



Foto: iStock.com/sanjeri / Bearbeitung: Fraunhofer SIT

EduMiDa – Erfolg durch Mitarbeiterdatenschutz

Teilvorhaben: IT-Sicherheits- und datenschutzrechtlich- ökonomische Aspekte

Sachbericht zum Verwendungsnachweis

Teil I: Kurzbericht

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Projekttitle	Erfolg durch Mitarbeiterdatenschutz
Akronym	EduMiDa
Titel des Teilvorhabens	IT-Sicherheits- und datenschutzrechtlich-ökonomische Aspekte
Förderkennzeichen	16KIS1361K
Zuwendungsempfänger	Fraunhofer-Institut für Sichere Informations-technologie (SIT)
Laufzeit des Vorhabens	01.06.2021 – 31.03.2024
Ansprechpartnerin	Dr. Annika Selzer

1 Aufgabenstellung und Forschungsgegenstand

Aufgrund des hohen Kostendrucks können sich Unternehmen heutzutage kaum Phasen erlauben, in denen Beschäftigte keine betrieblichen Aufgaben erledigen. Um diese Leerlaufzeiten und damit verbundene Kosten zu vermeiden, ist eine agile Ressourcenplanung wichtig. Besonders vielversprechend sind Echtzeiterhebungen von Attributen, beispielsweise den Echtzeit-Standortdaten der Beschäftigten. Dabei kommt es darauf an, entsprechende Erhebungen datenschutzfreundlich zu gestalten und die Beschäftigten zu schützen. Ziel des Teilprojekts war es, automatisiert verifizierbare Datenschutzmetriken zu entwickeln. Das Teilvorhaben des Fraunhofer SIT hatte im Wesentlichen die folgenden technischen und datenschutzrechtlich-ökonomischen Ziele:

- Identifikation von Anforderungen der IT-Sicherheit.
- Definition von Datenschutzmetriken (gemeinsam mit den Projektpartnern).
- Beschreibung einer Architektur für den EduMiDa-Demonstrator sowie Entwicklung des Demonstrators (gemeinsam mit dem Anwendungspartner).
- Evaluation der datenschutzrechtlich-ökonomischen Rahmenbedingungen von Metriken.
- Datenschutzrechtlich-ökonomische Untersuchung, wie die Angemessenheit von Datenschutzmaßnahmen systematisch und nachvollziehbar bewertet werden kann.
- Rechtlich-ökonomische und IT-sicherheitstechnische Evaluation des Demonstrators.

Die datenschutzrechtlichen Anforderungen, die im Rahmen von EduMiDa auf Basis automatisiert verifizierbarer Datenschutzmetriken überprüft werden sollten, sowie die Anforderungen an die EduMiDa-Lösung selbst ergaben sich insbesondere aus der Datenschutz-Grundverordnung sowie dem neuen Bundesdatenschutzgesetz.

2 Ablauf des Vorhabens

Die Gesamtlaufzeit des Projekts betrug 34 Monate vom 1. Juni 2021 bis zum 31. März 2024. Zu Beginn des Projektes wurden Anwendungsfälle der Umplanung von Beschäftigten an verschiedenen Arbeitsplätzen in der Intralogistik identifiziert und zwei davon für die Umsetzung ausgewählt: 1. Mehrbedarf an Beschäftigten und 2. Umplanung wegen eines Technikausfalls.

Schritt 1: Entwicklung von Kennzahlen und Messverfahren: Fraunhofer SIT entwickelte Kennzahlen und Messverfahren, die geeignet sind, die Umsetzung des Mitarbeiterdatenschutzes zu kontrollieren und belastbare Aussagen über den Status des Datenschutzniveaus zu liefern. Das Datenschutzrecht war der Ausgangspunkt der Metriken, Mess- und Vergleichsverfahren, z. B. in Bezug auf Anforderungen an die Löschung personenbezogener Standortdaten.

Schritt 2: Ableitung konkreter Maßnahmen und Identifizierung geeigneter Datenquellen: Aus den rechtlichen Anforderungen wie die Datenminimierung und Speicherbegrenzung wurden konkrete Maßnahmen abgeleitet (z. B. „Eine grundlose Erhebung von Mitarbeiterstandorten ist zu unterlassen.“) und die Architektur des Metrikensystems festgelegt. Datenquellen (z. B. Standortdaten von Beschäftigten, Anzahl der Standortabfragen, Aufbewahrungszeit) wurden auf ihre Aussagekraft überprüft und priorisiert.

Schritt 3 Umsetzung eines Demonstrators: Fraunhofer SIT unterstützte den Anwendungspartner bei der Auswahl der Metriken für die Implementierung und Testung des Demonstrators.

Schritt 4: Evaluation der EduMiDa-Lösung: Als Teil der Evaluation wurden die Praktikabilität, Datenschutzkonformität und IT-Sicherheit der Lösung betrachtet.

3 Wesentliche Ergebnisse

Die Architektur des Metrikensystems sieht einen EduMiDa-Proxy vor, der auf Basis von Echtzeit-Standortdaten die Beschäftigten (die dem Ziel-Arbeitsplatz am nächsten sind) für eine Umplanung auswählt, die Vorgänge protokolliert und entsprechende Datenschutzmetriken berechnet. Zur Darstellung des erreichten Datenschutzes ist eine EduMiDa-App vorgesehen. Diese sorgt für Transparenz für die Beschäftigten. Über die App können sie Information über Anlässe der Umplanung und erfolgte Standortbestimmungen ansehen.

Für die Überprüfung der Datenminimierung wurden Metriken z. B. zur Beschränkung von Standortbestimmungen und Standortabfragen sowie zur Unterlassung unbegründeter Standortermittlungen entwickelt. Für die Überprüfung der Speicherbegrenzung dienen Metriken zur Löschung der Standortdaten nach Beendigung der Umplanung und nach Erfüllung des Verarbeitungszwecks. Zudem wurden

Metriken für den Zugangs- und Zutrittsschutz sowie für die Verschlüsselung und Datenintegrität entwickelt. Diese Datenschutzmetriken bieten Hinweise auf Datenschutzverstöße und Umsetzungsmängel und können dadurch zur Verbesserung des Datenschutzes beitragen. Die Metriken lassen sich auch auf andere Szenarien mit personenbezogenen Standortdaten und anderen Sensordaten (z. B. Daten von Wearables) übertragen. Ein Metriken-Dashboard gibt Übersichten über Kennzahlen in Form von Diagrammen von aggregierten Kennzahlen (über Zeiträume, Anlässe, Beschäftigte etc.) und realisiert unterschiedliche Sichten z. B. für Beschäftigte, Geschäftsleitung oder Datenschutzbeauftragte.

Die Verarbeitung der Daten ist angemessen, denn die Daten werden nur anlassbezogen vom Proxy abgerufen und verarbeitet. Zudem werden nur Daten von denjenigen erhoben, die für Umplanung auch qualifiziert sind. Die Verarbeitung ist erheblich, weil die Personaleinsatzplanung nur die Standorte der Beschäftigten anfragt, die auch gerade anwesend und abkömmlich sind. Die Verarbeitung ist beschränkt, weil nur die für die Umplanung notwendigen Daten erhoben werden. Der Zugriff ist zudem eingeschränkt und rollenbasiert. Die Messdaten und berechneten Standortdaten werden laufend überschrieben und nach erfolgter Umplanung gelöscht. Die Personaleinsatzplanung bekommt nur pseudonyme Kennungen und kann diese den Beschäftigten zuordnen.

Die datenschutzrechtlich-ökonomische Untersuchung ergab, dass für die datenschutzkonforme Gestaltung neu geplanter Metrikensysteme im Wesentlichen die folgenden vier Schritte umzusetzen sind: 1. Die Entscheidung darüber, ob das neu geplante Metrikensystem personenbezogene oder anonyme Daten verarbeiten soll; 2. Die Vorprüfung der Machbarkeit aus rechtlicher und technischer Sicht; 3. Die Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts, z. B. der Planung des Einholens einer Einwilligung und der Planung der Umsetzung von Löschpflichten; 4. Die Planung der Umsetzung technischer und organisatorischer Schutzmaßnahmen, wie z. B. die Umsetzung des Vier-Augen-Prinzips und das Verschlüsseln von Daten. Die Ergebnisse sind dafür vorgesehen, den Umsetzungsgrad des Datenschutzes von Beschäftigten im laufenden Betrieb kontinuierlich zu verifizieren. Dies macht die Datenschutzabläufe im Unternehmen transparent und ermöglicht, gemäß den gesetzlichen Vorgaben, umgehend auf eventuelle Datenschutzverstöße zu reagieren.

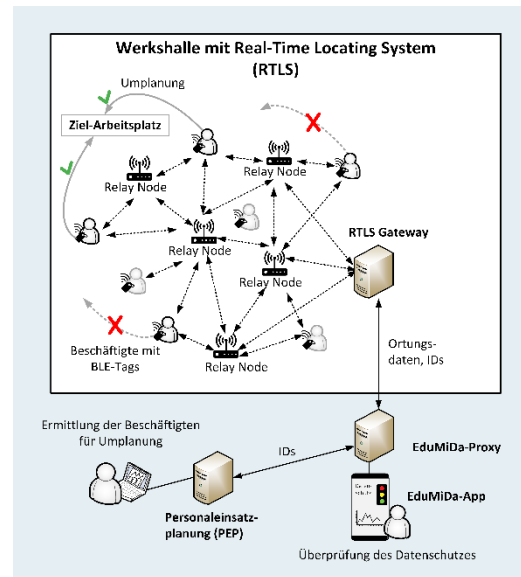




Foto: iStock.com/sanjeri / Bearbeitung: Fraunhofer SIT

EduMiDa – Erfolg durch Mitarbeiterdatenschutz

Teilvorhaben: IT-Sicherheits- und datenschutzrechtlich- ökonomische Aspekte

Sachbericht zum Verwendungsnachweis

Teil II: Eingehende Darstellung

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Projekttitel	Erfolg durch Mitarbeiterdatenschutz
Akronym	EduMiDa
Laufzeit des Vorhabens	01.06.2021 – 31.03.2024
Förderkennzeichen	16KIS1361K
Zuwendungsempfänger	Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Ansprechpartner/in	Dr. Annika Selzer
Projektpartner	p.i.i. solutions GmbH (PLI) Universität Bremen (UNIB) Westfälische Wilhelms-Universität Münster (WWU)
Datum	3. September 2024

Die in diesem Bericht enthaltenen Arbeitsergebnisse sind sorgfältig und unter Zugrundelegung des bekannten Standes der Wissenschaft erstellt worden, stellen jedoch Forschungsansätze dar. Eine Haftung oder Garantie dafür, dass die Arbeitsergebnisse/Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird aus diesem Grund nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Inhalt

1	Zusammenfassung der Projektziele	4
2	Erzielte Ergebnisse	5
2.1	Anwendungsszenarien (Arbeitspaket 1).....	5
2.2	Anforderungsanalyse und rechtlich-ökonomische Untersuchung (Arbeitspaket 2)	9
2.3	Metrikenspezifikation (Arbeitspaket 3).....	12
2.3.1	Vorgehensweise	13
2.3.2	Definition der Datenschutzmetriken.....	14
2.4	Architekturbeschreibung (Arbeitspaket 4).....	21
2.4.1	Prozesse im EduMiDa-System.....	22
2.4.2	Umsetzung des Datenschutzes.....	24
2.4.3	Sicherheitseigenschaften von BLE-Mesh	25
2.5	Testumgebung (Arbeitspaket 5).....	25
2.6	Metrikenimplementierung (Arbeitspaket 6).....	26
2.6.1	Darstellung der Datenschutzmetriken.....	26
2.6.2	Definition von Use-Cases für den Demonstrator	27
2.7	Evaluation (Arbeitspaket 7)	27
2.7.1	Evaluation des Gestaltungsvorschlags.....	27
2.7.2	Evaluation des Demonstrators	28
2.7.3	Angemessenheit von Metrikensystemen für den Mitarbeiterdatenschutz	28
2.7.4	Evaluation des Demonstrators aus Sicht der IT-Sicherheit.....	30
3	Wichtigste Positionen des zahlenmäßigen Nachweises	31
4	Notwendigkeit und Angemessenheit der geleisteten Arbeit	31
5	Darstellung des Verwertungsplans	31
6	Darstellung des Fortschritts auf dem Gebiet des Vorhabens	32
7	Darstellung der erfolgten oder geplanten Veröffentlichungen	33

1 Zusammenfassung der Projektziele

Das übergeordnete Ziel von EduMiDa war die Entwicklung neuer Ansätze und Tools zur Modellierung und Quantifizierung von Eigenschaften zur Erfüllung von Datenschutzanforderungen bei der Verarbeitung von Mitarbeiterdaten auf Basis von Metriken für den Mitarbeiterdatenschutz. Somit kann das Unternehmen einerseits selbst sicherstellen, bei der Verarbeitung ihrer Mitarbeiterdaten die geltenden Datenschutzbestimmungen – insbesondere die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG) – angemessen umzusetzen und somit den hohen Bußgeldrahmen der Datenschutz-Grundverordnung zu vermeiden. Andererseits wird für die einzelnen Mitarbeiter nachvollziehbar, wie der Mitarbeiterdatenschutz im Unternehmen umgesetzt ist, was wiederum Vertrauen in den Arbeitgeber schafft und das Unternehmen als attraktiven Arbeitgeber stärkt. Auch interne Fachstellen – wie z. B. der Betriebsrat und der betriebliche Datenschutzbeauftragte eines Unternehmens – sowie externe Stellen wie bspw. die jeweils zuständige Datenschutz-Aufsichtsbehörde könnten sich bei Bedarf mit Hilfe der Datenschutzmetriken von der datenschutzkonformen Umsetzung des Mitarbeiterdatenschutzes im Unternehmen überzeugen, wodurch z. B. auch einer Vielzahl an Mitwirkungs- und Kontrollpflichten des Betriebsrats und betrieblichen Datenschutzbeauftragten nachgekommen werden kann. Bei der Entwicklung der Metriken waren auch die Besonderheiten der neuen Arbeitswelt in Bezug auf die Notwendigkeit der Standortbestimmung von Mitarbeitern und in Bezug auf feste, entliehene und freie Mitarbeiter sowie ggf. agile Wechsel zwischen diesen „Rollen“ zu berücksichtigen.

Ziele des Teilvorhabens

Das Teilvorhaben hatte im Wesentlichen die folgenden technischen sowie datenschutzrechtlich-ökonomischen Ziele:

- Identifikation von Anforderungen der IT-Sicherheit, deren Umsetzung auch in der DSGVO explizit geregelt ist.
- Definition von Datenschutzmetriken (gemeinsam mit den Projektpartnern).
- Beschreibung einer Architektur für den EduMiDa-Demonstrator sowie Entwicklung des Demonstrators (gemeinsam mit dem Projektpartner p.l.i. solutions).
- Evaluation der datenschutzrechtlich-ökonomischen Rahmenbedingungen von Metriken im Allgemeinen und für den Mitarbeiterdatenschutz im Speziellen.
- Datenschutzrechtlich-ökonomische Untersuchung, wie die Angemessenheit von Datenschutzmaßnahmen systematisch, ausgewogen und nachvollziehbar bewertet und kategorisiert werden kann, um Datenschutzmetriken für den Mitarbeiterdatenschutz angemessen umsetzen zu können.
- Evaluation des Demonstrators aus rechtlich-ökonomischer Sicht und aus IT-Sicherheitssicht.

Um die vorgenannten Ziele des Teilvorhabens zu erreichen, musste das Projekt den folgenden bisher ungelösten Problemen und Herausforderungen begegnen:

- **Unternehmen kennen den ökonomischen Nutzen von Mitarbeiterdaten und Mitarbeiterdatenschutz nicht.**

EduMiDa adressierte dieses Problem durch eine Analyse der Wirtschaftlichkeit von Mitarbeiterdaten und des Mitarbeiterdatenschutzes und einer Quantifizierung deren Kosten und Nutzen.

- **Unternehmen verfügen über keine Werkzeuge, mit denen sie den Grad der Umsetzung des Mitarbeiterdatenschutzes messen und transparent machen können.**

EduMiDa adressierte dieses Problem durch die Entwicklung eines Verfahrens zur automatisierten Verifikation von Datenschutzerfordernungen für den Mitarbeiterdatenschutz, die auch zur Unterstützung von Kontroll- und Mitwirkungspflichten von Datenschutzbeauftragten und Betriebsräten verwendet werden können.

- **Arbeitnehmern fehlen Möglichkeiten, die Rechtmäßigkeit ihrer Daten zu kontrollieren und die Verarbeitung aktiv zu beeinflussen.**

EduMiDa adressierte dieses Problem, indem es Mitarbeiter durch das entwickelte Metrikensystem in die Lage versetzt zu sehen, welche Daten durch den Arbeitgeber verarbeitet werden und darüber hinaus ermöglicht aktiv auf die Datenverarbeitung einzuwirken, z. B. durch das Anstoßen einer Löschung von Bewegungsdaten nach dem Aufsuchen eines sensiblen Orts (z. B. Aufsuchen einer Spezialklinik in der Mittagspause).

2 Erzielte Ergebnisse

Das folgende Kapitel stellt die von Fraunhofer SIT erzielten Projektergebnisse anhand der Arbeitspakete, im Rahmen derer die Ergebnisse erzielt wurden, vor.

2.1 Anwendungsszenarien (Arbeitspaket 1)

Der Projektpartner p.l.i. solutions GmbH verfügt über Kunden aus den Bereichen Logistik, Produktion, Einzelhandel, Dienstleistungen, Health-Care und IT-Services. Um die Anwendungsszenarien des EduMiDa-Projektes definieren zu können, musste zunächst die Auswahl des Anwendungsschwerpunkts aus einen dieser sechs Bereiche erfolgen. Nach mehreren geleiteten Diskussionen entschied sich das Konsortium, den EduMiDa-Anwendungsschwerpunkt auf den Bereich der Logistik zu legen. Dies erfolgte insbesondere aus den folgenden Gründen:

- Die agile Mitarbeiterereinsatzplanung ist in der Logistik höchstrelevant – bereits Ausfallzeiten von 15-30 Minuten führen zur tiefgreifenden Umplanung des Personaleinsatzes.
- Die Erhebung von Standortdaten der Beschäftigten – einem der im EduMiDa-Projektantrag als Schwerpunkt beschriebenen Anwendungsszenarien – spielt für die agile Mitarbeiterereinsatzplanung in der Logistik eine große Rolle, da die relevanten Betriebsgelände bis zu 100.000 Quadratmeter betragen.
- Aufgrund der angespannten Beschäftigungssituation in der Logistik ist die Überprüfung der Einhaltung von Erholungspausen der Beschäftigten sehr wichtig, da Beschäftigte dazu neigen, auf ihre Erholungspausen zu verzichten – dieser Umstand muss in der Personaleinsatzplanung Berücksichtigung finden.

- Auch wenn Logistikunternehmen Arbeitssicherheitsmaßnahmen, wie z. B. Brandschutzmaßnahmen, umsetzen, besteht in der Logistik eine erhöhte Gefahr für Unfälle und Verletzungen. Die Erhebung von besonderen Kategorien personenbezogener Daten, wie etwa den Vitalwerten (u. a. Körpertemperatur, Herzfrequenz, Blutdruck) der Beschäftigten, die aus datenschutzrechtlicher Sicht einem besonders hohen Schutz unterliegen und sich daher zur Überprüfung der datenschutzkonformen Verarbeitung durch ein Datenschutzmetrikensystem besonders eignen, kann die Gefahr von Unfällen und Verletzungen eindämmen bzw. die schnelle Versorgung des verletzten Beschäftigten unterstützen.
- Obwohl – oder gerade weil – die Beschäftigungssituation in der Logistik angespannt ist, setzen sich die Betriebsräte der Logistikunternehmen sehr stark für die Beschäftigten ein und haben hinsichtlich der Überwachung von Vitalwerten und Standortdaten der Beschäftigten eine tendenziell ablehnende Haltung – der Bedarf an einem Datenschutzmetrikensystem, der die Erhebung solcher Daten erlaubt, aber dessen datenschutzkonforme Umsetzung für den Betriebsrat kontrollierbar macht, ist im Bereich der Logistik daher sehr hoch.

Aus diesen Gründen wurde der Bereich der Logistik als Anwendungsschwerpunkt des EduMiDa-Projektes ausgewählt, so dass sich die Anwendungsszenarien des Projektes aus diesem Bereich ergeben. Die Anwendungsszenarien wurden durch Fraunhofer SIT und p.l.i. solutions definiert und – hinsichtlich der Motivation des Anwendungsszenarios, der im Szenario verarbeiteten personenbezogenen Datenarten und der im Szenario bestehenden Datenverarbeitungsumstände (z. B. beteiligte Organisationen, Drittstaatübermittlungen, Auftragsverarbeitungsverhältnisse) beschrieben. Sie umfassen:

- **Anwendungsszenario 1: Umplanung des Mitarbeiterereinsatzes wegen Technikausfall.** In einem Betriebsgelände von ca. 100.000 Quadratmetern fällt eine Maschine aus, die für den Ablauf des Logistikunternehmens zwingend erforderlich ist. In jeder Schicht gibt es mehrere Beschäftigte, die in der Lage wären, die Maschine zu reparieren. Durch die Verknüpfung des Mitarbeiterereinsatzplanungstools mit Standortdaten der Beschäftigten soll entschieden werden, welcher Beschäftigtensich am nächsten an der Maschine befindet und die Maschine daher am schnellsten erreichen und reparieren kann. Die Reparaturarbeiten können wenige Minuten bis mehrere Stunden andauern, der Kreis der Beschäftigten, die diese Aufgabe erledigen können, ist sehr gering.
- **Anwendungsszenario 2: Umplanung des Mitarbeiterereinsatzes wegen kurzfristiger Mehrbelastung.** In einem Betriebsgelände von ca. 100.000 Quadratmetern kommt es an einer Stelle kurzfristig – für ca. 15-60 Minuten zu einem erhöhten Bedarf am Einsatz von Beschäftigten. In der Regel lassen sich solche Aufgaben von nahezu allen anwesenden Beschäftigten unterstützen. Durch die Verknüpfung des Mitarbeiterereinsatzplanungstools mit Standortdaten der Beschäftigten soll entschieden werden, welche Beschäftigten sich am nächsten an dem Ort des Mehrbedarfs befindet und daher am schnellsten Unterstützung leisten könnten.
- **Anwendungsszenario 3: Planung von Pausen der Beschäftigten zur Gefahrenabwehr.** Die Beschäftigten eines Logistikunternehmens arbeiten häufig, ohne gesetzlich festgelegte Pausenzeiten zu berücksichtigen. Für das Logistikunternehmen ist es daher erforderlich, die Einhaltung von Pausenzeiten durch eine entsprechende

Auswertung von Standortdaten (hält sich der Beschäftigte wirklich außerhalb des Betriebsgeländes bzw. in den Pausenräumen auf?) zu überprüfen. Zusätzlich ist es möglich, dass Beschäftigte aufgrund eines hohen Arbeitsaufkommens oder einer zu langen starken körperlichen Belastung zusätzliche Erholungspausen benötigen. Vor diesem Grund ist aus Sicht der Logistikunternehmen die Überwachung der Vitalwerte (insbesondere Körpertemperatur, Herzfrequenz, Blutdruck) der Beschäftigten wünschenswert, um ggf. eine weitere Erholungspause der Beschäftigten anordnen zu können.

- **Anwendungsszenario 4: Nutzung von Mitarbeiterereinsatzplanungsdaten zur Bewältigung von Katastrophenfällen.** Im Katastrophenfall sollen die Daten des Mitarbeiterereinsatzplanungstools, Daten aus Anwesenheitskontrollen („Stechuhr“) und Standortdaten zusammengeführt werden, um so schnell wie möglich feststellen zu können, wie viele und welche Beschäftigte sich in einem Betriebsabschnitt befinden, in dem der Katastrophenfall besteht. Die Zusammenführung der Daten aus den verschiedenen Systemen soll unter anderem aufzeigen, ob ein Beschäftigter zwar für den Einsatz in dem Betriebsabschnitt vorgesehen war, in dem der Katastrophenfall besteht, er sich jedoch gerade nicht dort aufhält (oder umgekehrt). Als zusätzliche Option würden die Vitalwerte der Beschäftigten helfen, zu beurteilen, ob und welche Hilfe für die Beschäftigten notwendig ist.

Im Anschluss an die Identifizierung der Anwendungsszenarien wurden Themenfelder datenschutzrechtlicher Anforderungen identifiziert, auf die ebenfalls im Rahmen der Anwenderworkshops zurückgegriffen werden sollte: Auch wenn aus rechtlicher Sicht grundsätzlich sämtliche für eine bestimmte Datenverarbeitung einschlägigen Datenschutzerfordernungen umgesetzt werden müssen, so kann die Verifizierung des Umsetzungsgrades bestimmter Anforderungen aus Sicht möglicher Anwender besonders interessant sein, bspw. wenn sie dazu beitragen können, den Betriebsrat vom Einsatz von Mitarbeiterereinsatzplanungstools zu überzeugen. Vor diesem Hintergrund sollten die Teilnehmer der Anwenderworkshops die datenschutzrechtlichen Anforderungen hinsichtlich ihres Interesses an der automatisierten Verifizierung dieser Anforderungen im Rahmen der Nutzung eines Metrikensystems einordnen. Das Ergebnis dieses Schrittes sollte in die Priorisierung der im Rahmen von EduMiDa spezifizierten Metriken einfließen.

Die im Rahmen der Workshops zu bewertenden Anforderungen waren:

- Vorliegen einer einschlägigen Rechtsgrundlage (z. B. Einwilligung, Vertrag),
- Bedingungen an die Einwilligung zur Erhebung von Standortdaten (während Pausen),
- Bedingungen an die Einwilligung zur Erhebung von Vitalwerten (z. B. für Pausenregelungen, für den Katastrophenfall),
- Besondere Bedingungen an die Einwilligung von Mitarbeitern (insb. in Bezug auf die Freiwilligkeit),
- Datenminimierung und Speicherbegrenzung (nur notwendige Daten erheben und rechtzeitig löschen),
- Integrität und Vertraulichkeit (angemessene Umsetzung technischer und organisatorischer Schutzmaßnahmen),
- Auftragsverarbeitung (Datenverarbeitung durch Dienstleister),
- Drittstaatübermittlung (Datenverarbeitung durch Dienstleister außerhalb Europas),
- Betroffenenrechte (z. B. Recht auf Auskunft, Berichtigung, Löschung),

- Besondere Bedingungen des Arbeitsrechts (z. B. in Bezug auf die Einhaltung des Arbeitszeitgesetzes).

Nach Identifizierung dieser Anwendungsszenarien und Anforderungen wurden Anwenderworkshops vorbereitet, die zum Ziel hatten,

- die Relevanz der oben genannten Anwendungsszenarien zu bestätigen und/oder zusätzliche, für mögliche Anwender der EduMiDa-Arbeiten relevante Anwendungsszenarien zu identifizieren,
- die oben genannten sowie ggf. zusätzlich identifizierten Anwendungsszenarien in eine Reihenfolge hinsichtlich ihrer Relevanz aus Sicht möglicher Anwender zu bringen und
- zuvor identifizierte Themenfelder datenschutzrechtlicher Anforderungen in eine Reihenfolge aus Sicht möglicher Anwender zu bringen.

Die Workshopvorbereitung wurde vom Gesamtkonsortium durchgeführt. Fraunhofer SIT übernahm gemeinsam mit der Universität Bremen die Identifizierung der aus datenschutzrechtlicher Sicht relevanten rechtlichen Anforderungen und diskutierte wiederum gemeinsam mit p.l.i. solutions, wie diese rechtlichen Anforderungen im Rahmen der Anwenderworkshops am besten in ein Ranking münden können (u. a. in Bezug auf notwendige Wissensvermittlungen der Workshopteilnehmer als Grundlage eines durch sie erfolgenden Rankings). Alle Partner diskutierten gemeinschaftlich die Auswahl der zur Durchführung der Workshops eingesetzten Softwarelösung. Die Universität Münster skizzierte Orientierungspunkte für mögliche weitere Anwendungsszenarien. Die Workshops selbst wurden von p.l.i. solutions durchgeführt.

Die Workshops führten zu dem Ergebnis, dass die Anwendungsszenarien „Umplanung des Mitarbeiterinsatzes wegen Technikausfall“ und „Umplanung des Mitarbeiterinsatzes wegen kurzfristiger Mehrbelastung“ auf das größte Interesse stoßen. In Bezug auf die datenschutzrechtlichen Anforderungen ergab sich, dass alle im Rahmen der Workshops präsentierten Anforderungen aus Nutzersicht exakt gleichwertig und -wichtig sind und daher eine Priorisierung der Metriken aus Nutzersicht – in Vorbereitung der Metrikenspezifikation – nicht möglich war.

Im Rahmen des EduMiDa-Projektes werden dementsprechend die beiden Anwendungsszenarien „Umplanung des Mitarbeiterinsatzes wegen Technikausfall“ und „Umplanung des Mitarbeiterinsatzes wegen kurzfristiger Mehrbelastung“ im Mittelpunkt der weiteren Betrachtungen stehen.

Des Weiteren wurden im Rahmen des AP 1 die Zielgruppen des EduMiDa-Metrikensystems final festgelegt. Diese sind:

- **Geschäftsführung des Verantwortlichen:** Der Geschäftsführung soll durch die Nutzung des EduMiDa-Metrikensystems ermöglicht werden, zu überprüfen, ob die eigene Organisation bei der Verarbeitung ihrer Mitarbeiterdaten die geltenden Datenschutzbestimmungen angemessen umsetzt. Durch die Nutzung soll die Geschäftsführung insbesondere hohe Bußgelder gegen die Organisation sowie Reputationsschäden durch Datenschutzvorfälle (mit Auswirkungen für die Organisation) vermeiden.

- **Datenschutzbeauftragter des Verantwortlichen:** Dem Datenschutzbeauftragten soll durch die Nutzung des EduMiDa-Metrikensystems ermöglicht werden, zu überprüfen, ob die eigene Organisation bei der Verarbeitung ihrer Mitarbeiterdaten die geltenden Datenschutzbestimmungen angemessen umsetzt. Durch die Nutzung soll er insbesondere in die Lage versetzt werden, Maßnahmen zur Verbesserung des Datenschutzniveaus im Unternehmen zu unterbreiten und zu begründen.
- **Betriebsrat des Verantwortlichen:** Dem Betriebsrat soll durch die Nutzung des EduMiDa-Metrikensystems ermöglicht werden, zu überprüfen, ob die eigene Organisation bei der Verarbeitung ihrer Mitarbeiterdaten die geltenden Datenschutzbestimmungen angemessen umsetzt. Durch die Nutzung soll er insbesondere in die Lage versetzt werden, Datenverarbeitungen, die sowohl mit hohen Chancen für die Organisation und die Beschäftigten, aber auch mit Risiken für die Beschäftigten durch weitführende Datenverarbeitungen verbunden sind, aufgrund der Compliance-Kontrollfunktion im Rahmen ihrer Mitbestimmungsrechte zu ermöglichen und ggf. eine Entscheidung für eine Datenverarbeitung wieder zurückzunehmen, sofern die Metrikenergebnisse aufzeigen, dass die Datenverarbeitung nicht datenschutzkonform erfolgt.
- **Beschäftigte des Verantwortlichen:** Den Beschäftigten soll durch die Nutzung des EduMiDa-Metrikensystems ermöglicht werden, zu überprüfen, ob ihr Arbeitgeber bei der Verarbeitung der eigenen personenbezogenen Daten die geltenden Datenschutzbestimmungen angemessen umsetzt. Durch die Nutzung sollen sie insbesondere in die Lage versetzt werden, transparent über die Datenverarbeitung informiert zu werden und ggf. ihre Betroffenenrechte, inkl. des Rechts, sich bei der zuständigen Datenschutzaufsichtsbehörde zu beschweren, umzusetzen, sofern sie über die Ergebnisaufbereitung des Metrikensystems Datenschutzverstöße bemerken.
- **Zuständige Datenschutzaufsichtsbehörde:** Der zuständigen Datenschutzaufsichtsbehörde soll durch die Nutzung des EduMiDa-Metrikensystems ermöglicht werden, zu überprüfen, ob eine Organisation tatsächlich einen Datenschutzverstoß begangen hat, wenn sich ein Beschäftigter mit einer entsprechenden Beschwerde an sie wendet. Auch weitere Kontrollrechte der Datenschutzaufsichtsbehörde gegenüber der betreffenden Organisation könnten über das Metrikensystem (teilweise) durchgeführt werden.

Die verschiedenen Zielgruppen müssen insbesondere im Rahmen der Entwicklung der Benutzerschnittstellen Berücksichtigung finden, da die unterschiedlichen Nutzerrollen des Metrikensystems ggf. einer unterschiedlichen Aufbereitung der Messergebnisse bedürfen (u. a. in Bezug auf die Tiefe und die Art der Ergebnisdarstellung).

2.2 Anforderungsanalyse und rechtlich-ökonomische Untersuchung (Arbeitspaket 2)

Das Ziel dieses Arbeitspakets war eine strukturierte Erfassung von Anforderungen des Mitarbeiterdatenschutzes und von Anforderungen an die EduMiDa-Lösung selbst, u. a. durch Analyse der einschlägigen IT-Sicherheitsstandards, Rechtsvorschriften, Gesetzeskommentierungen und Rechtsprechung. Des Weiteren wurden rechtlich-ökonomische Untersuchungen durchgeführt und aus diesen weitere Anforderungen an die EduMiDa-Lösung abgeleitet.

Anforderungsanalyse IT-Sicherheit

In den EduMiDa-Anwendungsszenarien werden Daten von Beschäftigten der betreffenden Logistikunternehmen, beispielsweise Name, Qualifikation und Standortdaten, verarbeitet. Hierbei handelt es sich um personenbezogene Daten mit einem hohem Schutzbedarf. Die Hauptfunktionalität des EduMiDa-Systems ist die Berechnung und Darstellung von Datenschutzmetriken zur Überprüfung der datenschutzkonformen Verarbeitung dieser Daten. Die dazu benötigte vernetzte Informationstechnik des EduMiDa-Systems kann als IoT-Architektur betrachtet werden. Dabei lassen sich folgende vier Architekturebenen unterscheiden:

- **Datenerfassungsebene** zur Erhebung von Standortdaten und anderen personenbezogenen Daten der Beschäftigten durch heterogene Sensoren, zentrale und dezentrale Terminals und mobile Datenerfassungsgeräte über kontaktlose Schnittstellen. Die Datenerfassungsgeräte sind Teil des Firmennetzwerks.
- **Datenübermittlungsebene** mit drahtgebundener oder drahtloser Kommunikation der Komponenten mit lokalen Datenbanken, um die Messdaten zu erheben und zu filtern, in ihren jeweiligen Kontext zu stellen und zu speichern. Über das Internet werden die Daten ggf. an Cloud-basierte Anwendungen des betreffenden Unternehmens und an den EduMiDa-Service weitergeleitet.
- **Datenverarbeitungsebene** mit dem eigentlichen EduMiDa-Service in der Cloud. Dort werden Datenschutzmetriken berechnet. Die Ergebnisse werden über rollenbasierte Benutzungsschnittstellen der Anwendungsebene zur Verfügung gestellt.
- **Datenanwendungsebene** mit den Anwendungen für die Endnutzer des EduMiDa-Systems, beispielsweise die EduMiDa-App für die betroffenen Beschäftigten und Anwendungen für verschiedene Verwaltungssysteme, beispielsweise für das Workforce und Human Resource Management des betreffenden Unternehmens.

Die Vertrauenswürdigkeit der teilnehmenden Akteure wurde wie folgt festgelegt:

- **EduMiDa-Anbieter:** Dem Hersteller und Anbieter der EduMiDa-Anwendungssoftware wird vertraut.
- **EduMiDa-Anwender:** Kunden des EduMiDa-Anbieters. Diese werden grundsätzlich als vertrauenswürdig eingestuft, auch wenn einzelne Personen das Interesse besitzen könnten, mehr über die Beschäftigten zu erfahren als ihnen zusteht.
- **EduMiDa-Betroffene:** Die von der Metrikenerfassung betroffenen Personen, d. h. Beschäftigte des jeweiligen Logistikunternehmens. Diese gelten grundsätzlich als vertrauenswürdig, auch wenn damit gerechnet werden muss, dass einzelne Personen in Bezug auf die Daten anderer Betroffener übergreifend sein können.
- **Cloud-Anbieter:** Im Rahmen des EduMiDa-Anwendungskontextes beauftragte Auftragsverarbeiter, die zumindest die physische Infrastruktur und die Virtualisierungs-umgebung kontrollieren und per Definition als nicht vertrauenswürdig gelten.
- **Komponenten-Hersteller:** Hersteller der Endgeräte, Infrastrukturkomponenten und weiteren technischen Komponenten, die im EduMiDa-System eingesetzt werden. Die Hersteller gelten als nicht unbedingt vertrauenswürdig. Es finden aber im Rahmen von EduMiDa keine Sicherheitsprüfungen von Komponenten Dritter und keine verbindliche Festlegung auf bestimmte Drittanbieter statt.

Für die Bedrohungs- und Anforderungsanalyse wurde entsprechende Literatur über die Sicherheit von IoT, Cloud, Smart Cities und Webanwendungen herangezogen und auf die im AP 1 beschriebenen Anwendungsfälle angewendet. Auf der Datenerfassungsebene existieren

unmittelbare Bedrohungen aus der physischen Umgebung. Auf der Datenübermittlungsebene können sich Sicherheitsprobleme unter anderem dadurch ergeben, dass das EduMiDa-System über die Kommunikationsnetze die Messdaten verschiedener IoT-Geräte bezieht und die Geräte über unterschiedlich abgesicherte Protokolle kommunizieren und damit IoT-basierte Angriffe und Cyberangriffe ermöglichen. Auf der Datenverarbeitungsebene existieren Cloudbasierte Bedrohungen, während sich auf der Anwendungsebene die Angriffe aller Ebenen auswirken können.

Fraunhofer SIT definierte entsprechende Sicherheitsanforderungen und orientierte sich dabei an den Listen des Open Web Application Security Projects (OWASP) zu Web-basierten und mobilen Sicherheitsrisiken, an Technischen Richtlinien und dem Cloud-Computing-Kriterienkatalog des BSI. Entsprechend wurden Sicherheitsanforderungen für die folgenden Bereiche zusammengestellt: Architektur; Quellcode; Kryptografie; Authentifizierung, Identitäts- und Zugangsmanagement; Netzwerkkommunikation; Datenspeicherung und Datenschutz. Fraunhofer SIT hat dementsprechend die Architektur des EduMiDa-Systems mitgestaltet und die definierten Sicherheitsanforderungen insbesondere in das AP 4 „Architektur“ und AP 6 „Metrikenimplementierung“ eingebracht. Fraunhofer SIT hat schließlich die Einhaltung der Sicherheitsanforderungen in Rahmen des AP 7 „Evaluation“ überprüft.

Rechtlich-Ökonomische Untersuchung

Die DSGVO regelt, dass Datenschutzmaßnahmen unter Berücksichtigung u. a. der Art und Umstände der Verarbeitung, der Eintrittswahrscheinlichkeit und Schwere der Risiken für natürliche Personen und der Implementierungskosten umzusetzen sind. Durch die Berücksichtigung der genannten Faktoren soll sichergestellt werden, dass Datenschutzmaßnahmen – nicht zuletzt aus ökonomischer Sicht – angemessen in Bezug auf den konkreten Verarbeitungskontext umgesetzt werden.

Was die Berücksichtigung dieser ökonomischen und rechtlichen Faktoren für die Umsetzung des Datenschutzes im Allgemeinen und für die Umsetzung von Metriken für den Mitarbeiterdatenschutz im Speziellen bedeuten, wurde von Fraunhofer SIT untersucht. Hierfür wurde im Rahmen der rechtlich-ökonomischen Untersuchung zunächst der Diskussionsstand zu den oben genannten Faktoren zusammengetragen. Hierzu zählen unter anderem

- die Abgrenzung des Standes der Technik zum Stand der Forschung und zu den allgemein anerkannten Regeln der Technik,
- die Berücksichtigung von Implementierungsfolgekosten,
- die Diskussion der in Art (u. a. Datenarten, Verarbeitungsarten, Kategorien betroffener Personen, genutzte Verarbeitungstechnik), Umfang (u. a. Menge der betroffenen Personen und der verarbeiteten Daten), Umstände (u. a. Verarbeitungsort, Verarbeitungszeit, eingesetzte Systeme, wirtschaftliche Interessen des Verantwortlichen) und Zwecke (kritische und/oder weit gefasste Verarbeitungszwecke) der Verarbeitung zu berücksichtigenden Aspekte,
- die Diskussion der physischen, materiellen und immateriellen Schäden für die betroffenen Personen sowie
- die Diskussion unterschiedlicher Schutzstufen personenbezogener Daten.

Im nächsten Schritt wurden konkrete Empfehlungen zur datenschutzrechtlich angemessenen Gestaltung technischer Entwicklungs- und Implementierungsarbeiten abgeleitet, an denen sich die Entwicklung und Implementierung des EduMiDa-Metrikensystems orientieren sollte.

Hintergrund dieser Gestaltungsempfehlung ist der Umstand, dass bei der Planung neuer IT-Systeme, mit denen personenbezogene Daten von Kunden oder Mitarbeitern verarbeitet werden sollen, den Planer des IT-Systems häufig vor große Herausforderungen stellt, die Entwicklung und Inbetriebnahme des neuen IT-Systems unter Beachtung der einschlägigen datenschutzrechtlichen Anforderungen umzusetzen. Häufigster Hemmschuh für eine datenschutzkonforme Entwicklung und Inbetriebnahme eines neuen IT-Systems sind einerseits fehlende Fachkenntnisse zu datenschutzrechtlichen Rahmenbedingungen – insbesondere die datenschutzrechtlichen Anforderungen, die sich aus der Datenschutz-Grundverordnung ergeben und die entsprechend des darin verankerten risikobasierten Ansatzes angemessen umzusetzen sind – sowie andererseits fehlende Erfahrungen zur Gestaltung der Umsetzung dieser Anforderungen, auch hinsichtlich der Einbindung von Funktionsträgern seitens des Planers des IT-Systems. Der im Rahmen von EduMiDa entwickelte Gestaltungsvorschlag zur angemessenen Datenschutzumsetzung im Rahmen technischer Entwicklungs- und Implementierungsarbeiten leistet vor diesem Hintergrund einen Beitrag zur Umsetzung des Datenschutzes „by Design“.

Entsprechend des entwickelten Gestaltungsvorschlags sind für die datenschutzkonforme Gestaltung neu geplanter IT-Systeme im Wesentlichen vier Schritte umzusetzen:

- die Entscheidung darüber, ob das neu geplante IT-System personenbezogene oder anonyme Daten verarbeiten soll;
- die Vorprüfung der Machbarkeit aus rechtlicher und technischer Sicht;
- die Planung der Umsetzung der allgemeinen Grundsätze des Datenschutzrechts, z. B. der Planung des Einholens einer Einwilligung und der Planung der Umsetzung von Löschpflichten;
- die Planung der Umsetzung technischer und organisatorischer Schutzmaßnahmen, wie zum Beispiel die Umsetzung des Vier-Augen-Prinzips und das Verschlüsseln von Daten.¹

Jeder der vier vorgenannten Schritte wurde sodann detailliert ausgeführt, indem sowohl die jeweils einschlägigen datenschutzrechtlichen Anforderungen benannt wurden, diese um ausführbare Aufgaben ergänzt und konkretisiert wurden sowie Empfehlungen zur personellen Zuständigkeit und zeitlichen Planung gegeben wurden.

2.3 Metrikenspezifikation (Arbeitspaket 3)

Datenschutzmetriken stellen einen Kontrollmechanismus dar, um die Einhaltung der Datenschutzerfordernungen (z. B. Datenminimierung oder Speicherbegrenzung) verifizieren zu können. Sie messen den Grad der Umsetzung dieser datenschutzrechtlichen Anforderungen. Auf diese Weise können Datenschutzmetriken helfen, den Missbrauch oder die unrechtmäßige Erhebung personenbezogener Daten aufzudecken. Als Ergebnis liefern die Metriken eine Kennzahl (z. B. Prozentwert), die einen Hinweis auf den Grad der Umsetzung einer Maßnahme bzw. auf einen Datenmissbrauch gibt.

¹ Selzer/Timm, HMD Praxis der Wirtschaftsinformatik 2022 (als online first).

2.3.1 Vorgehensweise

Die Arbeiten zur Metrikenspezifikation begannen mit der Priorisierung der für die im Rahmen von EduMiDa ausgewählten Anwendungsszenarien relevanten, datenschutzrechtlichen Anforderungen.

Aus rechtlicher Sicht wurden die Metriken in zwei Prioritätsgruppen unterteilt, die sich aus einer vom Verordnungsgeber der Datenschutz-Grundverordnung selbst getroffenen Einteilung der Normen in Art. 83 Abs. 4 und 5 DSGVO ergeben. Diese Vorschrift gibt den Bußgeldrahmen wieder, allerdings wird dabei lediglich der Rechtsgedanke zur Einteilung der Normen durch den Verordnungsgeber genutzt und sich nicht an einem möglichen Bußgeld orientiert. Dadurch ergeben sich folgende Prioritätsgruppen: Die Prioritätsstufe 1 beinhaltet Vorgänge die Rechtmäßigkeit des individuellen Datenverarbeitungsvorgangs und Wahrung der Betroffenenrechte betreffend, Art. 5, 6, 7, 9, 12-22, 44-49 DSGVO sowie die Anweisungen der Datenschutzbehörden und die Vorschriften des BDSG und die Prioritätsstufe 2 die Dokumentations- und sonstige Pflichten, Art. 8, 11, 25-39, 42 und 43 DSGVO.

Aus technischer Sicht wurden die datenschutzrechtlichen Anforderungen u.a. vor dem Hintergrund der Machbarkeit einer technischen Verifikation der Anforderung auf Basis bereits vorhandener technischer Messdaten und -verfahren sowie deren Erhebungsaufwand, Validität, Reliabilität und Sicherheit priorisiert. Die Prioritätsstufe 3 erhielten Anforderungen, die keinen technisch bewertbaren Gehalt haben; die Prioritätsstufe 2 erhielten Anforderungen, die technisch umsetzbar sind; die Prioritätsstufe 1 erhielten Anforderungen, die sowohl technisch umsetzbar als auch besonders relevant für die EduMiDa-Anwendungsszenarien sind (u. a. in Bezug auf die Erhebung von Standortdaten und Vitaldaten von Mitarbeitern).

Aus Nutzersicht erhalten alle datenschutzrechtlichen Anforderungen die Priorität 1, da sämtliche Datenschutzerfordernisse aus Nutzersicht eine hohe Priorität haben.

Im Gesamtergebnis ergab die Priorisierung der Anforderungen aus rechtlicher, technischer und Nutzersicht die Prioritätsstufe 1 folgender Anforderungen:

- Rechtmäßigkeit (insbesondere Einwilligung, auch für die Erhebung besonderen Kategorien von Daten)
- Integrität und Vertraulichkeit (insbes. angemessenes Schutzniveau)
- Betroffenenrechte (insbesondere Auskunft, Berichtigung, Löschung, Sperrung, Datenübertragbarkeit)
- Datenminimierung (insbesondere Vergrößern des Standortes, keine Erhebung „unnötiger“ Daten/Erforderlichkeit der Datenverarbeitung)
- Speicherbegrenzung (insbesondere zeitnahes Löschen von Standortdaten).

Im nächsten Schritt erfolgte nun die Spezifikation von Metriken, die aus der o. g. Liste von Anforderungen der Prioritätsstufe 1 abgeleitet werden. Dies erfolgte anhand des Top-Down- („Übersetzen“ von rechtlichen Anforderungen in technisch überprüfbare Maßnahmen) und Bottom-Up-Ansatzes (Identifizierung technischer Datenquellen und Vorbereitung der technischen Überprüfung der im Rahmen des Top-Down-Ansatzes abgeleiteten Maßnahmen).

In Bezug auf die mit der Prioritätsstufe 1 priorisierte Anforderung der Speicherbegrenzung hat sich Fraunhofer SIT auch mit datenschutzrechtlichen Aufbewahrungs- und Löschpflichten von Betriebsräten beschäftigt. In Bezug auf die Ergebnisse des EduMiDa-Metrikensystems werden

Betriebsräte in der Regel nur aggregierte Ergebnisse der Datenschutzverifizierung einsehen können. Führt jedoch das Ergebnis einer Datenschutzverifizierung zu einem Konflikt zwischen der Arbeitgeber- und Arbeitnehmerseite, in die der Betriebsrat einbezogen wird, so ist es denkbar, dass der Betriebsrat personenbezogene Daten einzelner Mitarbeiter einsehen kann, die die Grundlage der Metrikenberechnung darstellen. Zur datenschutzkonformen Betriebsratsarbeit ist es sodann wiederum erforderlich, dass für diese Daten Löschfristen definiert und umgesetzt werden, damit personenbezogene Mitarbeiterdaten, die die Grundlage von Metrikenberechnungen bildeten, nicht länger als erforderlich im Betriebsrat verarbeitet werden. Sobald ein ggf. zwischen Arbeitgeber- und Arbeitnehmerseite bestehender Konflikt aufgrund der Metrikenergebnisse endgültig beigelegt ist, sind die o.g. personenbezogenen Daten regelmäßig beim Betriebsrat zu löschen.

2.3.2 Definition der Datenschutzmetriken

Fraunhofer SIT entwickelte Metrikensteckbriefe (u. a. Zielgruppen, Skala, Maßeinheit, Messhäufigkeit, Schwellwerte, Zielwert, Datenquellen und Indikatoren) unter anderem für die folgenden acht Metriken:

M1.1 – Beschränkung von Standortbestimmungen

Hinsichtlich des Datenschutzgrundsatzes „Datenminimierung“ soll Mithilfe dieser Metrik verifiziert werden, ob Standortbestimmungen (d. h. die Berechnung eines oder mehrerer Standorte in einem Zusammenhang) auf Fälle konkreter Abfragen (d. h. einer Standortsuche nach bestimmten Beschäftigten) beschränkt sind. Die Metrik berechnet für einen bestimmten Zeitraum t die Anzahl der Standortabfragen im Verhältnis zur Anzahl der Standortbestimmungen.

M1.1 – Beschränkung von Standortbestimmungen	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte
Formel	$f_{M1.1}(t) = \frac{\text{Anzahl Standortabfragen}}{\text{Anzahl Standortbestimmungen}}$
Skala	kontinuierliche metrische Skala (Wertebereich: [1; ∞])
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal täglich). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $0,75 \leq f_{M1.1}(t) \leq 1,00$: Die Anzahl der Standortbestimmungen erscheint angemessen. 2. $0,40 \leq f_{M1.1}(t) < 0,75$: Es besteht der Verdacht, dass zu viele Standortbestimmungen durchgeführt wurden. 3. $0,00 < f_{M1.1}(t) < 0,40$: Die Anzahl der Standortbestimmungen ist unangemessen hoch.
Zielwert	$f_{M1.1}(t) = 1,00$ (Anzahl der Standortabfragen = Anzahl der Standortbestimmungen)
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Anzahl der Standortabfragen: Personaleinsatzplanung (z. B. Einträge in Logdateien) 2. Anzahl der Standortbestimmungen: Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle

	(Einträge in Logdateien z. B. im omlox-Hub, siehe Abschnitt 2.4)
--	--

M1.2 – Beschränkung von Standortabfragen

Hinsichtlich des Datenschutzgrundsatzes „Datenminimierung“ soll Mithilfe dieser Metrik verifiziert werden, ob Standortabfragen auf Fälle beschränkt sind, in denen ein konkreter Anlass vorliegt. Die Metrik bestimmt für einen gegebenen Zeitraum t den Anteil der real veranlassten Abfragen für eine standortbasierte Einsatzplanung von der Gesamtzahl der Standortabfragen.

M1.2 – Beschränkung von Standortabfragen	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte
Formel	$f_{M1.2}(t) = \frac{\text{Anzahl Standortabfragen wg. Anlass} \cdot 100}{\text{Gesamtzahl Standortabfragen}}$
Skala	kontinuierliche metrische Skala (Wertebereich: [1; ∞])
Maßeinheit	Prozent
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal täglich). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $75\% \leq f_{M1.2}(t) \leq 100\%$: Die Anzahl der Standortabfragen erscheint angemessen. 2. $40\% \leq f_{M1.2}(t) < 75\%$: Es besteht der Verdacht, dass zu viele nicht veranlasste Standortabfragen durchgeführt wurden. 3. $0\% < f_{M1.2}(t) < 40\%$: Die Anzahl der nicht veranlassten Standortabfragen ist unangemessen hoch.
Zielwert	$f_{M1.2}(t) = 100\%$ (Anzahl der Standortabfragen aufgrund von Anlässen = Gesamtzahl der Standortabfragen)
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Anzahl der Anlässe: Personaleinsatzplanung (z. B. Einträge in Datenbanken oder Logdateien) 2. Anzahl der Standortabfragen: Personaleinsatzplanung (z. B. Logdateien)

M1.3 – Unterlassung unbegründeter Standorterhebungen

Hinsichtlich des Datenschutzgrundsatzes „Datenminimierung“ soll Mithilfe dieser Metrik verifiziert werden, ob die Erhebung von Standorten Beschäftigter, die nicht für einen Einsatz in Frage kommen, unterlassen wurde. Die Metrik berechnet für eine bestimmte Abfrage A die Anzahl der für einen Einsatz in Betracht kommenden Beschäftigten im Verhältnis zur Anzahl der ermittelten Standorte.

M1.3 – Unterlassung unbegründeter Standorterhebungen	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte

Formel	$f_{M1.3}(A) = \frac{\text{Anzahl in Betracht kommender Beschäftigte}}{\text{Anzahl ermittelter Standorte}}$
Skala	kontinuierliche metrische Skala (Wertebereich: [1; ∞])
Messhäufigkeit	Die Messung erfolgt für jeden Anlass, d. h. für jede Standortabfrage der Personaleinsatzplanung.
Schwellwerte	<ol style="list-style-type: none"> 1. $f_{M1.3}(A) \geq 1,00$: Es wurden gleich viele oder weniger Standorte ermittelt als Beschäftigte in Betracht kommen. Das ist im Sinne des Datenschutzes in Ordnung. 2. $1,00 > f_{M1.3}(A) > 0,75$: Es besteht der Verdacht, dass von mehr Personen als von denen, die in Betracht kommen, der Standort ermittelt wurde. 3. $0,75 \geq f_{M1.3}(A) \geq 0,00$: Die Anzahl der ermittelten Standorte von Beschäftigten ist unangemessen hoch.
Zielwert	$f_{M1.3}(A) \geq 1,00$ (Anzahl der in Betracht kommenden Beschäftigten entspricht mindestens der Anzahl der ermittelten Standorte)
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Informationen zum konkreten Anlass (z. B. erforderliche Qualifikationen, Zeitpunkt des Anlasses): Personaleinsatzplanung 2. Anzahl der in Betracht kommenden Beschäftigten mit der erforderlichen Qualifikation: Personaleinsatzplanung 3. Anzahl der ermittelten Standorte: Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle (z. B. omlox-Hub, siehe Abschnitt 2.4)

M2.1 – Löschung der Standortdaten nach Beendigung der Umplanungen

Hinsichtlich des Datenschutzgrundsatzes „Speicherbegrenzung“ soll mithilfe dieser Metrik verifiziert werden, ob zu einer konkreten, bereits angeschlossenen Umplanung noch Standortdaten im System vorhanden sind. Für die Überprüfung wird vorausgesetzt, dass zu jeder Umplanung ein eindeutiges Tag erzeugt wird. Alle Standortdaten werden mit dem Tag der dazugehörigen Umplanung versehen (Standortdaten werden „getagged“). Die Metrik bestimmt für eine **abgeschlossene** Umplanung *rescheduling_i* das Verhältnis aus der Anzahl noch im System vorhandener Standortdaten und der Anzahl aller im Rahmen dieser Umplanung erhobenen Standortdaten.

M2.1 – Durchschnittliche Aufbewahrungszeit von Standortdaten	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte
Formel	$f_{M2.1}(\text{rescheduling}_i) = \frac{\text{Anzahl vorhandener Standortdaten}}{\text{Anzahl aller erhobener Standortdaten}}$
Skala	kontinuierliche metrische Skala (Wertebereich: [1; ∞])
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal täglich). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $f_{M2.1}(re) = 0,00$: Zu dieser bereits abgeschlossenen Umplanung sind keine Standortdaten mehr im System

	<p>vorhanden, d. h. alle Standortdaten wurden gelöscht.</p> <ol style="list-style-type: none"> 2. $0,25 \geq f_{M2.1}(re) > 0,00$: Es existieren im System noch wenige Standortdaten zu dieser Umplanung, obwohl die Umplanung bereits abgeschlossen wurde. 3. $1,00 \geq f_{M2.1}(re) > 0,25$: Es existieren im System noch sehr viele Standortdaten zu dieser Umplanung, obwohl die Umplanung bereits abgeschlossen wurde. Diese Daten müssen umgehend gelöscht werden.
Zielwert	$f_{M2.1}(re) = 0,00$ (Anzahl noch vorhandener Standortdaten = 0)
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Anzahl der noch vorhandener Standortdaten zu einer bereits abgeschlossenen Umplanung: Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle (Einträge in Logdateien z. B. im omlox-Hub, siehe Abschnitt 2.4) 2. Anzahl aller im Rahmen einer bereits abgeschlossenen Umplanung erhobenen Standortdaten: Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle (Einträge in Logdateien z. B. im omlox-Hub, siehe Abschnitt 2.4) 3. Information darüber, ob eine konkrete Umverteilung bereits abgeschlossen wurde: Personaleinsatzplanung

M2.2 – Löschung der Standortdaten nach Erfüllung des Verarbeitungszwecks

Hinsichtlich des Datenschutzgrundsatzes „Speicherbegrenzung“ soll mithilfe dieser Metrik verifiziert werden, ob zu abgeschlossenen Anlässen (Beendigung des Verarbeitungszwecks) die dazugehörigen Standortdaten gelöscht wurden. Die Metrik bestimmt für einen bestimmten Zeitraum t das Verhältnis aus der Anzahl abgeschlossener Anlässe mit gelöschten Standortdaten und der Gesamtzahl der abgeschlossenen Anlässe.

M2.2 – Löschung der Standortdaten nach Erfüllung des Verarbeitungszwecks	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte
Formel	$f_{M2.2}(t) = \frac{\text{Anz. abgeschl. Anl. mit gelöschten Standortdaten}}{\text{Gesamtzahl abgeschlossener Anlässe}} \cdot 100$
Skala	kontinuierliche metrische Skala (Wertebereich: [0; 100])
Maßeinheit	Prozent
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal täglich). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $75\% \leq f_{M2.2}(t) \leq 100\%$: Die Aufbewahrungszeit der Standortdaten erscheint angemessen. 2. $40\% \leq f_{M2.2}(t) < 75\%$: Es besteht der Verdacht, dass Standortdaten häufig zu lange aufbewahrt werden. 3. $0\% < f_{M2.2}(t) < 40\%$: Die Aufbewahrungszeit der Standortdaten ist unangemessen hoch.
Zielwert	$f_{M2.2}(t) = 100\%$ (Anzahl abgeschlossener Anlässe mit gelöschten Standortdaten = Gesamtzahl der abgeschlossenen Anlässe)

Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Anzahl abgeschlossenen Anlässe im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien 2. Anzahl der Veranlassungen von Löschungen von Standortdaten im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien 3. Anzahl der Löschungen von Standortdaten im gegebenen Zeitraum: Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle (Einträge in Logdateien z. B. im omlox-Hub, siehe Abschnitt 2.4)
-------------------------------------	---

M2.3 – Recht auf Löschung

Hinsichtlich des Datenschutzgrundsatzes „Speicherbegrenzung“ soll mithilfe dieser Metrik verifiziert werden, ob auf von Beschäftigten gestellte Löschanfragen entsprechend reagiert wurde und die Daten gelöscht wurden. Die Metrik bestimmt für einen bestimmten Zeitraum t das Verhältnis aus der Anzahl gelöschter Daten und der Anzahl der Löschanfragen.

M2.3 – Recht auf Löschung	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte
Formel	$f_{M2.3}(t) = \frac{\text{Anzahl gelöschter Daten}}{\text{Anzahl der Löschanfragen}}$
Skala	kontinuierliche metrische Skala (Wertebereich: $[0; \infty]$)
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal täglich). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $f_{M2.3}(t) \geq 1,00$: Es wurden mehr Daten gelöscht, als Löschanfragen gestellt wurden. Anscheinend wurde auf alle Löschanfragen entsprechend reagiert. 2. $1,00 > f_{M2.3}(t) > 0,75$: Es besteht der Verdacht, dass auf einige Löschanfragen nicht durch entsprechende Löschung reagiert wurde. 3. $0,75 \geq f_{M2.3}(t) \geq 0,00$: Es existieren zu viele Löschanfragen, auf die nicht durch entsprechende Datenlöschung reagiert wurde.
Zielwert	$f_{M2.3}(t) \geq 1,00$ (Anzahl gelöschter Daten ist mindestens so hoch, wie die Anzahl der Löschanfragen)
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Anzahl der Löschanfragen im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien 2. Anzahl der Veranlassungen von Löschungen von Standortdaten im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien 3. Anzahl der Löschungen von Standortdaten im gegebenen Zeitraum: Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle (z. B. omlox-Hub, siehe Abschnitt 2.4)

M3.1 – Datenschutzkonforme Einwilligung

Hinsichtlich der Rechtmäßigkeit der Verarbeitung soll mithilfe der Metrik verifiziert werden, ob die in einem festgelegten Zeitraum eingeholten Einwilligungen zur Verarbeitung von Standortdaten während der Pausenzeiten auch wirksam sind. Die Metrik bestimmt für einen bestimmten Zeitraum t und für einen bestimmten Beschäftigten B die Anzahl der wirksamen Einwilligungen im Verhältnis zur Gesamtzahl der Einwilligungen.

M3.1 – Datenschutzkonforme Einwilligung	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte
Formel	$f_{M3.1}(t, B) = \frac{\text{Anzahl der wirksamen Einwilligungen}}{\text{Gesamtzahl der Einwilligungen}} \cdot 100$
Skala	kontinuierliche metrische Skala (Wertebereich: [0; 100])
Maßeinheit	Prozent
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal täglich). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $75\% \leq f_{M3.1}(t, B) \leq 100\%$: Der Anteil der wirksamen Einwilligungen erscheint angemessen. 2. $40\% \leq f_{M3.1}(t, B) < 75\%$: Es besteht der Verdacht, dass zu viele unwirksame Einwilligungen eingeholt wurden. 3. $0\% < f_{M3.1}(t, B) < 40\%$: Die Anteil der unwirksamen Einwilligungen ist unangemessen hoch.
Zielwert	$f_{M3.1}(t, B) = 100\%$ (Anzahl der wirksamen Einwilligungen = Gesamtzahl der Einwilligungen)
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Zeitpunkte der Einwilligungen: Personaleinsatzplanung, Logdateien 2. Zeitpunkte der Standortabfragen: Personaleinsatzplanung, Komponente für die Standortbestimmung in einer Werk- oder Lagerhalle (z. B. omlox-Hub, siehe Abschnitt 2.4) 3. Einwilligungstext (Verarbeitungszweck, Messdaten): Personaleinsatzplanung 4. Konfiguration des Einwilligungs- und Widerrufsmechanismus (u. a. Aktivität zur Erteilung der Einwilligung): Personaleinsatzplanung, Smart Device des Beschäftigten

M4.1 – Durchschnittliche Beantwortungszeit in Tagen

Hinsichtlich des Auskunftsrechts der betroffenen Personen soll mithilfe der Metrik verifiziert werden, ob die durchschnittliche Beantwortungszeit von Auskunftersuchen angemessen ist, d. h., die Beantwortung innerhalb eines Zeitraums von einem Monat (30 Tagen) erfolgte. Die Metrik bestimmt für einen bestimmten Zeitraum t die durchschnittliche Beantwortungszeit als Verhältnis aus der Summe aller Beantwortungszeiten und der Anzahl der Auskunftersuche.

M4.1 – Durchschnittliche Beantwortungszeit in Tagen	
Zielgruppen	Datenschutzbeauftragte, Aufsichtsbehörden, Beschäftigte

Formel	$f_{M_{4,1}}(t) = \frac{\text{Summe über alle Beantwortungszeiten in Tagen}}{\text{Anzahl der Auskunftersuche}}$
Skala	kontinuierliche metrische Skala (Wertebereich: [0; ∞])
Maßeinheit	Tage
Messhäufigkeit	kontinuierlich in festgelegten Zeitabständen (z. B. einmal pro Quartal). Der Messzeitraum ist der Zeitraum seit der letzten Messung.
Schwellwerte	<ol style="list-style-type: none"> 1. $f_{M_{4,1}}(t) < 30$ Tage: Die durchschnittliche Beantwortungszeit erscheint angemessen. 2. $30 \text{ Tage} \leq f_{M_{4,1}}(t) \leq 40$ Tage: Es besteht der Verdacht, dass die durchschnittliche Beantwortungszeit häufig etwas zu hoch ist. 3. $f_{M_{4,1}}(t) > 40$ Tage: Die durchschnittliche Beantwortungszeit ist unangemessen hoch.
Zielwert	$f_{M_{4,1}}(t) < 30$ Tage
Datenquellen und Indikatoren	<ol style="list-style-type: none"> 1. Zeitpunkte des Auskunftersuchens im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien 2. Zeitpunkte der Beantwortung von Auskunftersuchen im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien 3. Anzahl der Auskunftersuche im gegebenen Zeitraum: Personaleinsatzplanung, Einträge in Logdateien

Metriken und Indikatoren zu den Themen IT-Sicherheit und Datenschutz

Neben den oben beschriebenen Datenschutzmetriken, die unmittelbar auf die Überprüfung der Einhaltung des Mitarbeiterdatenschutzes abzielen, definierte Fraunhofer SIT weitere Metriken, die der Überprüfung der IT-Sicherheit und des Datenschutzes des EduMiDa-Systems allgemein dienen. Hierbei handelt es sich um Metriken und Indikatoren zu unterschiedlichen Themen, wie zum Beispiel dem Zugangs- und Zutrittsschutz, der Verschlüsselung und der Datenintegrität. Im Folgenden werden exemplarisch einige dieser Metriken und Indikatoren aufgelistet.

Zugangs- und Zutrittsschutz:

- Aktualität des Berechtigungskonzepts
- Stärke der Mechanismen für den Zugriffsschutz
- Administrative Zugriffe (z. B. Zugriffe ohne Logout, Zugriffe zu ungewöhnlichen Zeiten)
- Anzahl unberechtigter Zugriffsversuche

Verschlüsselung:

- Qualität der Verschlüsselungsverfahren
- Qualität der Maßnahmen zum Schutz privater Schlüssel
- Anteil der verschlüsselten an der Gesamtzahl aller Kommunikationsverbindungen

Integrität:

- Anzahl der festgestellten Verletzungen der Integrität
- Anzahl der Vorfälle, bei denen es nicht gelang, Integritätsverletzungen zu korrigieren (Backup)

2.4 Architekturbeschreibung (Arbeitspaket 4)

Die in Abschnitt 2.1 beschriebenen Szenarien erfordern, den Standort von Beschäftigten auf dem Firmengelände und insbesondere innerhalb der Werks- und Lagerhallen zu bestimmen. Ortungssysteme, die nur im Freien funktionieren, wie etwa GPS, kommen daher nicht in Frage. Stattdessen sollte ein Echtzeit-Ortungssystem, das auf Bluetooth Low Energy (BLE) und Bluetooth Mesh basiert, zum Einsatz kommen. Die Architektur sieht dazu vor, dass in jeder Werkshalle ein Bluetooth Mesh installiert und mit einem zentralen Gateway eines sogenannten Real-Time Location Systems (RTLS, Echtzeit-Lokalisierungssystem) verbunden wird. Die Beschäftigten werden mit BLE-fähigen Geräten (einfache BLE-Tags oder auch vorhandene Smartphones) ausgestattet, die jeweils in periodischen Zeitabständen asynchrone Broadcast-Nachrichten senden. Innerhalb des BLE Mesh fungiert dann jeder Relay Node sowohl als Empfänger als auch als Sender und leitet jede Nachricht an jeden seiner Nachbarn weiter, außer zurück an die BLE-Tags. So kann mit relativ wenigen Nodes eine große räumliche Abdeckung erreicht werden. Die BLE-Tags haben jeweils eine eindeutige Kennung (ID) und diese kann genau einem Beschäftigten zugewiesen werden. Dadurch bekommen diese IDs den Charakter eines personenbezogenen Pseudonyms, dessen Auflösung möglichst nur im System der Personaleinsatzplanung (PEP) erfolgen sollte. Entsprechend soll die PEP nur die IDs der für die Umplanung gesuchten Beschäftigten an das RTLS senden.

Fraunhofer SIT spezifizierte zusammen mit dem Anwendungspartner p.l.i. solutions eine entsprechende EduMiDa-Architektur, siehe Abbildung 1. Insbesondere wurden von Fraunhofer SIT die im Rahmen des Demonstrators (AP 6) zu entwickelnden Komponenten (EduMiDa-Proxy, EduMiDa-Service und EduMiDa-App) konzipiert. Für diese Komponenten wurden jeweils die Kommunikationsabläufe mit den anderen Komponenten beschrieben und die dafür benötigten Schnittstellen und Kommunikationsprotokolle spezifiziert. Zudem wurde festgelegt, welche Daten die einzelnen Komponenten in welcher Form speichern müssen und wie lange die Daten vorgehalten werden müssen. Darüber hinaus wurden für die Komponenten definiert, welche Sicherheitsmaßnahmen umgesetzt werden müssen (basierend auf den in AP 2 spezifizierten Anforderungen). Hierzu zählen unter anderem eine gegenseitige Authentifizierung und ein Zugriffsschutz.

Als RTLS-System wird eine Middleware-Implementierung des RTLS-Industriestandards omlox genutzt. Omlox ermöglicht die Vernetzung verschiedener Ortungstechnologien (RFID, SLAM, 5G, BLE, WLAN, GPS, optische Ortung, Ultraschallbasierte Ortung etc.), so dass Logistikkunden ein beliebiges, ggf. bereits vorhandenes RTLS weiter nutzen können. Die omlox-Middleware stellt alle Standortdaten über eine REST-API einheitlich in Form von GPS-Koordinaten bereit und unterstützt die Definition der Ortungsbereiche (Ziel-Arbeitsplätzen, Sicherheitszonen etc.). Das RTLS-Gateway stellt die Ortungsdaten in Echtzeit bereit und überschreibt die jeweils vorigen Messdaten. Fraunhofer SIT diskutierte mit dem Anwendungspartner die optimale Integration der zuvor ausgewählten Middleware für die Standortbestimmung der Beschäftigten (omlox), d. h. insbesondere die Anbindung von omlox

an den EduMiDa-Proxy als Schnittstelle zwischen der omlox-Middleware und den übrigen Komponenten der EduMiDa-Architektur.

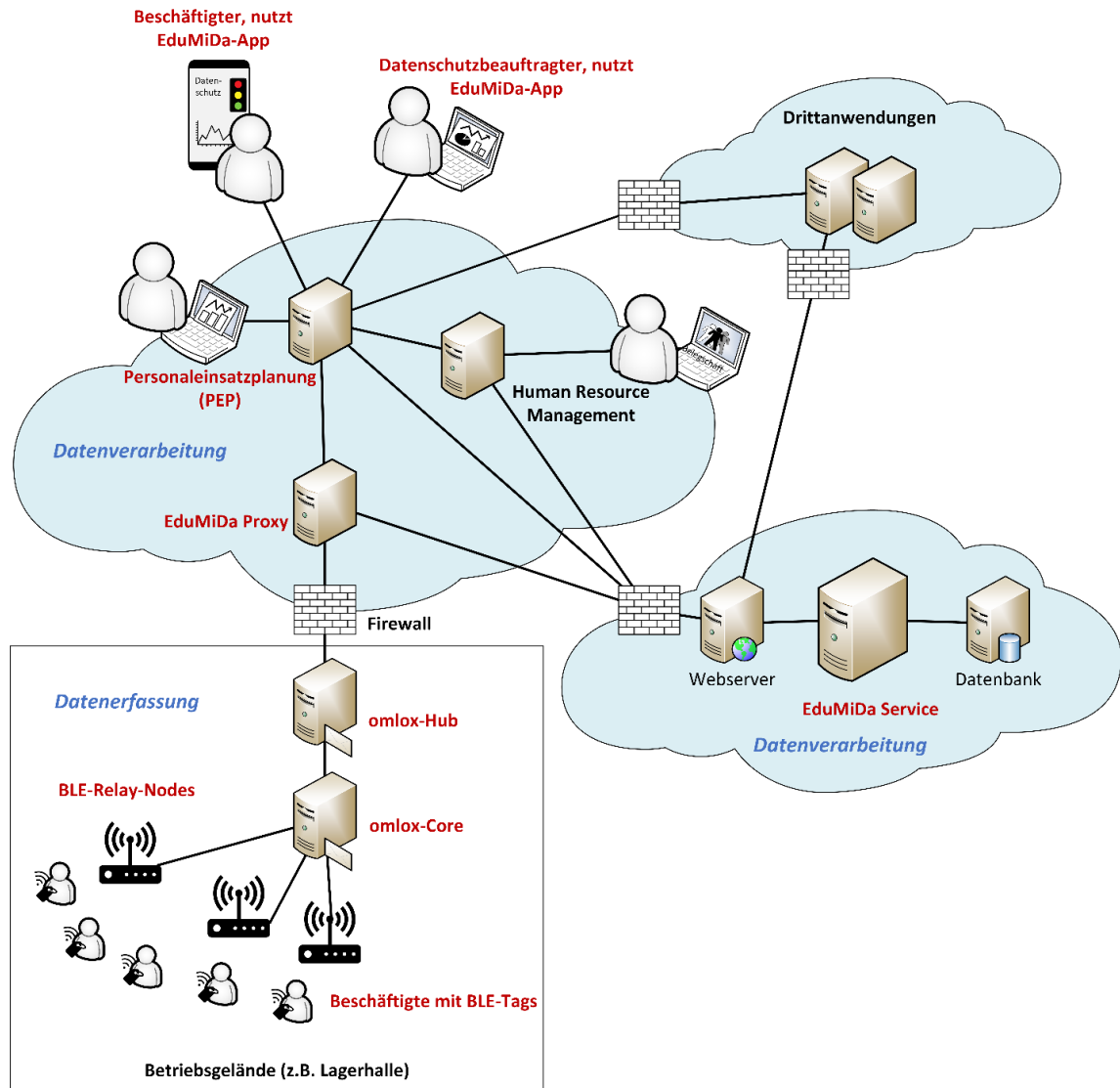


Abbildung 1: Architektur des EduMiDa-Systems

2.4.1 Prozesse im EduMiDa-System

Innerhalb des EduMiDa-Systems sind im Wesentlichen zwei Prozesse hervorzuheben: Die Umplanung des Mitarbeiterereinsatzes und die Überprüfung des Datenschutzes. Der Prozess zur Umplanung des Mitarbeiterereinsatzes ist in Abbildung 2 dargestellt.

Im ersten Schritt meldet die Personaleinsatzplanung (PEP) einen erhöhten Bedarf an Beschäftigten am Ziel-Arbeitsplatz. In Schritt 2 sendet die PEP an den EduMiDa-Proxy die BLE-Tag-IDs der in Frage kommenden Beschäftigten, die Anzahl n der benötigten Beschäftigten sowie den Ziel-Arbeitsplatz. Das RTLS-Gateway (omlox-Hub) ermittelt in Schritt 3 die Standortdaten der Beschäftigten. Der EduMiDa-Proxy wählt daraufhin diejenigen n

Beschäftigten (BLE-Tags) aus, die dem Ziel-Arbeitsplatz am nächsten sind (Schritt 4). Der EduMiDa-Proxy protokolliert den Vorgang (Zeitpunkt, Anlass, Tag-IDs usw.), auf diese Weise stehen die für die spätere Berechnung der Datenschutzmetriken benötigten Daten zur Verfügung. Im letzten Schritt sendet der EduMiDa-Proxy die ausgewählten Beschäftigten (d. h. die IDs der BLE-Tags) an die PEP und die eigentliche Umplanung kann durchgeführt werden.

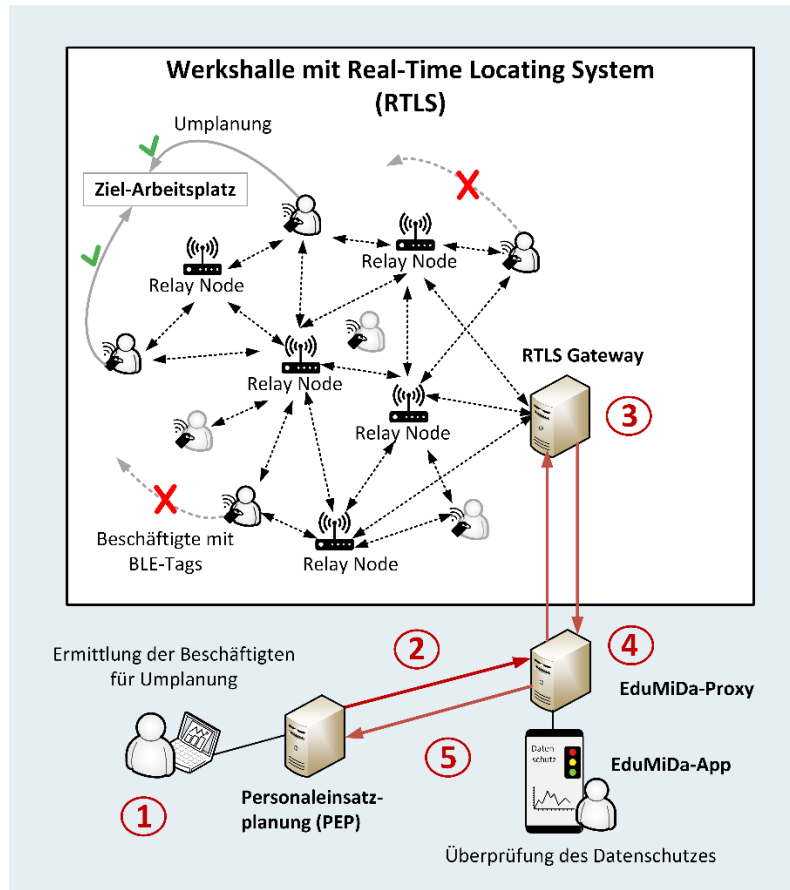


Abbildung 2: Umplanung des Mitarbeiterereinsatzes

Abbildung 3 zeigt den Prozess zur Überprüfung des Datenschutzes. Im ersten Schritt fragt die EduMiDa-App die Kennzahlen (Ergebnis der Datenschutzmetriken) von dem EduMiDa-Proxy ab. Einige der für die Berechnung der Metriken erforderlichen Daten hält der EduMiDa-Proxy selbst vor (vgl. Schritt 4 im zuvor beschriebenen Prozess zur Umplanung des Mitarbeiterereinsatzes). In den meisten Fällen werden für die Berechnung darüber hinaus jedoch noch weitere Daten benötigt (siehe Definitionen der Datenschutzmetriken in Abschnitt 2.3.2). Diese Daten fordert der EduMiDa-Proxy in Schritt 2 von der Personaleinsatzplanung PEP an. Stehen alle benötigten Daten zur Verfügung, berechnet der EduMiDa-Proxy in Schritt 3 die Metriken (Kennzahlen) und sendet diese zurück an die EduMiDa-App. Im letzten Schritt stellt die EduMiDa-App die Kennzahlen in geeigneter Form dar (z. B. Diagramme, Tabellen).

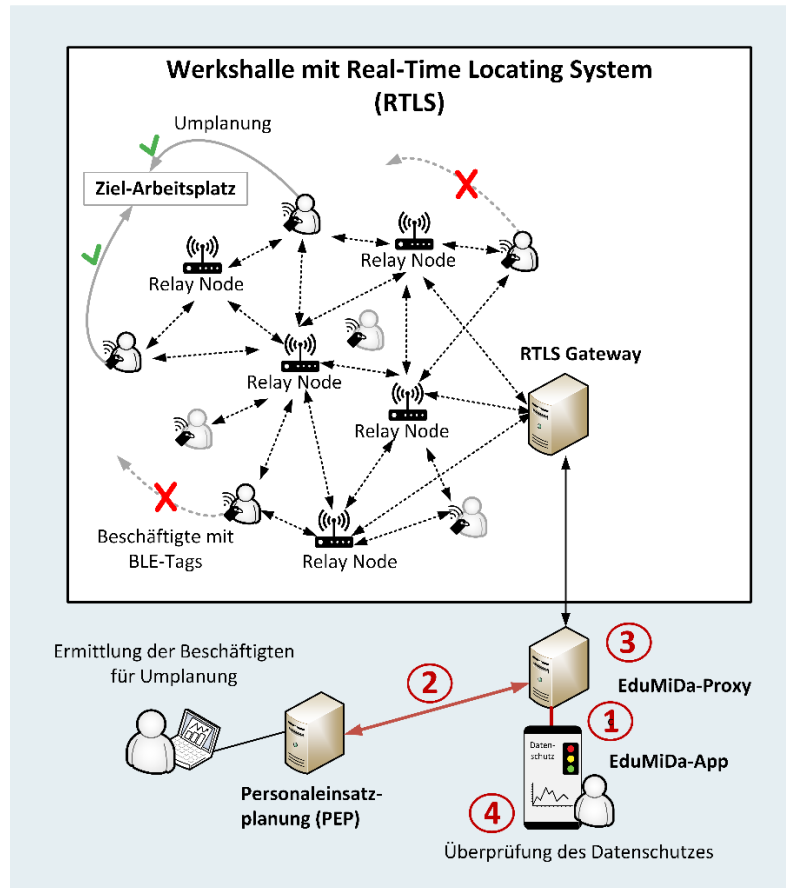


Abbildung 3: Überprüfung des Datenschutzes

2.4.2 Umsetzung des Datenschutzes

Im Fokus der Architekturbeschreibung stand die Umsetzung des Datenschutzes, d. h. insbesondere die Umsetzung der Datenschutzanforderungen Datenminimierung und Speicherbegrenzung. Hinsichtlich der Datenminimierung ist die Verarbeitung der Daten angemessen, weil die Daten nur anlassbezogen vom EduMiDa-Proxy abgerufen und verarbeitet werden. Es werden nur Daten von denjenigen Beschäftigten, die für die Umplanung geeignet bzw. qualifiziert sind, erhoben. Zudem ist die Verarbeitung der Daten erheblich, weil die Personaleinsatzplanung nur die Standorte der Beschäftigten anfragt, die auch gerade verfügbar (anwesend, abkömmlich) sind. Die Verarbeitung der Daten ist darüber hinaus beschränkt, weil nur die für die Umplanung notwendigen Daten (Tag-ID, Standortdaten) erhoben werden. Der Zugriff ist zudem eingeschränkt und rollenbasiert (Need-to-Know-Prinzip).

Um die Anforderung der Speicherbegrenzung zu erfüllen, wurden folgende Maßnahmen ergriffen: Die omlox-Komponenten überschreiben laufend die Messdaten (übermittelte Tag-IDs, Signalstärken) und berechnete Standortdaten, d. h. es werden keine Daten dauerhaft gespeichert. Im EduMiDa-Proxy werden die Standortdaten der Beschäftigten nach erfolgter Umplanung unmittelbar gelöscht. Die Personaleinsatzplanung bekommt als Ergebnis einer Standortabfrage nur die ausgewählten Tag-IDs, aber keine Standortdaten übermittelt. Nur die Personaleinsatzplanung kann die Tag-IDs den Beschäftigten zuordnen.

2.4.3 Sicherheitseigenschaften von BLE-Mesh

Für die Bestimmung der Standortdaten der Beschäftigten wurde zusammen mit dem Projektpartner p.l.i. solutions entschieden, Bluetooth Low Energy (BLE)-Mesh einzusetzen. Ein BLE-Mesh-System besteht aus sogenannten Relay-Nodes, die in bestimmten Abständen in der Lagerhalle montiert sind, und die mit einem zentralen RTLS²-Gateway über LAN oder WLAN verbunden sind. Die Beschäftigten sind mit einfachen BLE-Tags ausgestattet. Diese BLE-Tags senden in periodischen Zeitabständen ungerichtete Nachrichten an umliegende Relay-Nodes. Die BLE-Tags stellen eindeutige Kennungen dar, die genau einem Beschäftigten zugeordnet ist. Der Standort eines BLE-Tags wird anhand der Empfangssignalstärke an mindestens drei Relay-Nodes bestimmt. Das RTLS-Gateway berechnet die Ortungsdaten mittels Trilateration bis auf einen Meter genau. Ein Vorteil dieser Technologie ist, dass die Standortbestimmung auf bestimmte Bereiche innerhalb des Werksgeländes beschränkt werden kann. Außerdem können die Beschäftigten die BLE-Tags ablegen (z. B. während der Pausenzeiten) und werden dadurch nicht permanent geortet.

Fraunhofer SIT hat die Sicherheitseigenschaften von BLE-Mesh auf ihre Eignung für die ausgewählten Szenarien hin untersucht. Die Verwendung eines BLE-Mesh-Systems bietet einige Vorteile gegenüber der alternativen Verwendung von WLAN- oder Ultrabreitband (UWB)-basierten RTLS-Systemen. Für BLE-Mesh sprechen vor allem der einfache, verbindungslose Protokoll-Stack, der geringe Stromverbrauch, die geringen Kosten und die breite Unterstützung von BLE in vielen Geräten. Zudem sind die Sicherheitsmechanismen in BLE-Mesh nicht optional sind, sondern müssen aktiviert sein (Security-by-Design). Die Einrichtung eines BLE Mesh, das Hinzufügen oder Entfernen von Tags und das Verteilen von kryptografischen Schlüsseln erfolgt durch einen speziellen Node, den so genannten *Provisioner* und *Configuration Client*. Für den Schlüsselaustausch kommt das Diffie-Hellman-Verfahren (ECDH) zum Einsatz, es wird zwischen *Device Keys* (zum Konfigurieren), *Network Keys* (zum Obfusieren des Headers) und *Application Keys* (zum Verschlüsseln) unterschieden. Es werden Mechanismen zur Schlüsselerneuerung angeboten und Maßnahmen gegen Man-in-the-Middle-Angriffe eingesetzt. Während der Kommunikation werden Nachrichten grundsätzlich authentisiert und verschlüsselt (*AES-128 mit Counter-with-CBC-MAC (CCM)*). Des Weiteren sind Maßnahmen gegen Replay-Angriffe implementiert (*Sequence Number* im obfusierten Header).

2.5 Testumgebung (Arbeitspaket 5)

Ziel von AP 5 waren die Definition von Testszenarien und der Aufbau einer Testumgebung.

Fraunhofer SIT hat zusammen mit dem Anwendungspartner p.l.i. solutions die geeignete Testumgebung für die im Rahmen des Demonstrators durchgeführte Standortbestimmung von Beschäftigten spezifiziert. Es wurde entschieden, die Testumgebung zu simulieren, damit das Testen unabhängig von realen Logistikhallen und Beschäftigten erfolgen kann. Die Testumgebung bezieht die reale Personaleinsatzplanung mit ein, wobei ausschließlich fiktive

² RTLS: Real Time Location System

Beschäftigtendaten verwendet werden. Für den unter AP 4 genannte EduMiDa-Proxy ist es transparent, dass die Standortdaten von einem Simulator stammen und es sich bei den Beschäftigtendaten um fiktive Daten handelt.

Für den Aufbau der Testumgebung konnte auf Tools, die von der Middleware omlox bereitgestellt werden, zurückgegriffen werden. Diese Tools ermöglichen es, basierend auf einem Kartenmaterial wie Google-Maps fiktive Betriebsgelände mit Werks- oder Lagerhallen sowie technischen Anlagen mit den notwendigen Eigenschaften (GPS-Koordinaten, Länge, Breite, Höhe usw.) zu definieren. Für den Aufbau einer Testumgebung können mithilfe dieser Tools zudem fiktive Beschäftigte generiert werden. Diese können ebenfalls mit bestimmten Eigenschaften versehen werden (z. B. Rollen oder Qualifikationen) und können sich zufallsgesteuert innerhalb des zuvor definierten Betriebsgeländes bewegen.

2.6 Metrikenimplementierung (Arbeitspaket 6)

AP 6 umfasst den „Proof-of-Concept“ der zuvor definierten EduMiDa-Lösung in Form eines Demonstrators.

2.6.1 Darstellung der Datenschutzmetriken

Fraunhofer SIT unterstützte den Anwendungspartner bei der Implementierung des Demonstrators. Insbesondere unterstützte Fraunhofer SIT den Anwendungspartner bei der Darstellung der Datenschutzmetriken in einem Self-Service-Portal in Form von Diagrammen. Diese Diagramme sollen es den Anwendern (z. B. Beschäftigte oder der Betriebsrat) ermöglichen, auf einen Blick und möglichst leicht verständlich zu erkennen, ob es Hinweise auf Datenmissbrauch oder Probleme bei der Umsetzung von Datenschutzmaßnahmen in einem Unternehmen gibt. Fraunhofer SIT diskutierte zu diesem Zweck zunächst grundlegende Aspekte der visuellen Darstellung von Kennzahlen. Dies umfasste unter anderem die Auswahl geeigneter Farben, die Granularität der Darstellung von Informationen, die Abbildung von Daten auf Skalen (z. B. metrische Skalen vs. logarithmische Skalen) sowie die Auswahl geeigneter Icons. Im Anschluss entwarf Fraunhofer SIT für alle in Arbeitspaket 3 spezifizierten Metriken für den Mitarbeiterdatenschutz geeignete Diagramme zur Darstellung der Kennzahlen. Im Wesentlichen wurden für Metriken, die über einen zeitlichen Verlauf kontinuierlich berechnet werden, Balkendiagramme vorgeschlagen (vgl. Abbildung 4). Für Metriken, die Anteile von etwas berechnen, erschienen Kreisdiagramme die geeignete Wahl (vgl. Abbildung 5). Die Diagramme wurden in Form von Mock-Ups erzeugt. Sie dienten dem Anwendungspartner als Vorlage und konnten von ihm leicht in die Web-Oberfläche des Demonstrators integriert werden.

Um die Kontrolle des Datenschutzes zu ermöglichen und die Transparenz zu fördern, wurde ein Dashboard entwickelt, auf dem die verschiedenen Diagramme der Datenschutzmetriken angezeigt werden. Auf diese Weise kann zum Beispiel ein Datenschutzbeauftragter auf einen Blick erkennen, ob es Hinweise auf Datenmissbrauch oder Probleme bei der Umsetzung von Datenschutzmaßnahmen gibt. Dieses Dashboard wurde zudem um eine spezielle Anzeige für die einzelnen Beschäftigten erweitert. Dies ermöglicht es den betroffenen Beschäftigten, die über sie erhobenen Daten einzusehen. In einer tabellarischen Übersicht sehen die Beschäftigten, zu welchen Zeitpunkten ihr aktueller Standort erhoben wurde und zu welchem Zweck. Unterstützt wird diese Darstellung um Diagramme, mit deren Hilfe die Beschäftigten sehr schnell erkennen können, wie oft in welchen Zeiträumen ihr Standort erhoben wurde. Auf

diese Weise werden die Beschäftigten in die Lage versetzt, die Verarbeitung ihrer Standortdaten nachvollziehen zu können. Das Dashboard fördert somit die Transparenz im Sinne des Art. 5 Abs. 1 Var. 2 DSGVO bzgl. der Verarbeitung der Standortdaten von Beschäftigten.

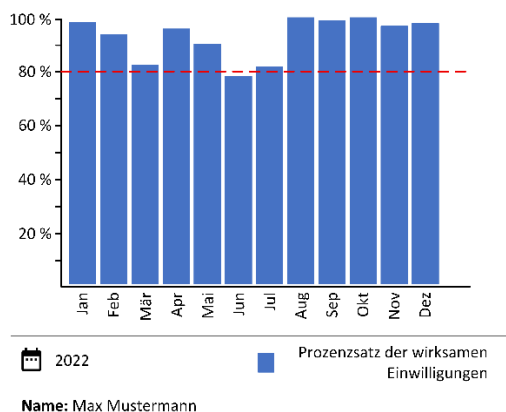


Abbildung 4: Balkendiagramm

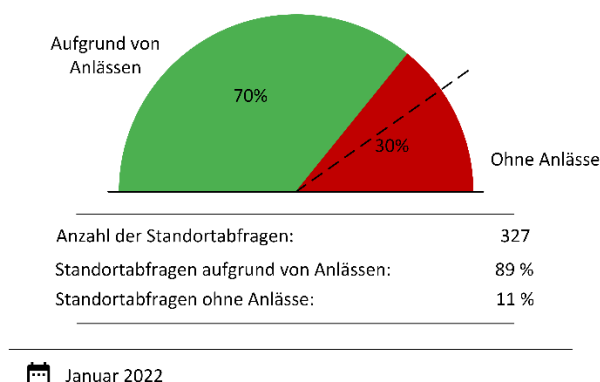


Abbildung 5: Kreisdiagramm

2.6.2 Definition von Use-Cases für den Demonstrator

Des Weiteren definierte Fraunhofer SIT im Rahmen dieses Arbeitspakets zahlreiche Use Cases für den Demonstrator. Diese Use Cases beschreiben die unterschiedlichen Aspekte, die mithilfe des Demonstrators gezeigt werden sollen. Hierzu zählen beispielsweise die Aufdeckung von Standortabfragen von Beschäftigten ohne Anlass mithilfe von Metriken, die Aufdeckung von Standortabfragen von Beschäftigten, die für eine Umplanung nicht in Frage kommen oder die Aufdeckung der Unterlassung der Löschung von Standortdaten nach abgeschlossener Umplanung. Die Use Cases bestehen im Wesentlichen aus den beteiligten Akteuren (z. B. Personaleinsatzplaner, betroffene Beschäftigte), den Vorbedingungen für den Use Case (d. h. wie muss der Demonstrator zuvor konfiguriert werden bzw. welche Daten sind erforderlich, damit der Use Case demonstriert werden kann), einem schrittweisen Ablauf, der beschreibt, wie der Use Case gezeigt wird sowie den Nachbedingungen (d. h. was ist das Ergebnis des Use Cases).

2.7 Evaluation (Arbeitspaket 7)

2.7.1 Evaluation des Gestaltungsvorschlags

Nach der initialen Erstellung des Gestaltungsvorschlags zur angemessenen Umsetzung datenschutzrechtlicher Anforderungen im Implementierungsprozess (vgl. Abschnitt 2.2) wurden sieben Erst- und Folgeworkshops mit jeweils zwei Personen durchgeführt, um den Gestaltungsvorschlag zu evaluieren. Im Rahmen der Erstworkshops, an denen zwei betriebliche Datenschutzbeauftragte / Datenschutzkoordinatoren, IT-Sicherheitsbeauftragte, Mitarbeiter von Rechtsabteilungen, Verfahrenseigner, betroffene Personen, Verantwortliche und Mitarbeiter von Datenschutzaufsichtsbehörden teilnahmen, wurde der Vorschlag initial vorgestellt und anhand eines vorbereiteten und validierten Gesprächsleitfadens diskutiert. Basierend auf diesen Diskussionen wurde der Vorschlag überarbeitet und sodann im Rahmen

von Folgeworkshops mit dem gleichen Teilnehmerkreis vorgestellt und die finale Rückmeldung der Teilnehmer (ebenfalls auf Basis eines validierten Gesprächsleitfadens) eingeholt. Die Rückmeldungen waren – insbesondere im Rahmen der Folgeworkshops – ausschließlich positiv.

Der Gestaltungsvorschlag wurde auch den EduMiDa-Projektpartnern vorgestellt und mit ihnen diskutiert.

2.7.2 Evaluation des Demonstrators

Im Rahmen des Arbeitspakets 2 wurden konkrete Empfehlungen zur datenschutzrechtlich angemessenen Gestaltung technischer Entwicklungs- und Implementierungsarbeiten sowie zur Umsetzung von IT-Sicherheitsanforderungen abgeleitet (vgl. Abschnitt 2.2), an denen sich die Entwicklung und Implementierung des EduMiDa-Metrikensystems orientieren sollte.

Im Rahmen des Arbeitspakets 7 standen die juristischen und technischen Mitarbeiter des Fraunhofer SIT den Entwicklern des EduMiDa-Demonstrators zu Rückfragen zu dem Gestaltungsvorschlag und zu den IT-Sicherheitsanforderungen zur Verfügung.

Gegen Ende der Projektlaufzeit erfolgten sodann zwei Evaluationsworkshops, im Rahmen derer die im Rahmen des Arbeitspakets 2 aufgestellten Anforderungen überprüft wurden. Der erste Evaluationsworkshop erfolgte nach Fertigstellung der Version 1 des Demonstrators, der zweite Evaluationsworkshop erfolgte kurz vor Ende der Fertigstellung der Version 2 des Demonstrators. Im Rahmen der Evaluation wurden Anregungen zur Verbesserung gegeben.

2.7.3 Angemessenheit von Metrikensystemen für den Mitarbeiterdatenschutz

Darüber hinaus wurde im Rahmen des Arbeitspakets 7 die Angemessenheit technischer und organisatorischer Maßnahmen im Allgemeinen und von Metriken für den Mitarbeiterdatenschutz im Speziellen diskutiert.^{3 4}

Art. 32 Abs. 1 1. Hs. DSGVO legt den Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und den Zweck der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen als die maßgeblichen Kriterien für die Auswahl angemessener technischer und organisatorischer Maßnahmen fest. In Frage steht daher, inwiefern Datenschutzmetriken diesen Anforderungen genügen, um als angemessene Umsetzung der Verpflichtung zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gelten zu können.

Datenschutzmetriken können auf laufender Basis technische und organisatorische Maßnahmen überprüfen. Dafür ist allerdings erforderlich, dass auch kontinuierlich Daten über die Verarbeitungsprozesse des Verantwortlichen erhoben werden. Dabei können auch personenbezogene Daten anfallen (z. B. Informationen zu Personen, die sich in einem System eingeloggt haben, Informationen über Administratorentätigkeiten). Auch wenn solche personenbezogenen Daten durch zusätzliche Maßnahmen (z. B. Pseudonymisierung, Verschlüsselung) geschützt werden können, ist dennoch fraglich ob folglich das Gebot der

³ Selzer, Gärtner: Angemessene technische und organisatorische Maßnahmen gem. Art. 32 DSGVO: Organisationen im (ökonomischen) Balanceakt zwischen Risiken und Kosten. DuD 2023, S. 289 – 294.

⁴ Gärtner, Selzer: Metrikensysteme als Beitrag zur Umsetzung des risikobasierten Ansatzes – Angemessene Umsetzung des technisch- organisatorischen Datenschutzes durch Metrikensysteme. DuD 2023, S. 367 – 371.

datenschutzfreundlichen Technikgestaltung in Art. 25 Abs. 1 DSGVO gewahrt werden kann. Das Gebot der datenschutzfreundlichen Technikgestaltung bezweckt eine Berücksichtigung des Schutzes personenbezogener Daten bereits bei der Planung und Entwicklung von Datenverarbeitungsprozessen, um dadurch die Datenschutzgrundsätze wirksam umzusetzen sowie den Anforderungen der DSGVO zu genügen und damit einen verbesserten Schutz informationeller Selbstbestimmung gewährleisten zu können. Hinsichtlich des Grundsatzes der Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO, könnte hinterfragt werden, ob die aufgrund der Datenschutzmetriken kontinuierlich erhobenen Daten auf das für den Zweck der Überprüfung der technischen und organisatorischen Maßnahmen notwendige Maß beschränkt sind, gerade wenn z. B. händische Datenschutzaudits weniger Daten verarbeiten.

Dabei muss aber berücksichtigt werden, dass es für die Überprüfung der Wirksamkeit und der Umsetzung technischer und organisatorischer Maßnahmen gerade gewinnbringend sein kann, den Umsetzungsgrad kontinuierlich zu überprüfen. Dies birgt den großen Vorteil, dass Fehler und Lücken in der Umsetzung schnell erkannt und unmittelbar behoben werden können. Folglich können Datenpannen in ihrem Ausmaß stark begrenzt, wenn nicht sogar ganz verhindert werden. Der Einsatz von Datenschutzmetriken verspricht also nichts Geringeres als einen effektiveren Schutz personenbezogener Daten und damit des Rechts auf informationeller Selbstbestimmung der betroffenen Personen. Dies entspricht auch gerade dem Sinn und Zweck der Verpflichtung zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen, Art. 32 Abs. 1 2. Hs. lit. d DSGVO, nämlich den aus veralteten Techniken hervorgehenden Gefahren rechtzeitig erkennen und begegnen zu können. Angesichts dessen ist die zusätzliche Verarbeitung personenbezogener Daten im Rahmen von Datenschutzmetriken ihrem Zweck angemessen und erheblich, sofern sie auf das notwendige Maß beschränkt ist und technische und organisatorische Schutzmaßnahmen getroffen werden, im Sinne von Art. 5 Abs. 1 lit. c DSGVO, sodass ein Verstoß gegen das Gebot der datenschutzfreundlichen Technikgestaltung in Art. 25 Abs. 1 DSGVO nicht angenommen werden kann.

Des Weiteren bergen Metrikensysteme – sobald sie initial implementiert wurden – einen finanziellen Vorteil für die einsetzende Organisation, da automatisierte Überprüfungen im Vergleich zu händischen Überprüfungen zu einem vergleichsweise kostengünstigen Preis durchgeführt werden können, ohne dass die Mitarbeiter der Organisation eigenes Know-How zur Bewertung technischer und organisatorischer Maßnahmen aufbringen müssen. Zusätzlich führt die automatisiert vorgenommene Dokumentation der Überprüfungen und deren Ergebnisse zu einer weiteren Entlastung der Organisation.

Im Ergebnis können Datenschutzmetriken, vorbehaltlich ihrer Weiterentwicklung zum Stand der Technik, als ein angemessenes Instrument zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen im Sinne von Art. 32 Abs. 1 2. Hs. lit. d DSGVO verstanden werden. Es gilt die Fortschritte der Forschung abzuwarten, um ihr vollständiges Potential für Verantwortliche, Auftragsverarbeitende sowie betroffene Personen einschätzen zu können, wenn auch schon jetzt Datenschutzmetriken große Vorteile für den Schutz personenbezogener Daten vermuten lassen.

Darüber hinaus kann die Angemessenheit der Datenschutzumsetzung durch die Anwendung von Metrikensystemen auch insbesondere im Kontext des Mitarbeiterdatenschutzes eine Stärkung erfahren, wenn Mitarbeiter die Möglichkeit erhalten, über ein Metrikensystem Kenntnis

über den Umsetzungsgrad des von ihrem Arbeitgeber umgesetzten Mitarbeiterdatenschutzes zu erhalten. Dies könnte sich insbesondere in Arbeitsumfeldern potenziell positiv auf die Mitarbeiterzufriedenheit auswirken, in denen die Mitarbeiter immer mehr zum gläsernen Menschen werden, wie z. B. in der Zustell- und Logistikbranche, in denen häufig den gesamten Arbeitstag hinweg die Standortdaten der Zusteller/Fahrer verarbeitet werden, um den Geschäfts- und Privatkunden anzuzeigen, wann ein Fahrer bei ihnen sein wird, um die bestellte Ware zuzustellen.

Die ständige Erhebung von Standortdaten der eigenen Mitarbeiter kann dem Arbeitgeber tiefgreifende und hochsensible Informationen über seine Mitarbeiter aufzeigen, u. a. kann die Information des Standortes vor und nach Pausenzeiten sowie Arbeitsbeginn und -ende Rückschlüsse zum Wohnort des Lebenspartners, zur Bildungseinrichtung der Kinder, zur Behandlung chronischer Erkrankungen, zur Ernährungsweise oder zum politischen oder religiösen Engagement in Vereinen ermöglichen. Während der Arbeitszeit kann die Erhebung von Standortdaten sowie ggf. weiterer personenbeziehbarer Daten der Mitarbeiter zur Leistungskontrolle genutzt werden. All diese Daten machen den Mitarbeiter anfällig für durch den Arbeitgeber umgesetzte Diskriminierungen (z. B. keine Vertragsverlängerung aufgrund des Verdachts auf eine chronische Erkrankung).

Über ein Metrikensystem, das den datenschutzkonformen Umgang mit derartigen Daten anzeigt – z. B. die Messung einer ordnungsgemäß durchgeführten Vergrößerung der Standortdatenerhebung, die in der Folge keine Rückschlüsse auf ein aufgesuchtes Krankenhaus, Restaurant, Vereinshaus o. ä. ermöglicht – kann Mitarbeitern die Sicherheit gegeben werden, nicht zum gläsernen Mitarbeiter zu werden und keine Diskriminierung o. ä. durch ihren Arbeitgeber befürchten zu müssen, die sich auf eine exzessive Datenverarbeitung stützt. Die Möglichkeit, als Mitarbeiter Einblick in die Metrikenauswertung zu nehmen kann auch gerade deshalb umgesetzt werden, weil das Metrikensystem eben nicht personenbezogene Daten anzeigt, sondern bloße Kennzahlen zur Auswertung des Datenschutzniveaus nutzt und daher von der gesamten Belegschaft eingesehen werden kann.

2.7.4 Evaluation des Demonstrators aus Sicht der IT-Sicherheit

Fraunhofer SIT führte zudem eine Evaluation des Demonstrators aus Sicht der IT-Sicherheit durch, um sicherzugehen, dass die in AP 2 aufgestellten Anforderungen an die EduMiDa-Lösung bzgl. der IT-Sicherheit berücksichtigt wurden. Die Evaluation umfasste im Wesentlichen die Komponenten „EduMiDa-Proxy“, „EduMiDa-Service“, „EduMiDa-App“ und das System zur Standortbestimmung (vgl. Abbildung 1 in Abschnitt 2.4). Basierend auf den in AP 2 aufgestellten Sicherheitsanforderungen wurden im Rahmen der Architekturbeschreibung (AP 4) umzusetzende Sicherheitsmaßnahmen für diese Komponenten definiert. Ziel der Evaluation war es festzustellen, inwieweit und auf welche Weise diese Sicherheitsmaßnahmen umgesetzt wurden. Zu diesem Zweck entwickelte Fraunhofer SIT einen Fragebogen bestehend aus 36 Fragen zu unterschiedlichen Themengebieten der IT-Sicherheit. Hierzu zählen unter anderem Authentifizierungsverfahren, sichere Kommunikation zwischen den Komponenten, Zugriffsschutz, Protokollierung, Abwehr von Angriffen wie Man-in-the-Middle-Angriffe oder Denial-of-Service-Angriffe sowie die Umsetzung der Standortbestimmung von Beschäftigten.

Dieser Fragebogen wurde von Mitarbeitern des Projektpartners p.l.i. solutions ausgefüllt und zurück an das Fraunhofer SIT gesendet. Fraunhofer SIT bewertete die Angaben zur Umsetzung der Sicherheitsmaßnahmen und gelangte zu dem Ergebnis, dass diese in ausreichendem Maße

im Rahmen des EduMiDa-Demonstrators implementiert wurden. Der Fragebogen ist darüber hinaus als Hilfestellung für den Projektpartner p.l.i. solutions im Rahmen einer späteren Produktentwicklung.

3 Wichtigste Positionen des zahlenmäßigen Nachweises

Im Rahmen der Durchführung des Teilprojektes sind Kosten in Form von Personalkosten und Reisekosten (insbesondere zu Konferenzen und Workshops) entstanden über die im Detail in den Verwendungsnachweisen berichtet wurde.

4 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Der Verlauf der Arbeit im Projekt folgte der im Projektantrag formulierten Planung. Alle im Arbeitsplan formulierten Aufgaben wurden erfolgreich bearbeitet, es waren keine zusätzlichen Ressourcen für das Projekt nötig. Wo es angebracht schien, wurde die Reihenfolge einiger Arbeitspakete im Projektverlauf geändert oder mehrere Arbeitspakete zu einem Arbeitskomplex verbunden, um eine bessere Kontinuität der Arbeiten zu erreichen.

Die Teilprojekte der drei Forschungspartner wurden jeweils um vier Monate kostenneutral verlängert, um ein mit dem Technologiepartner des Projektes einheitliches Projektende umzusetzen.

Insgesamt erarbeitete das Teilprojekt sowohl eine Reihe schriftlicher Deliverables als auch eine Implementierung des EduMiDa-Demonstrators und erreichte die in Abschnitt 0 dargestellten Publikationen und Vorträge in einschlägigen Fachzeitschriften und auf Fachkonferenzen. Dies alles, sowie die bereits erfolgte Verwertung von Projektergebnissen, die in dem Dokument „Kurzfassung zum Verwertungsplan“ näher dargestellt wird, bestätigen sowohl die wissenschaftliche als auch wirtschaftliche Relevanz der Ergebnisse des Fraunhofer-SIT-Teilvorhabens von EduMiDa.

5 Verwertungsplan

Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

Die Ergebnisse des Teilvorhabens bieten folgende Vorteile:

- Die entwickelten Datenschutzmetriken lassen sich auf andere Szenarien mit personenbezogenen Standortdaten und anderen Sensordaten (z.B. Daten von Wearables) übertragen. Es muss jedoch im Einzelfall geprüft werden, welche Messdaten und Indikatoren zur Verfügung stehen, ggf. müssen die Formeln zur Berechnung der Metriken angepasst werden.
- Unterstützung bei der Abwägung angemessener technischer und organisatorischer Schutzmaßnahmen durch Quantifizierung der durchschnittlichen Implementierungskosten, Schadensersatzhöhen und Bußgeldhöhen gem. DSGVO.

- Schaffung eines Werkzeugs zur angemessenen Umsetzung des Datenschutzes während technischer Entwicklungs- und Implementierungsprozesse, wie z.B. der Entwicklung und Implementierung eines Metrikensystems für den Mitarbeiterdatenschutz.

Fraunhofer SIT plant, die im Rahmen von EduMiDa entwickelten Ergebnisse in die folgenden Projekte und Forschungsaktivitäten einfließen zu lassen, um auf diese Weise die EduMiDa-Lösungen zu verbreiten:

Industrie- und Forschungsprojekte. Durch das Projekt EduMiDa erweiterte Fraunhofer SIT seine Expertise im Bereich von Datenschutz- und Datensicherheitsaspekten des Mitarbeiterdatenschutzes und der Datenschutzmetriken. EduMiDa ermöglicht es Fraunhofer SIT, in Zukunft im Rahmen von Industrie- und Forschungsprojekten auf diese Expertise zurückzugreifen. Zudem ermöglicht das Projekt EduMiDa es dem Fraunhofer SIT, Unternehmen hinsichtlich des Mitarbeiterdatenschutzes und hinsichtlich Datenschutzmetriken umfangreicher als vor der Durchführung von EduMiDa zu beraten.

Know-How- und Wissenstransfer. Fraunhofer SIT hat im Rahmen des Projekts die Projektwebseite www.EduMiDa.sit.fraunhofer.de zur freien Verfügbarkeit wichtiger Forschungsergebnisse des Projektes gehostet und gepflegt. Darüber hinaus hielten Mitarbeiter des Fraunhofer SIT wissenschaftliche Vorträge und veröffentlichten Fachbeiträge in Fachzeitschriften und Tagungsbänden. Des Weiteren führte Fraunhofer SIT zwei Lehrveranstaltungen durch, in die Ergebnisse des EduMiDa-Projektes einfließen, um die Projektergebnisse zu verwerthen.

6 Fortschritts auf dem Gebiet des Vorhabens

Insbesondere durch die COVID-19-Pandemie und den damit verbundenen Trend zum Home-Office und der Nutzung von Kollaborationssoftware hat der Mitarbeiterdatenschutz verstärkt Aufmerksamkeit erfahren. Auf dem Gebiet der automatischen Überprüfbarkeit des Mitarbeiterdatenschutzes mithilfe von Metriken sind uns allerdings keine anderen Projekte bekannt. Fortschritte sind verstärkt in der Entwicklung von Metriken zur Überprüfung der Cybersicherheit zu beobachten. So werden die EU-Staaten mit der EU-Richtlinie 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) insbesondere in Artikel 21 verpflichtet, ein konkretes, rechtsverbindliches Mindestniveau an technischen Maßnahmen für die Cybersicherheit einzuhalten. Dazu sind auch Verfahren notwendig, die Wirksamkeit von Cybersicherheitsmaßnahmen kontinuierlich zu bewerten, d. h. idealerweise mittels eines Systems von Metriken, Sensoren und Schwellenwerten automatisch zu überprüfen. Viele Metriken für die Cybersicherheit werden z. B. vom Centre for Internet Security (CIS) definiert. Es fehlen allerdings Hinweise für die automatische Überprüfung, geeignete Schwellenwerte und der direkte Bezug zu rechtlichen Anforderungen. Das in EduMiDa entwickelte Metrikensystem kann hierbei als Vorlage für die automatische Überprüfbarkeit von Sicherheit und Datenschutz dienen.

7 Erfolgte oder geplante Veröffentlichungen

Im Folgenden werden zunächst die Vorträge, die im Rahmen von EduMiDa gehalten wurden, beschrieben. Der zweite Unterabschnitt beschreibt die erfolgten Veröffentlichungen. Sodann erfolgt ein Überblick über die erfolgten Lehrveranstaltungen sowie über die Verbreitung von Projektergebnissen über die Projekt-Webseite.

Vorträge:

- Annika Selzer: An economic analysis of appropriateness under Art. 32 GDPR, CNIL Privacy Research Day, 28.6.2022 (Paris).
- Ulrich Waldmann: Messung der Datenminimierung für den Beschäftigtendatenschutz am Beispiel von Standortdaten – Verifikation der datenschutzrechtlichen Anforderungen an die Datenminimierung mithilfe von Metriken, GI Jahrestagung 2022, 26.9.2022 (Hamburg).
- Tanya Gärtner: Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen, IT-Tage, 13.12.2022 (virtuell).
- Annika Selzer: Eine ökonomische Analyse der Angemessenheit technischer und organisatorischer Maßnahmen gem. Art. 32 DSGVO, Jahreskonferenz Forum Privatheit, 13.10.2022, Berlin (virtuelle Teilnahme).

Veröffentlichungen:

- Annika Selzer / Daniel Woods / Rainer Böhme: An Economic Analysis of Appropriateness under Article 32 GDPR, EdpL 2021.
- Sarah Diel / Matthias Kohn / Janine Schleper / Annika Selzer: Datenschutzmetriken im Beschäftigungsverhältnis – Verifikation der datenschutzkonformen Einwilligung, DuD 2021.
- Janine Schleper / Matthias Kohn / Paulina Jo Pesch / Ulrich Waldmann / Thomas Kunz: Messung der Datenminimierung für den Beschäftigtendatenschutz am Beispiel von Standortdaten – Verifikation der datenschutzrechtlichen Anforderungen an die Datenminimierung mithilfe von Metriken, LNI – GI-Jahrestagung 2022, S. 231-236.
- Annika Selzer / Ingo J. Timm: Ein Vorschlag für die datenschutzkonforme Gestaltung von Datenschutz-Grundsätzen und -Schutzmaßnahmen in IT-Systemen – Angemessene technische und organisatorische Schutzmaßnahmen nach Art. 32 DSGVO, HMD Praxis der Wirtschaftsinformatik 2022.
- Annika Selzer / Tanya Gärtner: Angemessene technische und organisatorische Maßnahmen: Organisationen im (ökonomischen) Balanceakt zwischen Risiken und Kosten, DuD 2023, S. 289-294.
- Tanya Gärtner / Annika Selzer: Metrikensysteme als Beitrag zur Umsetzung des risikobasierten Ansatzes – Angemessene Umsetzung des technisch-organisatorischen Datenschutzes durch Metrikensysteme, DuD 2023, S. 367 – 371.
- Ulrich Waldmann / Thomas Kunz / Janine Schleper / Matthias Kohn / Paulina Jo Pesch: Legal Requirements and Technical Metrics for Controlling Privacy of Employees' Location Data. Mensch und Computer 2023 – 9. Usable Security and Privacy Workshop, 2023.

- Volker Johannhörster / Matthias Kohn / Thomas Kunz / Janine Schleper / Ulrich Waldmann: Live-Ortung von Beschäftigten in der agilen Personaleinsatzplanung - Umsetzung des Datenschutzes in der Intralogistik, DuD 2024, S. 450 – 455.

Lehrveranstaltungen:

- Annika Selzer: Technisch-organisatorischer Datenschutz, Lehrveranstaltung an der Universität Bremen, 10. und 11.5.2022 (virtuell).
- Annika Selzer: Das Datenschutzrecht erschließen, Lehrveranstaltung an der Universität Bremen, 1. und 2.6.2023 (virtuell).

Sonstiges:

- Sarah Stummer, "enteplexit Preis Informationsrecht" für die in EduMiDa betreute Masterarbeit "Datenschutzmetriken im Beschäftigungsverhältnis – Verifikation des Umsetzungsgrades von datenschutzrechtlichen Pflichten im Kontext der agilen Personaleinsatzplanung", Preisverleihung am 3.11.2022 im Rahmen des Informationsrechtstages der Hochschule Darmstadt.