Product für den Erstbetrieb und ständige Weiterentwicklung basierend auf Bewertungen bezeichnet werden.

Für die Plattform TRANSIT, die im Rahmen des Projektes für die Logistikbranche entwickelt wird, ergeben sich zusätzliche Kernfunktionalitäten und Aufgaben. Dazu gehört unter anderem die Bereitstellung von anonymisierten Daten für datenschutzerhaltende Analysen, die Organisation des Datenteilens zwischen Logistikdienstleistern mit feingranularer Datenfreigabe auf Eigenschaftsebene, die Möglichkeit für den Datengeber, geteilte Daten auch nach dem Finden

eines Datennutzers zu aktualisieren sowie die Einhaltung weiterer datenabhängiger rechtlicher Regelungen, wie z.B. Sonderbestimmungen für die Datenspeicherung bei Luftfracht.

Zusätzlich bietet die Plattform TRANSIT die meisten Funktionalitäten einer Logistiksoftware zur Verwaltung von Auftragsdaten, eine rechtsichere Heranführung der Logistiker an die Digitalisierung aller Datenverarbeitungen sowie die Möglichkeit, den Auftragsprozess und den Datenaustausch bei Auftragsabgabe komplett digital abzubilden. Auch das Exportieren von bestimmten Daten für erforderliche nicht digitale Dokumente gehört zu den Kernfunktionalitäten der Plattform.

Weitere ständige Aufgaben die durch den Datentreuhänder durchgeführt werden sind die Einhaltung und Überprüfung speziell für die Logistik geltende rechtliche Bestimmungen auf Anpassungen und Veränderungen. Eine weitere organisatorische Aufgabe ist die andauernde Kommunikation mit Datengeber und Nutzer im Bezug der Logistikanforderungen, um mögliche Schwächen in der Plattform aufweisen und lösen oder mögliche Erweiterungen vereinbaren und nach Entwicklung validieren zu können.

Neben diesen organisatorischen Aufgaben, gibt es noch eine Vielzahl an technischen, welche die Entwicklung einer ganzheitlichen Plattform für die Auftragsverwaltung unterstützen, also die gesamten Logistikprozesse digitalisieren. Dazu gehört die Integration neuer Module für Terminfracht, Gefahrgut, Luftfracht, etc., Integration von Mechanismen, um den Preis komplett über die Plattform aushandeln zu können oder Schaffung von weiteren Schnittstellen für Import und Export, sowie damit verbundener Datentransformation. Zu diesem Export kommen noch Aufgaben bzgl. der Anpassung auftragsrelevanter Dokumente, sowie die Überarbeitung an neue Bedürfnisse und Pflichten. Ein weiterer Punkt ist die stetige Erweiterung und Weiterentwicklung der Paketnachverfolgung, sodass immer qualifiziertere Aussagen zum Verbleib eines Paketes oder Zustand gegeben werden können.

Die letzte Aufgabe für die technische Weiterentwicklung ist die Ausweitung des Zugriffsmanagements. Hierbei sollen Effizienzsteigerungen umgesetzt werden, um das Datenteilen noch einfacher zu gestalten, wie z.B. abhängige Entitäten zu teilen bzw. dies anzubieten. Abschließend kommt an dieser Stelle die Aufgabe hinzu effektive Mechanismen für Entzugsmöglichkeiten der Lese- und Schreibrechte zu integrieren und weiterzuentwickeln.

Um diese Aufgaben zu erfüllen, sind zahlreiche Maßnahmen während der Erstellung und Implementierung der Datentreuhandplattform sowie bei deren Betrieb erforderlich. Dazu gehören u.a. das Einrichten von Zugriffsregelungen, die Bereitstellung von Datenanalysen und -auswertungen, die Anonymisierung und Pseudonymisierung von Daten sowie die Erstellung von druckbaren Dateien oder konfigurierbaren Schnittstellen zum Export von Daten.

1.2.3 Konzeption Datentreuhandmodell und Betriebskonzept

Datentreuhänderkonzept

Das Konzept des Datentreuhandmodells ist eine nicht gewinnorientierte Initiative, die darauf abzielt, ein Vertrauensverhältnis zwischen den Parteien herzustellen und Transparenz im Umgang mit Daten zu fördern. Im Wesentlichen geht es darum, eine Plattform zu schaffen, die es Datengebern und -nutzern ermöglicht, Informationen sicher auszutauschen. Das Modell wurde entwickelt, um das Vertrauen zwischen den beiden Parteien zu stärken, da Datengeber oft Bedenken haben, dass ihre Daten missbraucht werden könnten. Das Datentreuhandmodell soll dabei helfen, diesen Bedenken entgegenzuwirken, indem es als Vermittler zwischen den Parteien auftritt und somit einen sicheren Austausch der Informationen ermöglicht.

Die Plattform des Datentreuhandmodells soll es Datennutzern und -gebern ermöglichen, sicher und vertrauensvoll zusammenzuarbeiten. Das Modell verfolgt hierbei den Ansatz, dass

beide Parteien von der Zusammenarbeit profitieren können. So können beispielsweise Unternehmen wertvolle Daten erhalten, die sie zur Entwicklung neuer Produkte nutzen können, während die Datengeber dafür eine angemessene Vergütung erhalten.

Ein weiterer wichtiger Aspekt des Datentreuhandmodells ist die Sicherheit der Daten. Da sensible Informationen ausgetauscht werden, muss die Plattform höchste Standards in puncto Datensicherheit gewährleisten. Das Modell setzt deshalb auf fortschrittliche Verschlüsselungstechnologien und andere Sicherheitsmaßnahmen, um sicherzustellen, dass die Daten der Nutzer geschützt sind.

Zusammenfassend lässt sich sagen, dass das Datentreuhandmodell ein innovatives Konzept ist, das darauf abzielt, Datennutzer und -geber auf einer sicheren Plattform zusammenzuführen. Dabei wird besonderer Wert auf Transparenz, Vertrauen und Sicherheit gelegt, um einen erfolgreichen Austausch von Informationen zu ermöglichen.

Betriebskonzept

Ein Datentreuhänder (auch als Datenverwalter oder Datenverarbeitungsdienstleister bezeichnet) ist ein Unternehmen, das als unabhängiger Drittanbieter Daten im Auftrag von Kunden speichert, verarbeitet oder überträgt. Das Betriebskonzept eines Datentreuhänders könnte wie folgt aussehen:

Sicherheit und Datenschutz: Ein Datentreuhänder muss strenge Sicherheitsmaßnahmen und Datenschutzrichtlinien einhalten, um die Vertraulichkeit und Integrität der Daten zu gewährleisten. Dazu gehören die Verwendung von verschlüsselten Datenübertragungen, Firewall-Schutz, Zugriffskontrollen, regelmäßige Sicherheitsaudits und die Einhaltung von Compliance-Standards wie der DSGVO.

Flexibilität und Skalierbarkeit: Ein Datentreuhänder sollte in der Lage sein, die Speicher- und Verarbeitungskapazitäten seiner Kunden schnell und effizient zu skalieren, um sich ändernden Geschäftsanforderungen gerecht zu werden. Dies erfordert eine gut strukturierte IT-Infrastruktur und eine flexible Architektur, die es dem Datentreuhänder ermöglicht, schnell auf die Bedürfnisse seiner Kunden zu reagieren.

Vertrauen und Transparenz: Ein Datentreuhänder muss ein hohes Maß an Vertrauen und Transparenz aufrechterhalten. Er muss seine Kunden über seine Datenschutz- und Sicherheitspraktiken informieren und sicherstellen, dass sie immer über den Status ihrer Daten informiert sind.

Compliance und Regulierung: Ein Datentreuhänder muss in Übereinstimmung mit den geltenden Datenschutz- und Sicherheitsvorschriften arbeiten. Er muss sich an alle relevanten Vorschriften halten, um sicherzustellen, dass die Daten seiner Kunden geschützt und sicher sind.

Datenzugriff und Datenverwaltung: Ein Datentreuhänder muss sicherstellen, dass seine Kunden einen einfachen und sicheren Zugriff auf ihre Daten haben. Er muss auch eine effektive Datenverwaltung anbieten, um sicherzustellen, dass die Daten seiner Kunden immer aktuell und korrekt sind.

Kundenservice und Support: Ein Datentreuhänder muss eine hervorragende Kundenservice- und Support-Erfahrung bieten. Er muss in der Lage sein, schnell auf Kundenanfragen zu reagieren und kompetent Kundenprobleme zu lösen.

Damit die Datentreuhandplattform TRANSIT diese Punkte umsetzen und einhalten kann wird diese wie folgt spezifiziert: Um die Sicherheit und Datenschutz einzuhalten werden State-of-

the-Art Verschlüsselungsmechanismen, wie AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), für die Daten angewendet, sowie eine sichere Datenübertragung mit HTTPS (Hypertext Transfer Protocol Secure) umgesetzt. Dazu kommen noch weitere Sicherheitsmechanismen, die in der Clusterarchitektur mit integriert sind, wie eine Firewall oder ein Gateway. Zu diesen technischen Anforderungen kommen noch rechtliche, welche z.B. aus der DSGVO stammen und in AP2 umfangreich bewertet werden.

Um Flexibilität und Skalierbarkeit einzuhalten, werden die Programme im Cluster in einer containerisierten Umgebung ausgeführt, um diese Anforderungen umzusetzen (AP4). Somit ist die Grundlage geschaffen, um mit steigender Datenmenge und wachsender Benutzerzahl umzugehen und sich an sich ändernde Anforderungen und Bedürfnisse anzupassen.

Für Vertrauen und Transparenz: sorgt der Fakt, dass die Software und die Datenbanken bei der Universität Leipzig gehostet sind. Auch spielt hier der Punkt eine Rolle das geprüft wird, ob die Datengeber und -nutzer sowie deren Datenquellen vertrauenswürdig und transparent sind, sowie durch die Implementierung von Auditing- und Überprüfungsprozessen innerhalb der Plattformarchitektur weiter Vertrauen geschaffen wird.

Compliance und Regulierung umfasst die Analyse gegebener gesetzlicher Bedingungen, regelmäßige Überprüfung, ob sich die relevanten Bedingungen verändert haben, sowie Anpassung der Software (AP2).

Der Datentreuhänder muss ein umfangreiches Zugriffskonzept entwickeln und validieren, welches den Datenzugriff kontrolliert, sowie ein Datenmanagementkonzept aufstellen um die Daten ordnungsgemäß zu verwalten (AP2).

Der letzte Punkt, umfasst das Auswerten von Nutzerbewertungen oder die Erweiterung der Plattform, um Kundenwünsche und Probleme zu lösen, wozu Geschäftsmodellentwicklung, wie in (AP5), dazu gehört.

Im Überblick soll der zukünftige Datentreuhänder wie folgt konzeptioniert sein (siehe Abbildung 4: Datentreuhänder Modell).

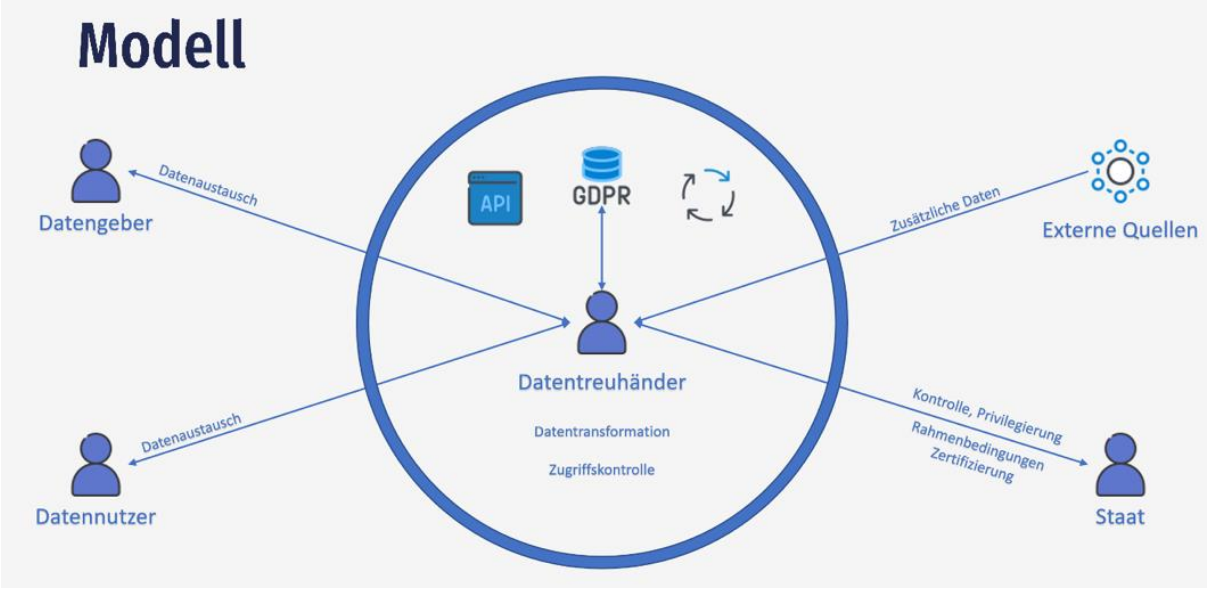

Abbildung 4: Datentreuhänder Modell

Um diese einzelnen Ziele für ein vollumfängliches System zu erreichen, gibt es grundlegend verschiedene theoretische Ansätze, die zur Auswahl und Umsetzung dieses Betriebskonzeptes einen Einfluss haben, wie z.B. On-Premise, Cloud-basiert, Managed-Service, Data-Trust-as-a-Service. Hierbei ist On-Premise ein Modell bei dem die Plattform auf den Servern des Kunden oder in dessen Rechenzentrum betrieben wird und der Kunde für die Wartung und Sicherheit der Plattform verantwortlich ist. Das komplette Gegenteil ist das Cloud-basierte Modell, wobei die komplette angebotenen Software in der Cloud gehostet wird und der Kunde für die Nutzung der Plattform zahlt, aber nicht für die Wartung und Sicherheit verantwortlich ist. Im Rahmen des „Managed-Service“ erfolgt selbst die Wartung und der Betreib bei einem Dritten, wobei der Kunde für die Nutzung an den Anbieter bzw. Vermittler bezahlt, welcher die dritte Partei entlohnt. Ein weiterer Ansatz ist das „Data Trust as a Service“ Modell (Richard K. Lomotey et al. 2022), wobei das Datentreuhandmodell als Service in der Cloud für beliebige Anwendungsdomänen, wie z.B. Medizin, IOT, Logistik angeboten wird, bzw. ein Service auf Anfrage in diese Plattform integriert wird. Dabei ist es in diesem Modellansatz zwingend erforderlich die technischen Anforderungen genau zu erfassen und danach das Betriebsmodell zu konzeptionieren, da schon eine Datenschutzverletzung das Vertrauen in die Plattform direkt erschüttern wird und nur langsam wiederaufbauen ist (siehe Abbildung 5) (Richard K. Lomotey et al. 2022).

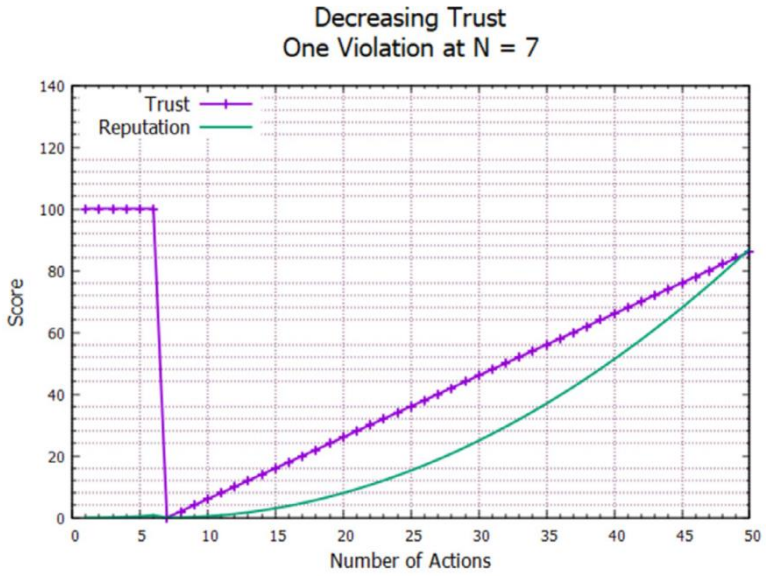

Abbildung 5: Verlauf Vertrauen bei einer Datenschutzverletzung (Richard K. Lomotey et al. 2022)

Es gibt eine Vielzahl an Ansätzen, wobei je nach Anwendungsfall und mit Absprache mit bestehenden und neuen Kunden für die Datentreuhandplattform abgeklärt werden muss, ob das bestehende Betriebskonzept bestehen oder abgeändert werden muss. So kann einerseits ein größerer Kundenstamm abgedeckt werden und anderseits das Vertrauen für alle Teilnehmer der Plattform erhöht werden.

Ein weiterer wichtiger Punkt für den Betrieb eines Datentreuhänders ist der Betreiber. In Tabelle 3 befinden sich zwei Schlüsselfragen, über die Finanzierung und die ausführende Organisation, um zu definieren wie der Datentreuhänder vertrauenswürdig gemacht werden kann.

Das Konzept der Datentreuhandgesellschaften wird als Lösung vorgeschlagen, um die Dominanz großer Unternehmen auf den Datenmärkten abzuschwächen, die Privatsphäre der Verbraucher zu schützen und Wettbewerb und Innovation zu fördern. Die Untersuchung zeigt auf, wie Datentreuhandgesellschaften als Vermittler fungieren können, die sicherstellen, dass die

Daten der Verbraucher in einer Weise genutzt werden, die mit ihren Interessen und ihrer Zustimmung übereinstimmt, wodurch eine Ausbeutung verhindert und ein gerechterer Datenfluss gefördert wird (Blankertz 2020).

TRANSIT soll dabei von einer nicht gewinnorientieren Instanz betrieben werden. So können ein gemeinnütziger Verein, eine staatliche Behörde oder ein Verbund der Betreiber sein.

Characteristic	Option 1	Option 2	Option 3
Funding: how to finance the trust's activities	Commission on data licenses	Public funding	Data-specific taxes
Executing organization: what type of organization can be a data trust	Any kind of organization, including for-profit companies	Non-profit organizations	State-run organizations
Decision-making mechanism: how the trustee makes decisions about data sharing	Majority voting by beneficiaries on individual sharing agreements	Voting of representatives	Aggregation of individual preferences
Default setting: the default regarding data sharing	Opt-in throughout	Consent champions or average of actively chosen settings	Opt-out throughout
Negotiation objectives: what the trustee should maximize in its negotiations with data-using organizations	Income only	Combined utility of income and consumer-friendly data usage	Consumer-friendly data usage only
Data monetization: if the trustee should monetize data	No a allowed	Exemption of sensitive data types from monetization	All data can be monetized
Benefit distribution: how a trustee distributes its benefits among beneficiaries	Dependent on their data contribution	As decided by its beneficiaries	Fully equal
Evaluation: how performance is assessed	Majority voting by members	Optional certification	Mandatory external certification

Tabelle 3:: Gestaltung der internen Governance (Blankertz 2020, S. 19)

1.2.4 Konzept zur Umsetzung von Datentreuhandmodellen

Entwicklung von Methoden zur Anonymisierung von unternehmensübergreifenden Geschäftsprozessdaten

Um die Daten DSGVO konform verarbeiten zu können, ist es erforderlich diese z.B. für die Forschung oder anderen Datenproduktanbietern anonymisiert bzw. pseudonymisiert mit Freigabe des jeweiligen Datengebers (Firma) bereitzustellen. Welche Daten einen Personenbezug bzw. Geschäftsgeheimnisse umfassen wurde entsprechend in M2.1 analysiert und in M2.2 erweitert.

Bereitstellung eines anonymisierten Datensatzes

Eine vollständige Anonymisierung der Daten ist hierbei nur nach 10 Jahren bzgl. der DSGVO möglich bzw. es kann z.B. für die Forschung nur ein anonymisierter Datensatz bereitgestellt werden, da die operativen Daten weiter für die jeweiligen Firmen verfügbar sein müssen.

Durch die Anonymisierung unterliegt der Datensatz auch nicht mehr der DSGVO und ist somit theoretisch frei verwendbar, wo aber im Rahmen der Datentreuhandplattform sich selbst in diesem Fall die Nutzer verifizieren müssen.

Die Anonymisierung von Daten soll die folgenden drei Risiken minimieren (Dewes 2022):

- Re-Identifikation einzelner Personen,
- Vorhersage von Attributwerten einzelner Personen,
- Möglichkeit der Verknüpfung anonymer Daten mit Dritt-Daten

Allgemein kann dies durch folgende grundlegende Techniken erreicht werden (Winter et al. 2019):

Generalisierung: Die jeweiligen Attributwerte werden durch weniger genaue Angaben ersetzt.

Löschung: Der Inhalt einzelner Zellen, Spalten oder Zeilen wird gelöscht. Dies entspricht einer Generalisierung zu einem allumfassenden und nichtssagenden Wert.

Mikroaggregierung: Die Daten werden nach Ähnlichkeit in den Attributwerten gruppiert (engl. clustering) und pro Gruppe werden die einzelnen Werte zu einem repräsentativen Wert zusammengefasst.

Verfälschung: Ein Teil der Daten oder alle Daten werden zufällig abgewandelt, durch zufällige Störungen von Werten, Vertauschung von Werten oder Erstellung synthetischer Daten.

Forschungsdatenbereitstellung

Dies könnte erreicht werden, indem basierend auf der Datenabgabezustimmung für die Forschung ein Abbild der bisherigen Datenbank in eine Anonymisierte regelmäßig erfolgt, und diesen verifizierten Forschern bereitgestellt wird.

Im Vornherein können hier z.B. die Mitglieder einer Firma aggregiert werden, z.B. auf die Mitarbeiteranzahl oder die Einteilung der Firmen in Buckets, da die Datentreuhandplattform für die Bereitstellung von Auftragsdaten und nicht die Nutzerdaten einer Firma umgesetzt ist.

Adressdaten

Für Adressen in Aufträgen kann bei der Anonymisierung z.B. der Ansprechpartner und Telefonnummer komplett gelöscht werden oder jeweils in Bucket geclustert werden. Die Clusterung kann entsprechend k-anonym, l-divers oder t-ähnlich sein, wobei das Problem besteht, das eine Re-Identifizierung möglich sein kann (Dewes 2022).

Bei der Adresse besteht auch die Herausforderung, dass Kunden der Transport-Firmen identifiziert werden können, indem die vollständige Adresse angegeben wird.

Um diese Adressen zu anonymisieren wurden folgende Methoden entwickelt:

- Zusammenfassen der Adressen zu Postleitzahlen, wobei manche Firmen eigenen PLZ. haben, was entsprechend auf die umliegenden PLZ. aggregiert werden muss
- Zusammenfassen aller Adressen einer Straße
- Bilden von Buckets der Hausnummern

- Ermitteln und Clustern der Koordinaten der Adressen und Zusammenfassen von nah aneinanderlegenden zu einem Mittelpunkt welcher mit Differential Privacy zufällig verschoben wird
- Präfixclusterung von PLZ und löschen der anderen Adressfelder
- Semantische Anonymisierung mit aktiven Ontologien, ähnlich zu (Aichroth et al. 2020)

Kundendaten

Das gleiche Problem besteht bei Kundendaten bei denen darauf geachtet werden muss, wo selbige Bearbeitung wie bei den Auftragsadressen stattfinden muss. Für Ansprechpartner wurde sich überlegt entweder diese komplett zu löschen oder diese pro Firma zu zählen, da mit nur einer Umschreibung mit einer ID die Arbeitseffizienz der Mitarbeiter Rückschlüsse auf einen einzelnen Mitarbeiter zulassen könnte.

Falls ein Firmenbezug zusätzlich anonymisiert werden soll ist ein weiterer Ausschluss von bereitgestellten Daten wie Ansprechpartner, eine anonyme ID für die beauftragte Firma usw. erforderlich.

Eine weitere Möglichkeit der Anonymisierung ist das Erstellen von synthetischen Daten z.B. mit einem, GAN (Generative Adversarial Networks) oder durch zufällige Auswahl von Werten aus der ermittelten Verteilung der Daten (Schwartmann et al. 2022).

Für die Löschung der einzelnen Felder, welche nicht bereitgestellt werden, wäre es auch möglich, diese Werte mit einem allgemeinen Pseudonym zu ersetzen, was für alle gelöschten Felder übereistimmt und somit keine Rückschlüsse ermöglicht.

Pseudonymisierungsmöglichkeiten im operativen Geschäft

Im operativen Geschäft wurde sich mit dem Praxispartner und weiteren Anwendern darauf geeinigt, die nicht freigegebenen Daten nicht bei Anfrage bereitzustellen und nicht nur zu pseudonymisieren. Dies wäre genauso für den operativen Betrieb der Plattform möglich indem dann nicht freigegebene Attributwerte mit Pseudonymen tabellenbasiert oder kryptografisch verschlüsselt gesendet werden. Dies ist möglich da generell Pseudonymisierung auch auf nicht-personenbezogene Daten angewandt werden kann, zum Beispiel mit der Zielstellung, Geschäftsgeheimnisse zu schützen (Dewes 2022).

Nutzung von kryptografischen Hashs

Eine Möglichkeit mit kryptografischen Hashs, wäre es ähnlich den Public Key Verfahren, die Felder der Entitäten, bei denen Zugriff gegeben wurde mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln und die nicht zugänglichen Felder mit dem eigenen Private-Key sodass beim Entschlüsseln nur die freigegebenen Felder einen Klartext ergeben.

Verarbeitung des Standortpunkts einer Adresse

Ein Algorithmus welcher in der Pseudonymisierung und Anonymisierung gleichermaßen verwendet werden kann, wurde für den Standort einer Adresse entwickelt, welcher von der jeweiligen Freigabekonfiguration und Anonymisierungskonfiguration abhängt.

Für die Pseudonymisierung wäre dann eine Übersetzungstabelle erforderlich, welche dann noch die Nachkommazahlen eines gemappten Punktes noch exakt auf einen Ausgangspunkt mappt.

Dazu werden die Felder Straße, Ort und PLZ herangezogen. Der ausgegebene Standort ergibt sich final aus folgender Tabelle:

Variante	PLZ	Ort	Straße	Standort
1	Nein	Nein	Nein	Mittelpunkt Deutschland
2	Nein	Ja	Nein	Mittelpunkt Ort
3	Nein	Ja	Ja	Exakter Ort
4	Nein	Nein	Ja	Mittelpunkt Deutschland
5	Ja	Nein	Nein	Mittelpunkt PLZ
6	Ja	Ja	Nein	Mittelpunkt Ort
7	Ja	Ja	Ja	Exakter Punkt

Tabelle 4: Anonymisierung Standortkoordinaten

Erarbeitung von Methoden zur Sensibilisierung beim Austausch vertrauenswürdiger Geschäftsprozessdaten

Der Austausch vertrauenswürdiger Geschäftsprozessdaten stellt eine zentrale Herausforderung in vielen modernen Wirtschaftszweigen dar, insbesondere in Bereichen wie Logistik, Finanzen und Gesundheitswesen. Die Sensibilisierung der Datengeber für die Bedeutung des sicheren und effizienten Datenaustauschs ist daher von entscheidender Bedeutung für die erfolgreiche Digitalisierung von Geschäftsprozessen. Das Arbeitspaket 3.5 zielt darauf ab, Methoden zu entwickeln, um Stakeholder effektiv von der Unabhängigkeit, Sicherheit, Transparenz und dem Mehrwert des Austausches vertrauenswürdiger Daten zu überzeugen (Balsa et al. 2022).

Zertifikate als Vertrauensgrundlage

Zertifikate spielen eine wichtige Rolle beim Aufbau von Vertrauen in digitale Plattformen und Datenökosysteme. Sie dienen als Nachweis dafür, dass bestimmte Sicherheitsstandards eingehalten werden und dass die Plattform oder das Unternehmen die Privatsphäre und Integrität der Daten respektiert. Im Rahmen von AP 3.5 werden Zertifizierungsprozesse entwickelt, die speziell auf die Bedürfnisse von Geschäftsprozessdaten ausgerichtet sind. Diese Zertifikate können beispielsweise von akkreditierten Institutionen ausgestellt werden und umfassen Prüfungen der IT-Sicherheit, der Datenschutzpraktiken sowie der Compliance mit relevanten gesetzlichen Vorgaben.

1.2.5 Präsentation der Ergebnisse und der Plattform

Die effektive Präsentation der Plattform und der damit verbundenen Ergebnisse ist ein weiterer wichtiger Schritt zur Sensibilisierung und Gewinnung von Datengebern. Dies beinhaltet detaillierte Demonstrationen der Plattformfunktionalitäten, Workshops mit potenziellen Nutzern und die Erstellung von Fallstudien, die den Nutzen der Plattform in realen Szenarien aufzeigen. Durch interaktive Elemente können Datengeber direkt erleben, wie die Plattform funktioniert und welche Vorteile sie bietet.

Integration und Darstellung von Mehrwertfunktionen

Die Einbindung von Mehrwertfunktionen in die Plattform ist entscheidend, um den Nutzen für die Anwender zu maximieren.

CRM Export

Die Möglichkeit, Daten direkt in Customer-Relationship-Management-Systeme (CRM) zu exportieren, erhöht die Effizienz und die Datenkonsistenz. Nutzer können wichtige Geschäftsprozessdaten automatisch in ihr CRM überführen, was die Pflege von Kundenbeziehungen und die Lead-Generierung vereinfacht.

Automatische Streckenlängenberechnung

Diese Funktion bietet insbesondere für Logistikunternehmen einen erheblichen Mehrwert, da sie die Planung und Kostenkalkulation von Transporten vereinfacht. Durch die automatische Berechnung der Streckenlänge können Unternehmen ihre Ressourcen effizienter planen und nutzen.

Sicherheitsmaßnahmen und Datenschutz

Die Sicherheit von Geschäftsprozessdaten ist ein zentrales Element, um Vertrauen bei den Datengebern zu schaffen. AP 3.5 befasst sich daher intensiv mit der Implementierung von fortschrittlichen Sicherheitstechnologien und -protokollen, einschließlich End-to-End-Verschlüsselung, regelmäßigen Sicherheitsaudits und strikten Zugriffskontrollen. Datenschutzkonformität wird durch die Einhaltung von Gesetzen wie der DSGVO und anderen relevanten Vorschriften sichergestellt. Im Rahmen von AP 3.5 ist die Gewährleistung der Datensicherheit und der Schutz personenbezogener Daten von höchster Priorität. Diese Priorität manifestiert sich in einer Reihe von implementierten Sicherheitsmaßnahmen und Datenschutzbestimmungen:

Implementierung von Sicherheitstechnologien

Die Plattform nutzt fortschrittliche Sicherheitstechnologien wie End-to-End-Verschlüsselung, um die Daten während der Übertragung und Speicherung zu schützen. Dies stellt sicher, dass Daten nur von autorisierten Nutzern eingesehen werden können, und minimiert das Risiko von Datenlecks oder unautorisiertem Zugriff.

Regelmäßige Sicherheitsaudits

Regelmäßige Sicherheitsaudits sind entscheidend, um sicherzustellen, dass die Sicherheitsmaßnahmen aktuell und effektiv sind. Diese Audits werden von unabhängigen Dritten durchgeführt, um eine objektive Bewertung der Sicherheitslage zu bieten. Solche Audits helfen auch, Schwachstellen zu identifizieren und zu beheben, bevor sie ausgenutzt werden können.

Datenschutzkonformität

Die Plattform hält sich streng an Datenschutzgesetze wie die DSGVO, das BDSG (neu) und das TTDSG. Diese Gesetze regeln, wie personenbezogene Daten gesammelt, gespeichert, verarbeitet und weitergegeben werden dürfen. Ein besonderes Augenmerk liegt auf der Einhaltung der Prinzipien der Datenminimierung und Zweckbindung sowie der Gewährleistung der Rechte der betroffenen Personen.

Transparenz als strategischer Vorteil

Transparenz in der Datenverarbeitung ist nicht nur eine rechtliche Anforderung, sondern auch ein entscheidender Faktor für das Vertrauen der Datengeber:

Offenlegung von Verarbeitungsaktivitäten

Durch die klare Kommunikation darüber, wie und zu welchem Zweck Daten verarbeitet werden, können Bedenken hinsichtlich des Datenschutzes effektiv adressiert werden. Nutzer müssen in der Lage sein, die Kontrolle über ihre Daten leicht auszuüben, was durch transparente Datenschutzrichtlinien und leicht zugängliche Datenschutzeinstellungen ermöglicht wird.

Beteiligung der Nutzer

Transparenz fördert auch die Beteiligung der Nutzer am Prozess. Durch regelmäßige Updates und die Einbindung von Feedback in die Weiterentwicklung der Plattform können Nutzer sich als Teil des Systems fühlen, was zur Akzeptanz und zur aktiven Nutzung der Plattform beiträgt.

Stakeholder-Engagement und Sensibilisierung

Effektives Stakeholder-Engagement ist für den Erfolg von AP 3.5 unerlässlich. Es umfasst verschiedene Strategien und Methoden, um verschiedene Gruppen zu erreichen und zu informieren:

Workshops und Schulungen

Durch die Organisation von Workshops und Schulungen können Datengeber und Nutzer direkt erreicht werden. Diese Veranstaltungen dienen dazu, die Funktionen der Plattform vorzustellen, praktische Anleitungen zu bieten und direktes Feedback zu sammeln. Solche interaktiven Formate sind besonders wirksam, um Komplexität zu reduzieren und die Vorteile der Plattform greifbar zu machen.

Fallstudien und Erfolgsbeispiele

Die Verwendung von Fallstudien und das Highlighten von Erfolgsbeispielen sind mächtige Werkzeuge, um den Mehrwert der Plattform zu demonstrieren. Sie zeigen potenziellen Nutzern konkret auf, wie die Plattform ihre Probleme lösen kann und welchen wirtschaftlichen Nutzen sie bietet.

Fortlaufende Kommunikation

Die fortlaufende Kommunikation mit Stakeholdern durch regelmäßige Updates, Newsletter und aktive Präsenz auf relevanten Plattformen und Konferenzen stellt sicher, dass das Projekt und seine Fortschritte sichtbar und relevant bleiben.

Methoden zur Datensensibilisierung

Implementierung einer Informationskampagne

Eine umfassende Informationskampagne kann dazu beitragen, das Bewusstsein und das Verständnis der Datengeber über die Vorteile des sicheren Datenaustauschs zu erhöhen. Diese Kampagne kann folgende Elemente umfassen:

Bildungsmaterialien: Erstellung und Verbreitung von leicht verständlichen Guides, Videos und FAQ-Dokumenten, die die Funktionen der Plattform und die Vorteile des Datenaustauschs erläutern.

Erfolgsgeschichten: Präsentation von Fallstudien und Testimonials von frühen Nutzern, die positive Erfahrungen mit der Plattform gemacht haben, um Vertrauen und Glaubwürdigkeit zu fördern.

Öffentliche Diskussionen und Webinare: Organisation von Diskussionsrunden und Webinaren mit Branchenexperten, die die Bedeutung des sicheren und effizienten Datenaustauschs betonen.

Entwicklung von Datenschutz-Toolkits

Zur Unterstützung der Datengeber können spezielle Datenschutz-Toolkits entwickelt werden, die Folgendes enthalten:

Datenschutzbest Practices: Leitfäden zur besten Praxis für Datensicherheit und Datenschutz, die speziell auf die jeweilige Branche zugeschnitten sind.

Checklisten zur Datensicherheit: Einfache Checklisten, die Datengeber Schritt für Schritt durch die erforderlichen Sicherheitsmaßnahmen führen.

Vorlagen und Werkzeuge zur Risikobewertung: Tools, die Unternehmen dabei helfen, ihre eigenen Datenschutzrisiken zu bewerten und entsprechende Maßnahmen zu planen.

Personalisierte Beratung und Support

Ein personalisiertes Beratungsangebot kann besonders wirkungsvoll sein, um das Vertrauen der Datengeber zu gewinnen. Dies könnte umfassen:

Individuelle Beratungsgespräche: Bereitstellung von Experten, die direkt mit den Datengebern zusammenarbeiten, um spezifische Bedenken oder Anforderungen zu adressieren.

Technischer Support: Einrichtung eines dedizierten technischen Supports, der schnell auf Fragen und Probleme der Nutzer reagieren kann.

Workshops vor Ort: Durchführung von Workshops in den Räumlichkeiten der Datengeber, um spezifische Features der Plattform zu demonstrieren und direkt auf individuelle Fragen eingehen zu können.

2 Wichtigste Positionen des zahlenmäßigen Nachweises

Eine umfangreiche Übersicht zu den einzelnen zahlenmäßigen Kosten- bzw. Ausgabenpositionen (Personal, Material, Reisen und Sonstige) ist separat dem zahlenmäßigen Verwendungsnachweis zu entnehmen.

3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Nur im Rahmen der Kooperation von Unternehmen und Forschungseinrichtungen war es möglich diesen Umfang an Projektergebnissen zu generieren. Dabei wurde im Zusammenhang der Kooperation vor allem die Integration von praktischer Expertise in die Forschungsbemühungen geschätzt, welche zu praxisnahen zielgruppenorientierten Lösungskonzepten und Forschungsergebnissen in TRANSIT führten. Dadurch konnte die erforderliche fachliche Expertise zusammengebracht werden, welche besonders für die Verknüpfung der Forschungsergebnisse und die Herstellung der Zusammenhänge erforderlich waren. Damit konnten neben den wissenschaftlichen Befähigungen der Universitäten bspw. auch die praxisnahen zielgruppenorientierten Kompetenzen in die Arbeiten involviert werden. Auf diese Art war es für jeden Partner möglich, das eigene Expertenwissen zur Unterstützung des gemeinsamen Projektvorhabens einzubringen. Eine Zusammenarbeit der verschiedenen Partner war dementsprechend notwendig, da keiner alleine über die nötigen Mittel zum Erreichen der Zielvorgaben hätte aufbringen können. Unter normalen wirtschaftlichen Bedingungen wäre das Vorhaben zu risikobehaftet und keiner der einzelnen Partner hätte ausreichend eigene Forschungsmittel zur Verfügung gehabt. Hinzukommt die interdisziplinäre Zusammenarbeit von Forschungseinrichtungen und KMUs zu dem das Vorhaben zentral beigetragen hat. Sowohl Prototypen als auch Konzepte sind Artefakte welche für die zukünftig fortführende Wissensgewinnung auch projektübergreifend genutzt werden können. Alle Tätigkeiten waren hinsichtlich des Inhalts und Umfang angemessen. Die aus dem Projekt speziell für Veröffentlichungen extrahierten Forschungsergebnisse sind separat aufgelistet und können öffentlich eingesehen werden (siehe Abschnitt 6).

4 Voraussichtlicher Nutzen und Verwertung

Es wurde bereits ab Beginn der Projektlaufzeit intensiv die Verwertung von wissenschaftlichen und wirtschaftlichen Projektergebnissen diskutiert. Des Weiteren wurden die Weiterverwendung und Entwicklung der generierten Softwareartefakte in Rahmen von FOX und weiteren am Testbetrieb des Prototypens beteiligten Unternehmen des Netzwerk Logistik Mitteldeutschland besprochen. Für weitere mögliche Forschungsprojekte welche die Grenzen des Projektes erweitern, dienen gewonnenen Erkenntnisse und Ergebnisse des TRANSIT-Projekts als wertvolle Grundlage.

TRANSIT konnte im Rahmen der Projektlaufzeit Ergebnisse im Bereich der Datentreuhänderschaft, effektives und effizientes sowie feingranulares Zugriffsmanagement und State-of-the-Art Datenverwaltungstools für Logistik, speziell Auftragsdaten erzielen. Zum Ende der Projektlaufzeit, hat sich herausgestellt, das für TRANSIT als Datentreuhandplattform als eigenständiges wirtschaftlich tragfähiges Produkt der Markt noch nicht bereit ist. Jedoch wurde damit begonnen die Projektergebnisse von den beteiligten Projektpartnern individuell zu verwerten.

INF konnte im Rahmen der Plattformentwicklung Expertise im Bereich der datentreuhändischen Datenverwaltung und –Verarbeitung aufbauen. Des Weiteren wurde in Kooperation mit IWI die Kompetenz der Integration neuer Zugriffskonzepte und -kontrollen aus der

Wissenschaft und deren praktische Umsetzung erweitert. Somit kann INF die gewonnenen Ergebnisse und Expertisen in zukünftige Projekte zu Datentreuhandplattformen, Datenverwaltungsplattformen und Zugriffskonzepten einsetzen.

IWI wird die Ergebnisse direkt in verschiedenen Forschungsbereichen verwerten und im Rahmen des Logistics Living Labs werden die Forschungsergebnisse für Bürger, Projektträger, Logistikakteure, Wissenschaftspartner und weitere Interessierte, z. B. aus der Wirtschaft, durch Demonstratoren greifbar machen. IWI kann die gewonnenen Erkenntnisse in weiteren zukünftigen und in Planung befindlichen Forschungsprojekten einbringen und noch weiter die wissenschaftliche Erkenntnisse vertiefen und weiterentwickeln, da bisher nur wenig bis gar keinen Veröffentlichungen im Bereich der Datentreuhand, speziell im Bereich der Logistik publiziert wurden.

FOX wird die Projektergebnisse im Netzwerk Logistik Mitteldeutschland verbreiten sowie die Prototypen weiterentwickeln um diesen anschließend im Rahmen des Vereins den Mitgliedern als datentreuhändische Datenverwaltungs- und -teilungsplattform anzubieten. Durch diese Bemühungen wird der Datenschatz der Datentreuhandplattform ständig erweitert werden, wozu in Abstimmung mit den Beteiligten der Plattform ein möglicher Zugang für Forschungsrichtungen ermöglicht wird.

lfd. Nr.	**Ergebnis und Verwertungsmöglichkeit**	**Zeithorizont**
1	Verbreitung der Ergebnisse über die Website des Vorhabens bzw. über die Webseiten des Projektpartners **IWI**	ab sofort laufend
2	Vorstellung des Vorhabens und der Ergebnisse auf Fachtagungen (z.B. Mitteldeutsches Logistikforum), Messen und Veranstaltungen (insb. im Logistics Living Lab)	ab sofort laufend
3	Transfer von Ergebnissen im Rahmen von Fachveranstaltungen und -workshops (insb. im Logistics Living Lab)	ab sofort laufend
4	Nutzung der TRANSIT-Ergebnisse in der Lehre insb. im Bereich der Vorlesungen zu Logistikdienstleistungssystemen	ab sofort laufend
5	Nutzung der TRANSIT -Ergebnisse für zukünftige Drittmittelprojekte; Beantragung anschließender FuE-Projekte	ab sofort laufend
6	Vermarktung und Transfer der TRANSIT-Plattform, sowie des Datentreuhandmodells zusammen mit dem InfAI e.V.	ab sofort laufend

Tabelle 5 Angepasster Verwertungsplan TRANSIT

5 Während der Durchführung des Vorhabens dem ZE bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Während der Durchführung des Vorhabens sind keine bedeutenden Fortschritte auf dem Gebiet des Datentreuhänders in der Logistik bekannt geworden.

6 Verbreitung

Bei den Vernetzungsveranstaltungen fand ein intensiver Austausch mit Partnerprojekten des Förderprogramms statt und im TRANSIT Konsortium wurde intensiv zu Querschnittthemen wie Datenfreigabekonzepten, effiziente Logistik-Datentreuhand-Software während mehreren Austauschmeeting zum Projektfortschritt Informationen und Erkenntnisse geteilt.

TRANSIT profitiere direkt durch den Einsatz von Open-Source-Softwarekomponenten, welche im Rahmen der Plattformentwicklung eingesetzt wurden. Somit konnte im Rahmen des Projektes ein wissenschaftlich erforschtes Zugriffskonzept direkt erweitert und den Nutzer direkt bei der Plattformnutzung als Datentreuhandkomponente zur Verfügung gestellt werden.

Erfolgte oder geplante Veröffentlichungen des Ergebnisses

Während der Laufzeit des Projektes, war es dem Konsortium bereits möglich erste wissenschaftliche Erkenntnisse zusammenzufassen und auf Konferenzen zu publizieren.

Kober, Sascha; Koch, Michael; Gaunitz, Benjamin; Franczyk, Bogdan (2023): Data Trust in Logistics: Price Prediction for Collaboration. In: 2023 14th International Conference on Information & Communication Technology and System (ICTS), S. 29–34. (Kober et al. 2023)

Koch, Michael; Kober, Sascha; Straburzynski, Stanislaw; Gaunitz, Benjamin; Franczyk, Bogdan (2023): Federated Learning for Data Trust in Logistics. In: Position Papers of the 18th Conference on Computer Science and Intelligence Systems: PTI. (Koch et al. 2023)

Die Ergebnisse zu den Prototypen von TRANSIT wurden auf folgenden Plattformen veröffentlicht:

TRANSIT-Projektwebseite: https://transit-project.de/

TRANSIT-Plattform: https://app.transit-project.de/

Quellcode DTM-Plattform: https://github.com/TRANSIT-Team/TRANSIT-Data-Trust

Quellcode Access-Control: https://github.com/TRANSIT-Team/Finer-Grained-Attribute-Based-Policy-Machine

Verbreitung

Verbreitung und Verwertung sind entscheidende Komponenten für den Erfolg und die Nachhaltigkeit der Projektergebnisse. Im TRANSIT-Projekt wurden diese Aktivitäten nicht nur geplant, sondern auch präzise durchgeführt, um sicherzustellen, dass die Ergebnisse ein breites Publikum erreichen und auch nach Abschluss des Projekts eine langfristige Wirkung haben.

Das TRANSIT-Projekt hat sich an einer Vielzahl von Verbreitungsaktivitäten beteiligt, wie im Förderantrag und in der nachfolgenden Planung dargelegt. Diese Aktivitäten umfassten Präsentationen, die Entwicklung einer Projektwebsite, die Verteilung von Werbematerialien, die Teilnahme an Messen, die Einbindung von universitären Forschungen durch Abschlussarbeiten, die Veröffentlichung von Papieren und die gemeinsame Nutzung von Open-Source-Code

auf GitHub. Zusätzlich wurde das Projekt durch das Engagement des Labors und seines Netzwerks verbreitet, was in der in der Excel-Datei bereitgestellten Veranstaltungsliste dokumentiert ist.

Präsentationen

Präsentationen waren ein Eckpfeiler der Verbreitungsstrategie und boten eine Plattform für das Projektteam, um direkt mit Interessengruppen und interessierten Parteien in Kontakt zu treten. Die Präsentationen deckten ein breites Themenspektrum ab, von den Anfangskonzepten und Rahmenbedingungen bis zu den Endergebnissen und dem Potenzial für zukünftige Anwendungen. Die Präsentationen fanden bei verschiedenen Veranstaltungen statt, darunter:

- **Master in Logistics Conference**: Diese Veranstaltung bot eine Gelegenheit, Einblicke mit akademischen Fachleuten und Branchenexperten über den internationalen Kollaborationsaspekt des Projekts zu teilen.
- **DTM Vernetzungskonferenz**: Die Netzwerkkonferenz in Berlin war ein bedeutendes Ereignis, das verschiedene Stakeholder zusammenbrachte, um über die Integration des Projekts und das Potenzial zur Schaffung eines vernetzten Datenmanagementsystems zu diskutieren.
- **Datentag- Chancen einer Datentreuhand:** Zu der Veranstaltung der Stiftung Datenschutz wurden Vertreter des Projektes Transit eingeladen, wobei auf dieser Veranstaltung nicht nur der aktuelle Stand der Forschung sondern auch die Bemühungen aus der Wirtschacht und der Rechtsgelehrten genauer erörtert wurde wie Datentreuhandplattformen etabliert werden können und sollten.
- **Forschungsinterview BMBF Begleitforschung**: Ein Online-Interview, das es ermöglichte, die Projektergebnisse mit einer breiteren Forschungsgemeinschaft zu teilen und die neben dem BMBF durchgeführte Forschung zu betonen

Projektwebsite und Werbematerialien

Die Website https://transit-project.de/ dient als digitales Gesicht des Projekts und bot der Öffentlichkeit und den Stakeholdern zugängliche Informationen. Sie wurde kontinuierlich mit Projektmeilensteinen, Nachrichten und Ressourcen wie den herunterladbaren Flyern aktualisiert. Die Website, zusammen mit Flyern und anderen Werbematerialien, half dabei, ein konsistentes und professionelles Image für das Projekt aufrechtzuerhalten. Weiterhin kann die finale Plattform TRANSIT über einen Menüpunkt erreicht werden.

Die benannten Flyer wurden bei zahlreichen Gelegenheiten verteilt wie in den foglenden Unterabschnitten aufgezählt.

Messen und Universitätsarbeiten

Die Teilnahme an der Logistikmesse in München und die Einbindung von Forschungsarbeiten der Universität in Form von Bachelor- und Masterarbeiten waren ebenfalls ein wesentlicher Teil der Verbreitungsstrategie. Die Messeauftritte, wie beispielsweise auf der Münchner Messe für Transport-Logistik, boten eine hervorragende Gelegenheit, direktes Feedback von Branchenvertretern zu erhalten und Kooperationsbeziehungen aufzubauen. Die Abschlussarbeiten stärkten die akademische Verankerung des Projekts und trugen zur Ausbildung der nächsten Generation von Fachkräften bei.

Diese waren:

- Datentreuhänder: Anomalieerkennung in Zugriffslogs

- KI-Preisbildung in einem Datentreuhänder der Logistik

Veröffentlichungen und Open-Source-Code

Wissenschaftliche Artikel und die Bereitstellung von Open-Source-Code auf Plattformen wie GitHub haben es ermöglicht, die Forschungsergebnisse und entwickelten Werkzeuge einem breiten Fachpublikum zur Verfügung zu stellen. Zum einen wurde das Paper „Federated Learning for Data Trust in Logistics“ (Koch et al. 2023) von Michael Koch auf der FEDCSIS 2023 – Konferenz einem breiten Publikum bereitgestellt. Mit der Innovativen Idee eines föderierten Lernens zu der Entwicklung eines gesamtheitlichen KI-Modells können die Daten der Logistiker in ihren lokalen Datenbanken belassen werden und nur die Modellupdates werden zu der Datentreuhandplattform übermittelt, welche die Modelle und das Training verwaltet.

Zum anderen konnte der Datentreuhänder auch international auf der ICTS 2023 in Indonesien mit der Idee einer Prozessautomatisierung mittels KI veröffentlicht werden (Kober et al. 2023).

Nach der Vollendung der Plattform wurde der Quellcode für die Plattform TRANSIT, bestehenden aus Frontend und Backend (Kober und Koch 2024b), sowie der Programmcode des Zugriffsservice (Kober und Koch 2024a) auf github.com veröffentlich. Diese können anderen Entwicklern Einsichten in die mögliche Umsetzung eines Datentreuhänders, sowie einen Startpunkt für eigene Entwicklung geben.

Diese transparente Form des Wissensaustauschs hat nicht nur zur Reputation des Projekts beigetragen, sondern auch den Grundstein für weiterführende Forschung und Entwicklung gelegt.

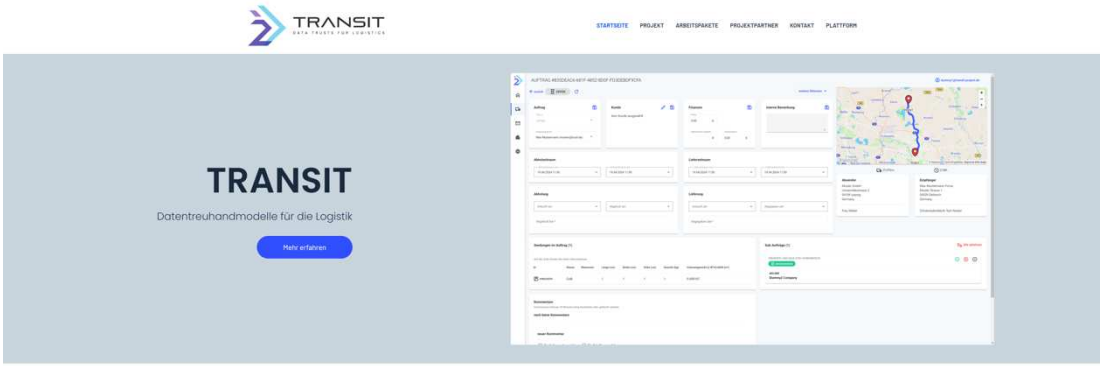

Abbildung 27: Webseite des Projektes TRANSIT

Abbildung 28:: Flyer TRANSIT-Projekt

Verbreitung über das Lab

Im Rahmen von mehreren Veranstaltungen zur Präsentation der Forschungsprojekte an welchen das Logistics Living Lab beteiligt ist und war, wurde das Projekt Transit vielen Interessenten aus Forschung und Wirtschaft vorgestellt. Eine Zusammenfassung der Veranstaltungen ist im Folgenden aufgeführt:

- **20.06.2022:** Besuch des Referat Digitale Stadt Leipzig
- **22.06.2022**: Besuch einer medizinischen Delegation aus Polen im Rahmen des Heartbit EU Projektes
- **29.06.2022:** Besuch der ungarischen Botschaftsdelegation
- **08.07.2022:** Besuch der Arbeit und Leben e.V.
- **15.07.2022**: Besuch der Digitalagentur Sachsen
- **19.09.2022**: Besuch einer technischen Delegation aus Tunesien von der ENETCOM – SEPT Universität
- **23.06.2023**: Besucher während der Lange Nacht der Wissenschaften
- **31.01.2024**: Besuch von DB Schenker Logistik Abteilung

Projektaustausch mit von BMBF geförderten Projekten

Es fanden Interviews und Austausch mit anderen Projekten in einen regen Austausch statt, welche über die Organisation der Veranstaltungen des Projektträgers hinaus gingen, wo übergreifende Themen diskutiert und Forschungsrichtungen und Erkenntnisse geteilt wurden. Diese Veranstaltungen umfassen:

- **20.08.2022:** Besuch des Referat Digitale Stadt Leipzig
- **15.04.2023**: Interview im Rahmen des ReFo_DaT Projektes

Verbreitung über Logistikpartner

Im Rahmen der Verbreitungsstrategie wurde auch potentielle Partner und Nutzer der Datentreuhandplattform angesprochen, welche zu einer Projektvorstellung in ihr Büro geladen haben.

Dazu zählen folgende Termine:

- **24.01.2023**: Projektvorstellung Peternek & Funke Logistik
- **03.03.2023**: Projektvorstellung Wirth GmbH

Verwertung der Ergebnisse

Nach Abschluss des Projektes ist die Weiternutzung und Wartung der programmierten Plattform im Netzwerk Logistik Mitteldeutschland vorgesehen.

Netzwerk Logistik Mitteldeutschland

Der Netzwerk Logistik Mitteldeutschland e.V. engagiert sich aktiv für die Förderung und Unterstützung seiner Mitglieder, die aus Logistikern, logistiknahen Dienstleistern, öffentlichen Verwaltungen, Kammern sowie Forschungs- und Bildungseinrichtungen bestehen. Mit rund 140 Mitgliedern dient es als Plattform, die Kooperation, Austausch und die Initiierung neuer Projekte anregt. Ziel ist es, den Logistikstandort Mitteldeutschland weiterzuentwickeln und als etabliertes Gateway nach Europa sowie als zentralen Distributionsstandort mit schnellen Anbindungen zu osteuropäischen und ostasiatischen Märkten zu fördern. Dies geschieht durch Präsenz auf Messen und Veranstaltungen im In- und Ausland.

Das Netzwerk kooperiert im Bereich Personal mit regionalen Arbeitsvermittlern, Personaldienstleistern und Qualifizierungsanbietern und stärkt die Zusammenarbeit mit anderen Clustern in der Region. Die Geschäftsstelle befindet sich am Flughafen Leipzig/Halle, mit weiteren Regionalbüros in Dresden und Chemnitz sowie einer Repräsentanz in Moskau.

Expertengruppen innerhalb des Netzwerks entwickeln kontinuierlich Strategien zur Steigerung der Wettbewerbsfähigkeit der Region, einschließlich Maßnahmen gegen den Fachkräftemangel und zur Förderung von Innovationen sowie aktuelle Informations- und Unterstützungsangebote (Netzwerk Logistik Mitteldeutschland 2024).

Monetarisierung

Durch eine Mitgliedergebühr sollen laufende Kosten und Wartung gedeckt werden. Der monatliche Betrag von ca. 70€ soll die Weiterentwicklung durch einen Softwareentwicklung abdecken, wenn auch nicht Vollzeit.

Sobald Extra-Dienstleistungen, wie eine Benutzerspezifische Auswertung und Dashboard angeboten werden können, sollen auch diese eine Zusatzvergütung einbringen.

Mit dem Betrieb in dem e.V. sollen zunächst den Mitgliedern Vertrauensängste genommen. Später, wenn genügend Mitglieder die Plattform aktiv nutzen, sollen durch Öffentlichkeitsarbeit und Werbung, weitere Logistiker an die Plattform herangeführt werden.

Betrieb im e.V.

Der Weiterbetreib der Software und die Datenspeicherung soll weiter an der Universität Leipzig angesiedelt sein. Hierbei ist auch eine Wartung durch die InfAI e.V. als Softwaredienstleiter möglich. Eine weitere Möglichkeit ist die Übernahme des Softwareweiterbetriebes durch das Netzwerk Logistik Mitteldeutschland e.V. wurde auch als Möglichkeit betrachtet, da durch die Mitgliedschaftsgebühren der Betreib und die Wartung weiterfinanziert werden können.

Die Einbringung der direkten Projektergebnisse in weitere Projekte wurde auch geplant und beantragt, wurde aber aufgrund des großen Interesses welcher mit der ersten Förderrichtlinie mit Datentreuhandplattformen einherging, bisher noch nicht erfolgreich umgesetzt und ist immer noch in Arbeit. Einzelne Teilkomponenten oder auch weitere Aspekte, welche im Rahmen der Veröffentlichungen näher betrachtet wurden, werden in neuen Projekten intensiver behandelt.

Des Weiteren ist jetzt und auch im Folgenden ein intensiver Austausch auf Konferenzen und Messen, sowie innerhalb von Presseterminen im Lab, die Vorstellung des Projektes geplant, um auch zukünftig mit entsprechenden Interessenten an Datentreuhandplattformen neue Ansätze für Datentreuhandplattformen im Rahmen von Förderprogrammen erforschen zu können.

Referenzen

Aichroth, Patrick; Battis, Verena; Dewes, Andreas; Dibak, Christoph; Doroshenko, Vadym; Geiger, Bernd et al. (2020): Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens: BITKOM. Online verfügbar unter https://publica.fraunhofer.de/entities/publication/1bae2aea-5805-4437-9279-7bde0ce60954/details.

B, Harshitha; N.S, Veerabhadra Swamy (2015): A Survey on Existing Network Security Protocols.

Balsa, Ero; Nissenbaum, Helen; Park, Sunoo (2022): Cryptography, Trust and Privacy: It's Complicated. In: Daniel J. Weitzner (Hg.): Proceedings of the 2022 Symposium on Computer Science and Law. CSLAW '22: Symposium on Computer Science and Law. Washington DC USA, 01 11 2022 02 11 2022. New York,NY,United States: Association for Computing Machinery (ACM Digital Library), S. 167–179.

Bernhard, Jochen; Hömberg, Kay; Jodin, Dirk; Kuhnt, Sonja; Schürmann, Christoph; Wenzel, Sigried (2007): Vorgehensmodell zur Informationsgewinnung–Prozessschritte und Methodennutzung. Online verfügbar unter https://eldorado.tu-dortmund.de/bitstream/2003/25931/1/technical%20report%2006008.pdf.

Blankertz, Aline (2020): Designing Data Trusts: Why We Need to Test Consumer Data Trusts Now.

Dewes, Andreas (2022): Verfahren zur Anonymisierung und Pseudonymisierung von Daten. In: Marieke Rohde, Matthias Bürger, Kristina Peneva und Johannes Mock (Hg.): Datenwirtschaft und Datentechnologie. Wie aus Daten Wert entsteht. Berlin, Heidelberg: Springer Vieweg (Open Access), S. 183–201. Online verfügbar unter https://link.springer.com/chapter/10.1007/978-3-662-65232-9_14.

IBM Analytics (2016): Analytics Solutions Unified Method. Online verfügbar unter ftp://ftp.software.ibm.com/software/data/sw-library/services/ASUM.pdf.

Kober, Sascha; Koch, Michael (2024a): Fine-Grained-Object-Specific-Policy-Machine. Online verfügbar unter https://github.com/TRANSIT-Infai/Fine-Grained-Object-Specific-Policy-Machine, zuletzt aktualisiert am 30.06.2024, zuletzt geprüft am 30.06.2024.

Kober, Sascha; Koch, Michael (2024b): TRANSIT-Project. Online verfügbar unter https://github.com/TRANSIT-Infai/TRANSIT-project, zuletzt aktualisiert am 30.06.2024, zuletzt geprüft am 30.06.2024.

Kober, Sascha; Koch, Michael; Gaunitz, Benjamin; Franczyk, Bogdan (2023): Data Trust in Logistics: Price Prediction for Collaboration. In: 2023 14th International Conference on Information & Communication Technology and System (ICTS), S. 29–34.

Koch, Michael; Kober, Sascha; Straburzynski, Stanislaw; Gaunitz, Benjamin; Franczyk, Bogdan (2023): Federated Learning for Data Trust in Logistics. In: Position Papers of the 18th Conference on Computer Science and Intelligence Systems: PTI.

Netzwerk Logistik Mitteldeutschland. EIN NETZWERK FÜR LOGISTIKER IN MITTELDEUTSCHLAND (2024). Online verfügbar unter http://www.logistik-mitteldeutschland.de/, zuletzt aktualisiert am 30.06.2024, zuletzt geprüft am 30.06.2024.

Richard K. Lomotey; Sandra Kumi; Ralph Deters (2022): Data Trusts as a Service: Providing a platform for multi-party data sharing. In: *International Journal of Information Management Data Insights* 2 (1), S. 100075. DOI: 10.1016/j.jjimei.2022.100075.

Schwartmann, Professor Rolf; Jaspers, Andreas; Lepperhoff, Niels; Weiß, Steffen; Meier, Professor Michael (2022): Praxisleitfaden zum Anonymisieren personenbezogener Daten. Anforderungen, Einsatzklassen und Vorgehensmodel.

Shafique, Umair; Qaiser, Haseeb (2014): A comparative study of data mining process models (KDD, CRISP-DM and SEMMA). In: *International Journal of Innovation and Scientific Research* 12 (1), S. 217–222.

Winter, Christian; Battis, Verena; Halvani, Oren (2019): Herausforderungen für die Anonymisierung von Daten, S. 339–352. Online verfügbar unter https://dl.gi.de/items/d5aeee27-49cb-4813-93b8-5a0470e8cb28.