WearPrivate

Datenschutzfreundliche Vermessung und Auswertung persönlicher Daten mit Wearables zur Erhöhung der Arbeitssicherheit

Fraunhofer IESE | Universität des Saarlandes | WearHealth | neusta mobile solutions

Schlussbericht

Berichtsversion	1.0
Datum	12.02.2025
Verfasser	Reinhard Schwarz, Stefanie Ludborzs, Philipp Neuschwander (Fraunhofer IESE) Bianca Steffes, Ajla Hajric (Universität des Saarlandes) Esteban Bayro-Kaiser (WearHealth) Marcus-Sebastian Schröder (neusta mobile solutions)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 16KIS1511K, 16KIS1512, 16KIS1514, 16KIS1665 und 16KIS1514 gefördert.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Ansprechperson

Dr. Reinhard Schwarz
Fraunhofer Institut für experimentelles Software Engineering IESE
Fraunhofer-Platz 1
67663 Kaiserslautern

E-Mail: reinhard.schwarz@iese.fraunhofer.de

Zusammenfassung

Wearables sind ein zunehmend populäres Werkzeug zur Selbstvermessung, etwa beim Freizeitsport, um das persönliche Training zu überwachen und sinnvoll zu dosieren. In der Arbeitswelt sind Arbeitnehmer zunehmendem mentalen und physischen Stress und zum Teil auch physischen Gefahren ausgesetzt. Wearables sind in der Lage, Anzeichen für solche Belastungs- oder Gefährdungssituationen zu erkennen. Es liegt daher nahe, die von den Wearables erhobenen Daten auch zum Zwecke des Gesundheitsschutzes und der Arbeitssicherheit einzusetzen.

Im Verbundvorhaben WearPrivate haben sich die Verbundpartner mit solchen Einsatzszenarien für Wearables im Arbeitsumfeld befasst. Forschungsgegenstand waren die damit einhergehenden Herausforderungen in Bezug auf den Datenschutz und die Wahrung der Privatsphäre betroffener Arbeitnehmer. Das Vorhaben hatte die Zielsetzung, Konzepte für den datenschutzfreundlichen Einsatz von Wearables am Arbeitsplatz zu entwickeln. Dies soll Anwendungen für den Arbeits- und Gesundheitsschutz der Belegschaft zu ermöglichen, ohne in die Privatsphäre der Arbeitnehmer einzudringen oder einer unethischen Leistungs- und Verhaltenskontrolle durch Wearables Vorschub zu leisten.

Zu diesem Zweck haben die Projektpartner zahlreiche Lösungsbausteine konzipiert und mit Hilfe einer Demonstratoranwendung erprobt. Diese Lösungsbausteine können je nach dem vorliegenden Anwendungsfall kombiniert werden.

Dieser Bericht beschreibt die Problemstellung und die Zielsetzung des Projekts. Er vermittelt einen Überblick über den wissenschaftlichen und technischen Stand, an den angeknüpft wurde, über die durchgeführten Forschungs- und Entwicklungsarbeiten sowie über die erzielten Projektergebnisse und die daraus entstandenen Lösungsbausteine.

Inhaltsverzeichnis

Liste der Abkürzungen

BDSG	Bundesdatenschutzgesetz
DP	Differential Privacy
DSGVO	Datenschutzgrundverordnung
FN	False Negatives
FP	False Positives
GG	Grundgesetz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRCH	Charta der Grundrechte der Europäischen Union
HRV	Herzratenvariabilität
IESE	Fraunhofer Institut für experimentelles Software Engineering (Projektpartner)
IND²UCE	Integrated Distributed Data Usage Control Enforcement
KI	Künstliche Intelligenz
NMS	neusta mobile solutions GmbH (Projektpartner)
O	Objectives (für das technische System)
OE	Environment Objectives (für die Systemumgebung)
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PMP	Policy Management Point
PRP	Policy Retrieval Point
PXP	Policy Execution Point
QR Code	Quick Response Code
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TIB	Technische Informationsbibliothek
TN	True Negatives
TP	True Positives

TPAxO	(Threats, Policies, Assumptions) $\times$ Objectives
UdS	Universität des Saarlandes (Projektpartner)
WH	WearHealth (Projektpartner)
XACML	Extensible Access Control Markup Languag
XML	Extensible Markup Language

1 Zielsetzung des Projekts

Im Verbundvorhaben WearPrivate haben sich die Verbundpartner mit dem Einsatz von Wearables für den Gesundheits- und Arbeitsschutz am Arbeitsplatz befasst und den damit einhergehenden Herausforderungen in Bezug auf den Datenschutz und die Wahrung der Privatsphäre betroffener Arbeitnehmer.

1.1 Problemstellung

Ziel des WearPrivate-Vorhabens war es, Konzepte für den datenschutzfreundlichen Einsatz von Wearables am Arbeitsplatz zu entwickeln. Dies soll Anwendungen für den Arbeits- und Gesundheitsschutz der Belegschaft ermöglichen, ohne in die Privatsphäre der Arbeitnehmer einzudringen.

In dem zugrunde gelegten Szenario messen am Körper getragene Geräte – zum Beispiel Smart Watches, Brustgurte oder Smart Shirts – kontinuierlich relevante Vital-, Bewegungs- und Umwelt-Parameter. Die erhobenen Daten ermöglichen dann Rückschlüsse auf die Belastungen und Gefährdungen, denen der Wearable-Träger ausgesetzt ist. Gefährdungspotentiale sind etwa Übermüdung, Unaufmerksamkeit sowie physische oder mentale Überbeanspruchung. Darüber hinaus können die Daten auch genutzt werden, um den Probanden Rückmeldung zu gesundheitsschädlichen oder riskanten Verhaltensweisen zu geben. Das System kann ihnen Alternativen aufzeigen, wie sie sich gesundheitsfördernder und sicherer verhalten können, zum Beispiel beim Tragen schwerer Lasten oder beim Aufenthalt in Gefahrenbereichen.

Es ist offensichtlich, dass in dem hier skizzierten Anwendungsbereich eine Reihe schützenswerter persönlicher Daten anfallen, die potenziell tiefen Einblick in das Verhalten, das Leistungsvermögen und den Gesundheitszustand des Wearable-Trägers gestatten. Ziel des WearPrivate-Projekts war es, Wearable-Anwendungen zu ermöglichen, in denen der Anwender ausgewählte Analysen seiner Wearable-Daten einem Dritten gestattet, dabei aber die größtmögliche Kontrolle über diese Daten und die daraus abgeleiteten Analyseergebnisse behält. Eine Verarbeitung personenbezogener Daten, die über die vom Anwender zugelassenen Zwecke hinausgeht, soll durch den Einsatz datenschutzfreundlicher Technik verhindert werden, um die Betroffenen vor einer Leistungs- oder Verhaltenskontrolle sowie dem Ausspähen ihres Gesundheitszustands zu bewahren.

1.2 Demonstrator-Anwendungsfall

Als Ausgangspunkt der Überlegungen im Projekt diente ein Wearable-basiertes System zur Überwachung der physischen und mentalen Belastung am Arbeitsplatz. Dieser beispielhafte Anwendungsfall weist viele der maßgeblichen Herausforderungen auf, die der Einsatz von Wearables am Arbeitsplatz mit sich bringt. Die daraus abgeleiteten Konzepte sind daher auf ein breites Spektrum von Anwendungsfällen übertragbar. Die Forschungs- und Entwicklungsarbeiten zielten darauf auf, einen Demonstrator für den nachfolgend beschriebenen Anwendungsfall zu realisieren.

Unser Anwendungsfall sieht vor, dass der Arbeitgeber seine Mitarbeitenden auf freiwilliger Basis mit Wearables ausstattet, die während der Arbeit verschiedene Vital- und Umgebungsparameter erfassen. Typische Wearable-Messwerte sind beispielsweise Puls, Herzraten-Intervalle, Blutsauerstoff-Sättigung, Beschleunigung entlang der Raumachsen, Standort, Umgebungstemperatur oder Luftfeuchtigkeit. Als Wearables können zum Beispiel Smart Watches, Smart Shirts, Brustgurte, GPS-Tracker oder auch einfache Schrittzähler dienen.

Das Wearable meldet seine Messdaten an die persönliche Mobil-App des Wearable-Trägers. Die Arbeitnehmer nutzen das Mobilgerät – typischerweise ein Smartphone – als Nutzerschnittstelle für die Vitaldaten-Kontrolle und außerdem, um ihre jeweiligen Verarbeitungs- und Datenschutzpräferenzen zu verwalten.

Die App sendet die ausgewählten Vitaldaten an einen Analysedienst. Der Dienst berechnet aus den übermittelten Rohdaten Belastungsindizes für die mentale und physische Belastung der Teilnehmer und meldet sie an die jeweilige Teilnehmer-App zurück. Die Teilnehmer erhalten so eine Rückmeldung in Echtzeit, wie es um ihr körperliches und mentales Stresslevel bestellt ist.

Auf Wunsch kann der Dienst auch Alarme an die Teilnehmer-App senden, wenn vordefinierte Belastungsgrenzen überschritten werden. Dies könnte zum Beispiel der Fall sein, wenn ein Dachdecker zu lange in praller Sonne gearbeitet hat und Gefahr läuft, einen Hitzeschlag zu erleiden. Die App kann den Nutzer dann warnen und Empfehlungen aussprechen, wie sich die ermittelte Belastung geeignet reduzieren lässt.

Neben der individuellen Rückmeldung an die Teilnehmer erstellt der Analysedienst auch aggregierte, anonymisierte Gruppenberichte für bestimmte Arbeitsteams. Dazu werden die Teilnehmer in hinreichend große, möglichst homogene Gruppen mit vergleichbarem Beschäftigungsprofil eingeteilt, und die Daten aller Gruppenmitglieder werden auf freiwilliger Basis über einen festgelegten Zeitraum gesammelt und zu Gruppenstatistiken ohne Personenbezug aufbereitet. Abbildung 1 zeigt eine typische Gruppenübersicht, wie sie der Analysedienst für den Arbeitgeber bereitstellen könnte. In Abbildung 2 und Abbildung 3 sind Auszüge aus beispielhaften Gruppenberichten dargestellt.

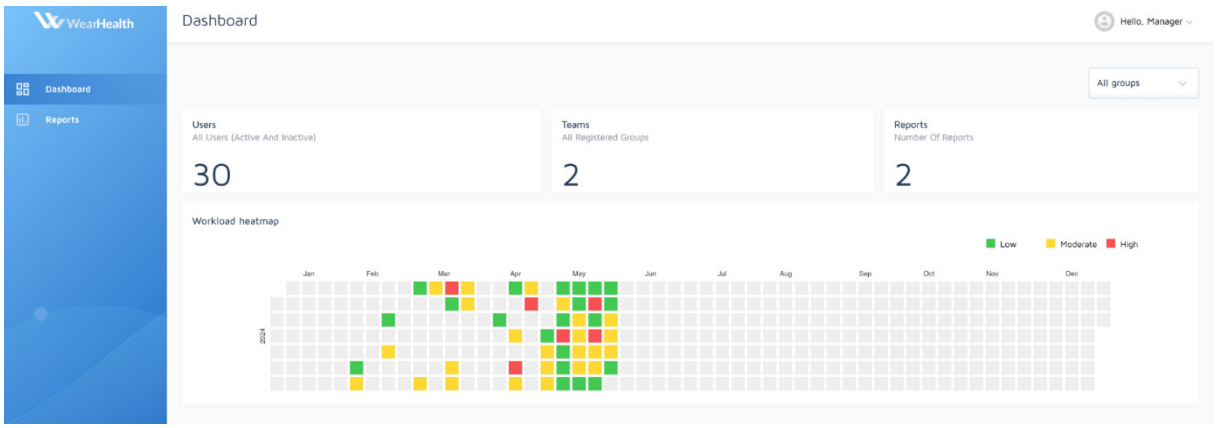


Abbildung 1 Typische Gruppenansicht im Dashboard des Gesundheitsmanagers. Dargestellt ist die mittlere tägliche Belastung eines Arbeitsteams. Jede Spalte entspricht den sieben Tagen einer Kalenderwoche.

Solche Gruppenübersichten und Gruppenberichte sind für das Gesundheitsmanagement des Arbeitgebers bestimmt und sollen Auskunft darüber geben, ob bestimmte Gruppen dauerhaften gesundheitsschädlichen Belastungen ausgesetzt sind. Weist der Gruppenbericht auf solche Überlastungen hin, sollte der Arbeitgeber die Arbeitsabläufe und deren Organisation überdenken und den Kontakt mit der betroffenen Gruppe aufnehmen, um deren Arbeitslast zu senken oder geeignete Ausgleichsmaßnahmen zu treffen.

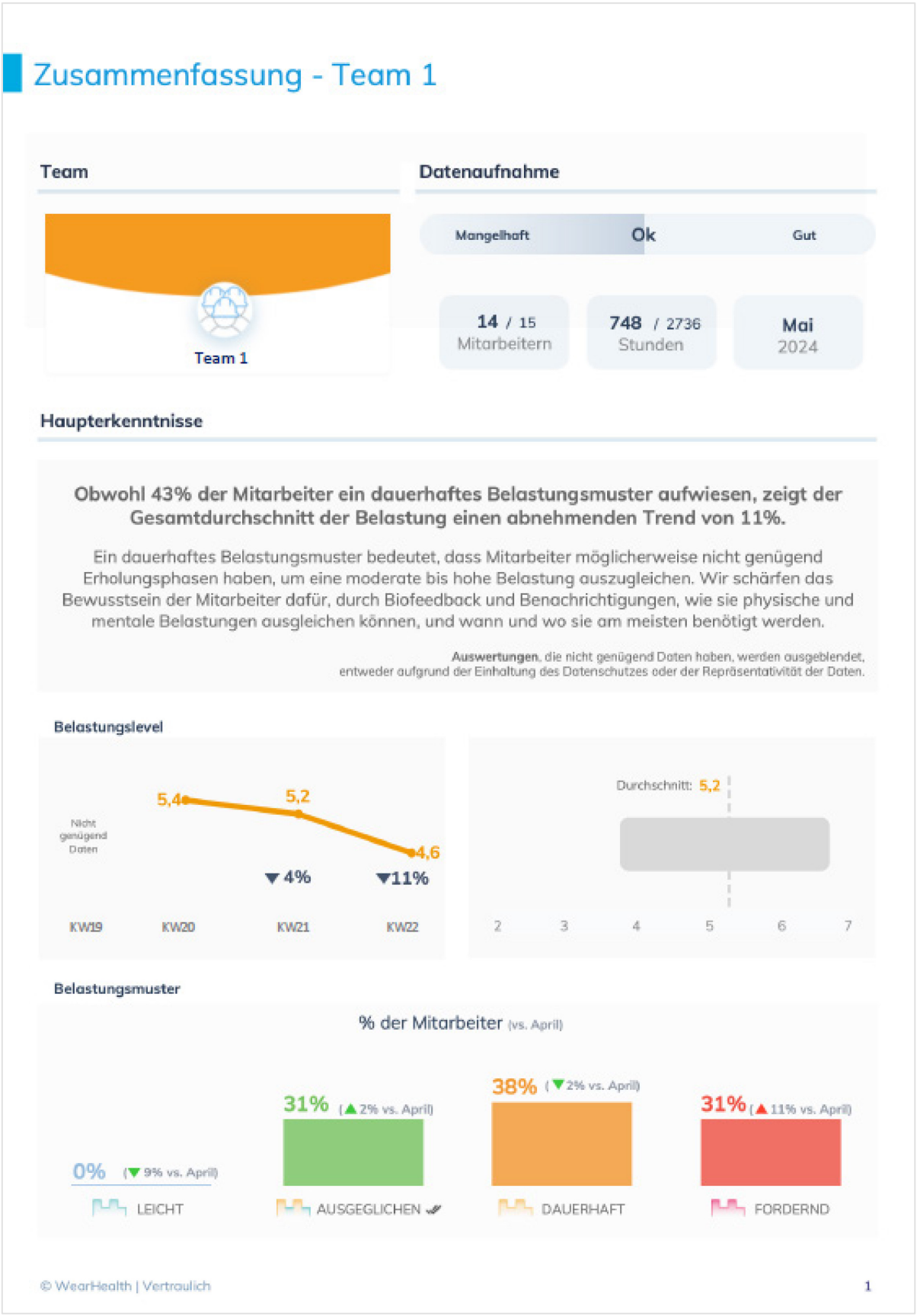


Abbildung 2 Beispielhafter Abschnitt eines Gruppenberichts: Übersicht über die Arbeitsbelastung

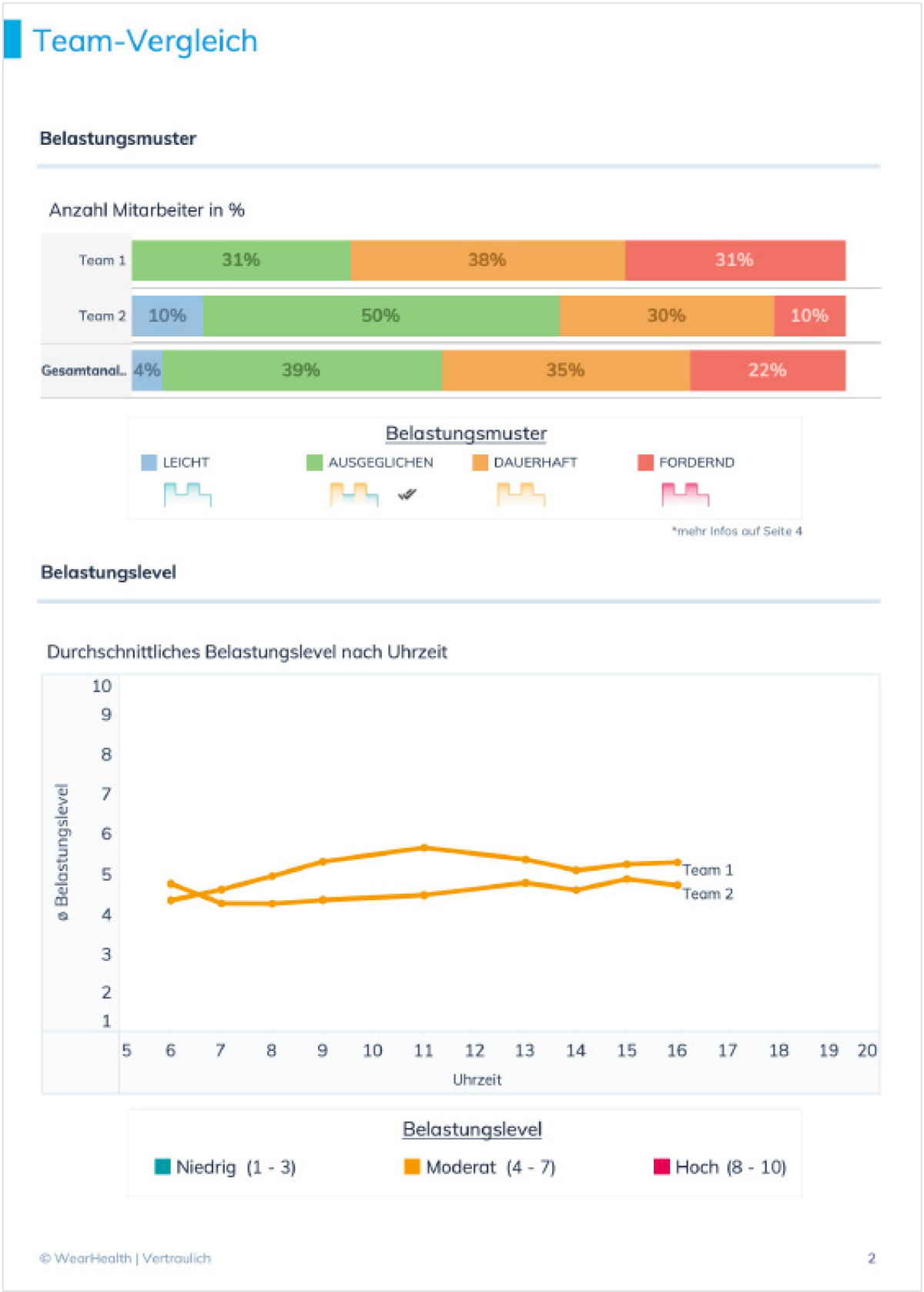


Abbildung 3 Beispielhafter Abschnitt eines Gruppenberichts: Vergleich zwischen verschiedenen Arbeitsteams

2 Wissenschaftlich-technischer Stand, an den angeknüpft wurde

Das Vorhaben WearPrivate fußt auf Vorarbeiten und begleitenden Untersuchungen anderer Projekte, auf die bei den eigenen Arbeiten Bezug genommen wurde.

Das Projekt TrUSD [1] (Laufzeit 09/2018 bis 07/2021) befasste sich mit dem Datenschutz im Arbeitnehmerkontext. Die Zielsetzung war es, mehr Transparenz für den Arbeitnehmer bei der Erhebung, Speicherung, Verbreitung und Nutzung persönlicher Daten am Arbeitsplatz zu schaffen und ihm die Wahrnehmung seiner Selbst- und Mitbestimmungsrechte zu ermöglichen. Ähnlich wie in WearPrivate sah TrUSD ein Privacy-Dashboard als ein Kernelement einer datenschutzfreundlichen Lösung vor. Das Dashboard soll dem Arbeitnehmer als zentrale Auskunftsinstanz in allen Fragen des Datenschutzes dienen und ist zugleich die universelle Schnittstelle, um in allen Unternehmensanwendungen persönliche Datenschutzpräferenzen vorzugeben. Anders als im Projekt WearPrivate zielte das TrUSD-Szenario aber vornehmlich auf klassische Personalstammdaten oder Logdaten von Informationssystemen am Arbeitsplatz, nicht jedoch auf dynamisch erhobene Vitaldaten.

Viele der Ideen aus TrUSD griff das Projekt D'Accord [2] (Laufzeit 9/2021 bis 8/2024) auf. Der Anwendungskontext waren hier digitale Ökosysteme, also Systemverbünde unabhängiger Partner, die ein gemeinsames, umfassenderes Geschäftsmodell realisieren. Angestrebt wurde, eine Ökosystem-Plattform mit einem fertigen Werkzeugkasten auszustatten, der für die gängigen Fragen des Datenschutzes vorgefertigte Lösungsbausteine anbietet, die sich flexibel zu Geschäftsmodell-spezifischen Datenschutzlösungen kombinieren lassen. Wie in TrUSD ist auch hier ein Datenschutz-Cockpit ein wichtiger Lösungsbaustein. Die Arbeiten in D'Accord berühren das Vorhaben WearPrivate insoweit, als die Verarbeitung von Wearable-Daten zumeist an eine Cloud-Lösung geknüpft ist. Eine Cloud als zentrale Datendrehscheibe ist meist involviert, weil einige KI-basierte Analyseverfahren erheblichen Rechen- und Speicherbedarf haben und weil Unternehmen mit entsprechendem Know-how ihre mühsam trainierten Analysemodelle nur ungern aus der Hand geben und in Endgeräte verlagern.

Das Projekt PERISCOPE [3] (Laufzeit 07/2021 bis 06/2024) verfolgte einen Ansatz, der komplementär zu dem des Projekts D'Accord ist: Anstatt die Datenschutzherausforderungen moderner Online-Plattformen als gegeben hinzunehmen und sie technisch zu lösen, zielt PERSICOPE darauf, möglichst datenschutzfreundliche Geschäftsmodelle zu entwickeln, die nur geringe Anforderungen an den Datenschutz stellen. Zusätzlich zu den technischen Lösungen berücksichtigt das Projekt auch ökonomische Analysen, um privatsphärenfreundliche Geschäftsmodelle effizient zu entwickeln. Eine von Grund auf datenschutzfreundliche Gestaltung ist auch für den Wearable-Einsatz am Arbeitsplatz von Bedeutung: Arbeitnehmer werden einer Wearable-Lösung nur zustimmen, wenn sie der Lösung vertrauen. Je privatsphärenfreundlicher die Architektur des Systems, seine dynamische Verarbeitungskette und das zugrundeliegende Geschäftsmodell sind, umso eher werden Arbeitnehmer bereit sein, einen solchen Dienst zu verwenden.

Das Projekt TESTER [4] (Laufzeit 8/2021 bis 8/2024) zielte darauf ab, Transparenz bezüglich der Daten aus der Selbstvermessung mit Wearables zu schaffen. Dazu dient eine auf den Nutzer zugeschnittene Aufbereitung der Daten über die Selbstvermessung in einem interaktiven System, dem Privacy Assistenten. Das Projekt suchte nach möglichst einfachen und unkomplizierten Darstellungsformen, die den unterschiedlichen Anwendern gerecht werden. Der Privacy-Assistent soll es dem Nutzer ermöglichen, informierte Entscheidungen zu treffen und diese auch durchzusetzen. Dies kann zum einen direkt im Privacy-Assistenten erfolgen, der über eine Schnittstelle zum Anbieter Interventionen wie die Löschung, Nichtweitergabe oder Sperrung bestimmter Messdaten direkt vornimmt. Zum

anderen können auch Datenschutzanfragen generiert und zum Beispiel per E-Mail zugestellt werden. TESTER geht dabei eher von einem Szenario aus, in dem die Daten nur zwischen Nutzer und Dienstleister ausgetauscht werden (z. B. Patient und Klinik). Eine Zwischeninstanz, wie etwa der Arbeitgeber im WearPrivate-Anwendungskontext, ist nicht vorgesehen.

Das Projekt InviDas [5] (Laufzeit 05/2020 bis 04/2023) erforschte den Datenschutz beim Einsatz von Smart Watches, Sportuhren und Fitness-Trackern zur Erfassung und Analyse von Gesundheitsdaten. Anders als in WearPrivate stand hier allerdings die private, individuelle Nutzung solcher Smart Wearables im Vordergrund, nicht der Einsatz im Arbeitsplatzkontext. Da die Daten zunächst nur zwischen Dienstanbieter und Nutzer geteilt werden, stellt sich die Situation hier juristisch etwas einfacher dar als am Arbeitsplatz. Im Arbeitsumfeld kann nicht uneingeschränkt von einer Freiwilligkeit der Dienstnutzung ausgegangen werden und die Daten werden hier – wenn auch nur in aufbereiteter Form – auch dem Arbeitgeber zugänglich gemacht. Das Hauptanliegen von InviDas war es, den Anwender über die Übermittlung und Verwendung seiner Daten hinreichend zu informieren, ihm also den Inhalt der Datenschutzerklärung möglichst benutzerfreundlich zu vermitteln. Die Projektergebnisse zielen also vor allem auf Transparenz als Voraussetzung für Selbstbestimmungen. Innovationen zur Ausübung der informationellen Selbstbestimmung sind in InviDas hingegen eher zweitrangig. WearPrivate setzt hier einen etwas anderen Schwerpunkt und zielt sowohl auf Konzepte für nachvollziehbaren Datenschutz (Transparenz) als auch auf Mechanismen für eine aktive Einflussnahme des Arbeitnehmers auf die Erhebung und Analyse seiner Daten (Selbstbestimmung).

Neben der Forschung interessiert sich auch die Industrie zunehmend für den Einsatz von Wearables am Arbeitsplatz. Gerade für gefahrenträchtige Tätigkeitsfelder gewinnen tragbare Monitoring- und Tracking-Lösungen an Bedeutung – etwa im Bergbau, in der Seefahrt, auf Großbaustellen oder auf Bohrinseln sowie bei militärischen Einsätzen. Zahlreiche Anbieter liefern Lösungen, um die physische oder auch psychische Verfassung der eingesetzten Kräfte und deren Umweltbedingungen kontinuierlich zu überwachen oder ihren Aufenthaltsort zu bestimmen [6][7]. In einigen Bereichen, wie etwa dem Tagebau in den USA, ist es sogar vorgeschrieben, die Beschäftigten mit Standort-Trackern auszustatten, um in Gefahrenbereichen rechtzeitig vor anwesenden Personen zu warnen oder bei Unfällen alle Betroffenen schnell aufspüren zu können. Da der Einsatz dieser Technik oft auf gesetzlichen Anforderungen beruht oder vor allem in Ländern mit geringen Datenschutzauflagen üblich ist, sind die Privacy-Schnittstellen solcher Systeme meist nur schwach ausgeprägt. Der Anwender hat dabei kaum Einflussmöglichkeiten, was die Verwendung seiner persönlichen Messdaten betrifft. Als wesentlicher Schutz der Privatsphäre sehen viele Systeme lediglich eine verschlüsselte Übertragung zwischen dem Wearable und dem auswertenden Vorgesetzten oder Betriebsarzt vor; auf eine weitergehende, auch innerbetriebliche Datennutzungskontrolle wird in der Regel verzichtet. Umfragen zeigen jedoch, dass Arbeitnehmer durchaus daran interessiert sind, wie ihre Daten genutzt werden, und dass sie gerne mehr Einfluss auf deren Erhebung und Nutzung nehmen würden [8].

Eine vertiefende Darstellung des wissenschaftlich-technischen Stands, an den das WearPrivate-Vorhaben anknüpft, findet sich im Ergebnisbericht D4.1 [9] des Projekts.

3 Anforderungserhebung

Zu Beginn des Projekts erhoben die Projektpartner die Anforderungen an Wearable-Lösungen für den Einsatz am Arbeitsplatz. Das Augenmerk galt dabei vor allem den Aspekten des Datenschutzes sowie des Interaktionsdesigns: Die Lösung muss nicht nur die Privatsphäre der Nutzer schützen. Sie soll auch IT-Laien eine leichte Bedienbarkeit und gute Verständlichkeit der Datenschutzkonzepte bieten, um dem Anspruch auf Transparenz und informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Messdaten gerecht zu werden.

Abgesehen von den Anforderungen der Nutzer an solche Wearable-Lösungen sind aber auch die berechtigten Interessen der übrigen Beteiligten an einem Messprogramm zu berücksichtigen. Dies betrifft zum einen die Arbeits- und Gesundheitsschutz-Interessen des Arbeitgebers als Initiator des Messprogramms, zum anderen aber auch die kommerziellen Ziele des Dienstleisters, der die Messwerte auswertet und aufbereitet.

Ziel der Anforderungserhebung war es somit, technische, gesetzliche sowie auch kommerzielle Anforderungen an Wearable-Lösungen im beruflichen Umfeld herauszuarbeiten und festzuhalten.

3.1 Analyse verschiedener Anwendungsszenarien

Zunächst führten die Partner eine Literatur- und Projektrecherche zum Stand der Forschung und Technik in Bezug auf Datenschutz und informationelle Selbstbestimmung im Kontext einer Erfassung persönlicher Daten durch. Das Hauptaugenmerk galt hier der Datenerfassung mittels Wearable-Einsatz. Außerdem sammelten die Partner Informationen zu möglichen Wearable-Anwendungen im Arbeitsumfeld für den Gesundheitsschutz oder zur Unfallverhütung.

Wie in Kapitel 2 skizziert wurde, haben sich in den letzten Jahren zahlreiche Forschungsvorhaben mit geeigneten Schnittstellen für die benutzerfreundliche, datenschutzkonforme Kontrolle persönlicher Daten befasst. Dabei wurden zahlreiche Entwurfsmuster für Transparenz, Selbstbestimmung und Zugriffskontrolle vorgeschlagen und erforscht. Diese Arbeiten zeigen anhand verschiedener Beispiele, wie ein Datenschutz-Cockpit in unterschiedlichen Anwendungsdomänen gestaltet werden kann, um den Nutzern eine bestmögliche Übersicht über alle datenschutzrelevanten Vorgänge und über die Regeln der jeweiligen Datenschutzerklärung zu geben. Erforscht wurden in verschiedenen Vorhaben auch Cockpit-Funktionen, die den Nutzern auf einfache und verständliche Weise ermöglichen, ihre Selbstbestimmungsrechte wahrzunehmen. Der Ergebnisbericht D4.1 [9] fasst die Recherchen des WearPrivate-Projekts zusammen und präsentiert typische Beispiele solcher Entwurfsmuster für Transparenz und Selbstbestimmung. Aus der Recherche konnten die Projektpartner wichtige Anforderungen and Wearable-Anwendungen im Arbeitsschutz-Kontext ableiten.

Parallel dazu ermittelten die Projektpartner Analysemöglichkeiten und Geschäftsmodelle für den Wearable-basierten Arbeitsschutz. Sie untersuchten, welche von Wearables ermittelbaren Rohdaten eingesetzt werden können, um den Gesundheitsschutz und die Arbeitssicherheit der Beschäftigten zu verbessern, und wie sich daraus Geschäftsmodelle ableiten lassen. Als Beispiele dienten unter anderem die Geschäftsmodelle des Projektpartners WH und der Firma Ambiotex. Zur Illustration für weitergehende Überlegungen erstellten die Partner Steckbriefe für typische Anwendungen:

- *Belastung im Manufacturing-Bereich:* Körperliche und mentale Belastung der Arbeitnehmer sowie Analyse ihrer Bewegungsmuster

- *Belastung in Risikosituation:* Überwachung der Fitness und Einsatzbereitschaft bei gefahrengeneigten Tätigkeiten und Warnung vor Gefahrensituationen
- *Lokalisierung:* Ortung, Zugangsbeschränkung und Routenoptimierung in großen, unübersichtlichen Arbeitsumgebungen mit besonderen Gefahrenbereichen
- *Ermüdungsmessung:* Überwachung der Fahrtauglichkeit von Berufskraftfahrern und Baumaschinenführern

Die Konkretisierung einzelner Anwendungsfälle erleichterte es, die besonderen Anforderungen in der jeweiligen Situation zu ergründen und relevante Stakeholder und deren Interessen besser zu verstehen. Die Anwendungsfälle wurden aus der Perspektive der verschiedenen Beteiligten analysiert, um deren jeweiligen Bedarfe und Vorbehalte zu ermitteln, die adressiert werden müssen.

Neben dem *Arbeitgeber* als Betreiber, dem betrieblichen *Gesundheitsmanagement* als Nutznießer eines Wearable-Messprogramms und den *Beschäftigten* als unmittelbaren Nutzern der Anwendung und ihrer Analyseergebnisse gibt es weitere Akteure mit berechtigten Interessen:

- *Betriebsrat:* Der Betriebsrat wacht über die Wahrung der Arbeitnehmerrechte, insbesondere über den betrieblichen Datenschutz und das Verbot der Leistungs- und Verhaltenskontrolle.
- *Lösungsanbieter:* Der Anbieter von Wearable-Lösungen und entsprechenden Analysediensten für den Arbeitsschutz hat einerseits berechtigte kommerzielle Interessen; zum anderen hat er weitgehende Zugriffsmöglichkeiten auf die Anwendung, die erhobenen Wearable-Daten und die abgeleiteten Analyseergebnisse, was erhebliche Missbrauchspotenziale birgt.

Die Betrachtung der spezifischen Interessen dieser Akteure diente dazu, gemeinsame, wiederkehrende Datenschutz- und Datennutzungsprobleme aus den Szenarien abzuleiten, darunter

- *Ablehnung des Messprogramms* durch einen der Beteiligten oder mangelnde Motivation der Belegschaft zur Teilnahme
- *Fehlende Abgrenzung von Arbeit und Freizeit* bei der Datenerhebung
- *Mangelnde Datenmenge oder Datenqualität* aufgrund störender Einflüsse
- *Mangelnder Schutz der Daten* und *mangelnde Kontrolle über deren Weitergabe*
- *Zweckentfremdung der Analyseergebnisse* und mögliche Nachteile für einzelne Teilnehmer des Messprogramms
- *Sozialer Druck* und mangelnde Entscheidungsfreiheit zur Teilnahme am Messprogramm

Anhand der Anwendungsfall-Analysen konnten sowohl technische und gesetzliche Anforderungen als auch Anforderungen an die Attraktivität und Sozialverträglichkeit der Anwendungsgestaltung ermittelt werden.

3.2 Eingangsbefragung

Um einen Eindruck zu gewinnen, wie Arbeitnehmer generell zu einem möglichen Wearable-Einsatz am Arbeitsplatz stehen, führten die Projektpartner zu Projektbeginn eine Eingangsbefragung durch. Die Befragung erfolgte online mit einem Befragungswerkzeug und es nahmen insgesamt 74 Personen daran teil – überwiegend Belegschaftsangehörige der Projektpartner IESE und NMS.

Die Befragung nahm bewusst noch keinen Bezug auf spezielle Lösungskonzepte des WearPrivate-Konzepts, um zunächst ein unbeeinflusstes Stimmungsbild zu gewinnen.

Abbildung 4 bietet einen Überblick über die Zusammensetzung der Befragungsgruppe; Abbildung 5 zeigt, inwieweit die Befragten mit der Verwendung von Wearables vertraut sind oder sich vorstellen könnten, Wearables – nicht notwendigerweise im Arbeitsumfeld – überhaupt zu nutzen.

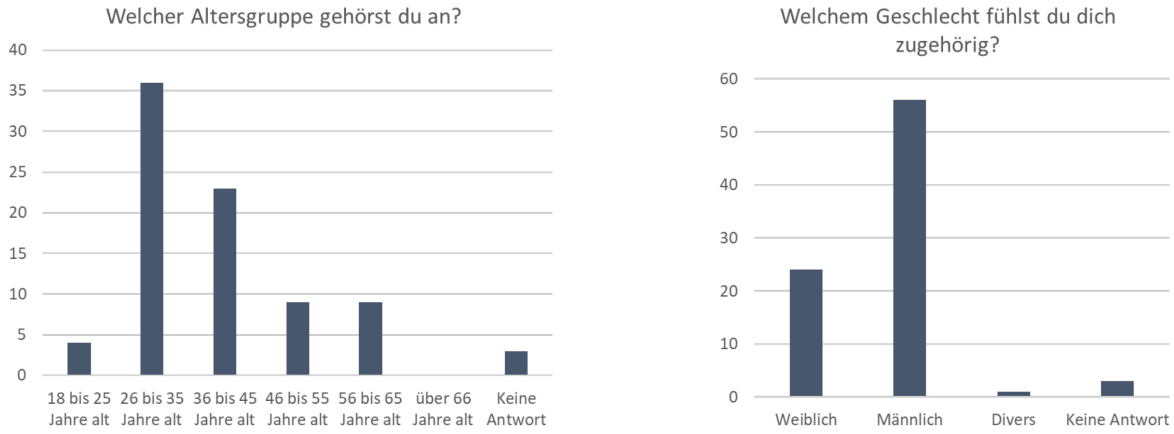


Abbildung 4 Demografische Angaben zu den 74 Teilnehmern der Eingangsbefragung

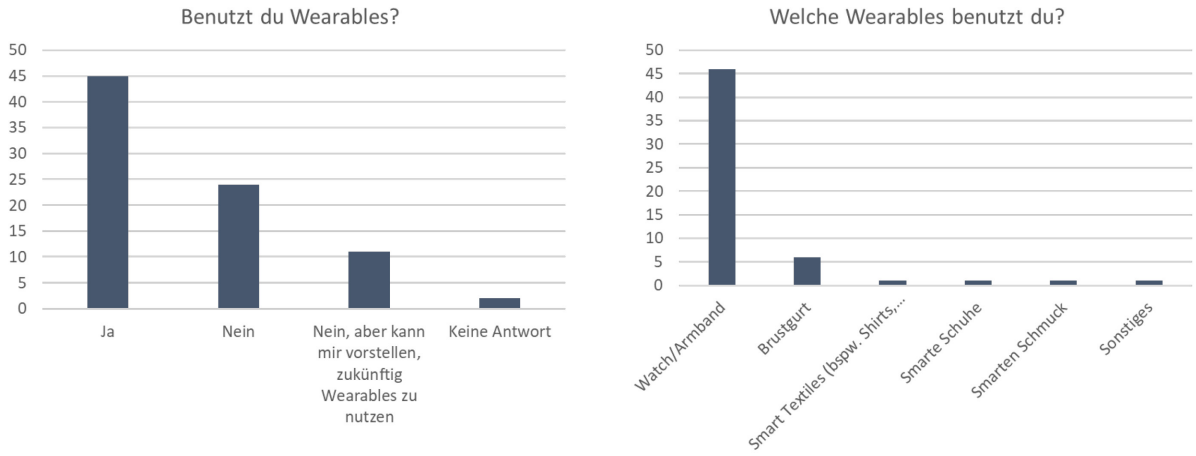


Abbildung 5 Erfahrung der Befragten mit gängigen Wearable-Technologien

Die Befragung sollte Aufschluss über mögliche Vorbehalte gegen Wearable-basierte Messprogramme liefern und über die Bereitschaft, Messdaten mit Dritten zu teilen. Sie sollte auch zeigen, welche Bedürfnisse die Befragten haben, damit sie bereit wären, eine Teilnahme an einem Messprogramm in Erwägung zu ziehen.

Darüber hinaus dienten die Befragungsergebnisse den Projektpartnern als Referenzwerte. Ein Vergleich sollte später zeigen, inwieweit die im Projekt vorgeschlagenen Datenschutz- und Interaktionskonzepte geeignet sind, die Zustimmung zu einer Teilnahme an einem Wearable-Messprogramm zu erhöhen.

Die Befragung ergab, dass mittlerweile viele Arbeitnehmer bereits persönliche Erfahrungen mit Wearables haben (Abbildung 5). Offenbar sind zumindest Smart Watches und Brustgurte im Sport- und Freizeitbereich inzwischen gut etabliert.

Betrachtet man Abbildung 6, so sehen die Befragten die Selbstvermessung offenbar als Privatsache an. Die Bereitschaft, Wearable-Daten zu teilen, beschränkt sich überwiegend auf den Familien- und Freundeskreis oder den Austausch im Sportbereich. Eine ähnlich hohe Bereitschaft findet sich nur noch

im Gesundheitsbereich gegenüber medizinischen Fachkräften. Kaum Zustimmung findet dagegen, Wearable-Daten mit dem Arbeitgeber zu teilen.

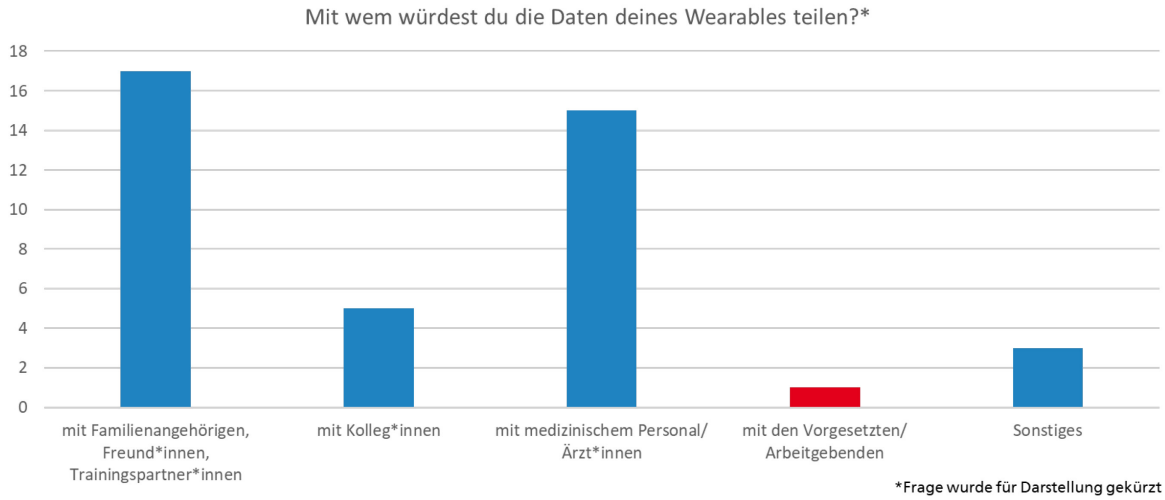


Abbildung 6 Bereitschaft der Befragten, ihre Wearable-Daten mit Dritten zu teilen

Dementsprechend gering fällt die Zustimmung aus, Wearables im beruflichen Kontext zu nutzen. Etwa die Hälfte der Befragten lehnt dies auf Basis ihrer bisherigen Erfahrungen mit einer Wearable-Nutzung ab (Abbildung 7). Dies zeigt, dass entsprechende Messprogramme im beruflichen Umfeld sehr viel Überzeugungsarbeit leisten müssen, um freiwillige Teilnehmer zu rekrutieren.

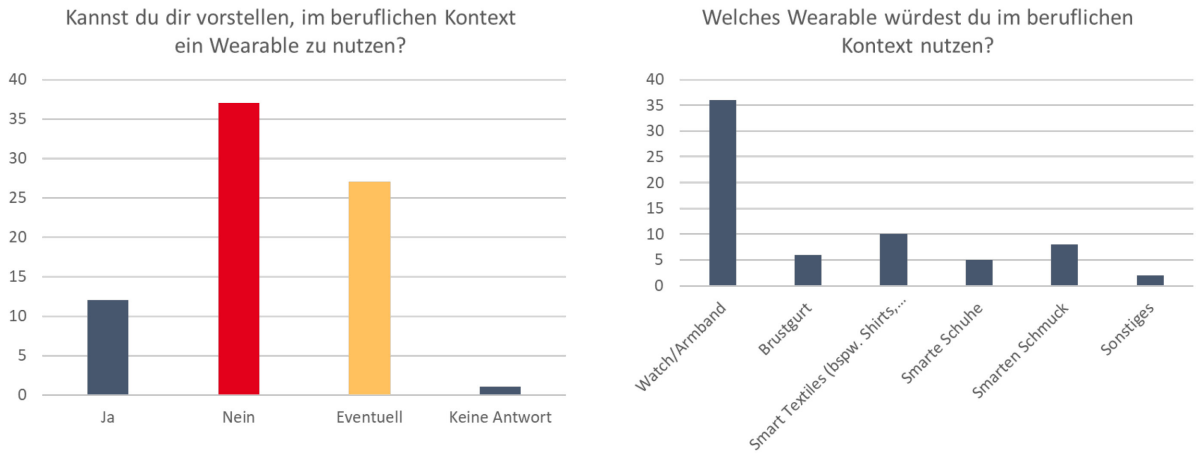


Abbildung 7 Bereitschaft der Befragten, Wearables im beruflichen Kontext zu nutzen: Hier gibt es unter den Befragten große Vorbehalte.

Selbst wenn man die gemessenen Rohdaten nicht ungefiltert teilt, sondern nur einen davon abgeleiteten abstrakten »Belastungsindex«, besteht nur eine geringe Bereitschaft, den eigenen individuellen Belastungsindex im beruflichen Kontext mit Kollegen oder mit dem Arbeitgeber zu teilen (Abbildung 8, links). Deutlich höhere Zustimmung lässt sich erzielen, wenn solche Belastungsmessungen nur als aggregierte Gruppenwerte geteilt werden sollen: Immerhin mehr als ein Fünftel der Befragten wäre bereit, solche Werte mit dem Vorgesetzten zu teilen (Abbildung 8, rechts).

Das Umfrageergebnis spiegelt die große Skepsis der Befragten wider, an einem Wearable-Messprogramm am Arbeitsplatz teilzunehmen, obwohl die Befragten gegenüber Wearables im privaten Bereich durchaus aufgeschlossen sind und überwiegend bereits Erfahrungen mit einer Selbstvermessung haben.

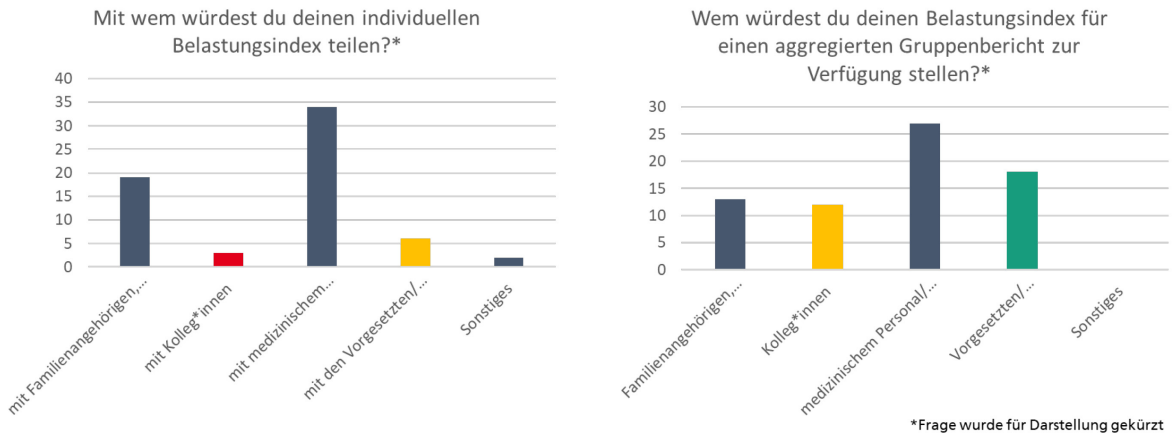


Abbildung 8 Bereitschaft der Befragten, einen persönlichen Belastungsindex (links) zu teilen oder für einen aggregierten Gruppenbericht offenzulegen (rechts): Man erkennt, dass die Befragten ihre individuelle Belastung am Arbeitsplatz eher nicht offenlegen würden; die Zustimmung steigt, wenn die Daten durch Aggregation anonymisiert werden.

Dies zeigt sich auch in den Freitext-Kommentaren der Befragten (Abbildung 9): Sie fürchten Überwachung oder persönliche Nachteile aufgrund unvorteilhafter persönlicher Messwerte.

Welche Bedenken und Vorbehalte hast du?

- "Fühlt sich wie Überwachung an."
- "Personen, die Personalentscheidungen treffen, sollten (…) keinen Zugriff auf Gesundheitsdaten haben, da diese sonst bei Personalentscheidungen eine Rolle spielen könnten."
- "… könnte die Firma ja denken, dass Nutzer häufiger krank wird und vorab kündigen, bevor höhere Personalkosten entstehen."
- "Physische und psychische Gesundheit (…) sind meine Privatsache. Ich teile derartige Anliegen nur mit vertrauten Personen."

Abbildung 9 Typische Vorbehalte der Befragten gegen Wearable-Messprogramme am Arbeitsplatz

Vergleicht man die Ergebnisse gemäß Abbildung 8 mit denen aus Abbildung 6, so liefert dies einen Fingerzeig, wie sich die Teilnahmebereitschaft prinzipiell steigern lässt:

- Statt unverarbeiteter Rohdaten sollten nur abgeleitete Kenngrößen mit dem Arbeitgeber geteilt werden, die keinen unmittelbaren Einblick in den Gesundheits- und Fitnesszustand der Betroffenen ermöglichen.
- Die ermittelten Kenngrößen sollten nur aggregiert bereitgestellt werden, bezogen auf eine Personengruppe (d.h. ein Arbeitsteam) statt auf einzelne Personen, um nicht Einzelne bloßzustellen.

Neben diesen begünstigenden Faktoren war den Befragten Transparenz und Selbstbestimmung besonders wichtig, also eigene Kontrolle über die Weitergabe und Nutzung ihrer Daten, sowie eine Freiwilligkeit der Teilnahme (Abbildung 10).

Unter welchen Voraussetzungen kannst du dir eine Nutzung vorstellen? Gibt es weitere wichtige Aspekte? (Auszug)

- "…nur **bewusstes Teilen** bestimmter Daten mit ausgewählten Personen."
- "**Kontrolle** über die Daten: **Transparenz**, was geteilt wird und was nicht ..."
- "Sehen, **wann** und **wer** hat meine Daten gesehen, und **welche** Daten genau..."
- „**Kontrolle** über meine Daten, **Transparenz** hinsichtlich der erfassten Daten "
- "…sichergestellt sein, dass **kein** direkter oder indirekter **Druck** auf Personen ausgeübt wird"
- "**Freiwilligkeit**! **Keine Überwachung**! Es soll, (…) praktischen Nutzen und Mehrwert für die Arbeit bieten."

Abbildung 10 Auszug aus den Freitextantworten der Befragten (Hervorhebungen im Text nachträglich ergänzt)

Einschränkend ist anzumerken, dass die Befragten überwiegend im Bereich der Software-Forschung und -Entwicklung beschäftigt sind. Sie hatten daher engere Berührungspunkte mit Datenschutzfragen als der Bevölkerungsdurchschnitt, weil Datenschutzanforderungen in Softwaresystemen zunehmend an Bedeutung gewinnen. Dies lässt erwarten, dass sie besonders sensibilisiert sind, wenn der Schutz ihrer Privatsphäre berührt ist, und dass sie daher einem Wearable-Messprogramm möglicherweise besonders kritisch gegenüberstehen. Hinzu kommt, dass eine Beschäftigung im Software-Bereich nicht zu den besonders gefahrengeneigten Berufen gehört – im Gegensatz zu Berufsfeldern wie etwa Bergbau, Seeschifffahrt, Forstwirtschaft oder Feuerwehr. Daher ist der persönliche Nutzen, den die Beschäftigten von einem Wearable-Messprogramm erwarten, in der Software-Domäne voraussichtlich geringer ausgeprägt als in Berufssparten mit hohen Gefährdungspotenzialen. Auch dies mindert die Motivation, sich an einem solchen Messprogramm zu beteiligen.

3.3 Datenschutzrechtlicher Rahmen

Im Projekt wurde auch der datenschutzrechtliche und ethische Rahmen für eine Verarbeitung personenbezogener Wearable-Daten betrachtet.

Geht es um die Verarbeitung personenbezogener Daten, sind Grundrechte auf unionsrechtlicher sowie auf nationaler Ebene betroffen. Konkret geht es um das allgemeine Persönlichkeitsrecht, welches das Recht auf informationelle Selbstbestimmung beinhaltet (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG), um das Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRCH) und das Recht auf den Schutz personenbezogener Daten (Art. 8 GRCH).

Zur rechtlichen und ethischen Bewertung wurde zunächst geprüft, welche Verordnungen, Richtlinien und Gesetze im Rahmen des Projekts von Relevanz sind. Neben der Datenschutzgrundverordnung (DSGVO), dem Data Act, dem European Health Data Space und der ePrivacy-Richtlinie sind auch das Bundesdatenschutzgesetz und das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) sowie die Landesdatenschutzgesetze anwendbar.

In dem Fall, dass eine vollständige Anonymisierung nicht möglich ist, war zunächst zu klären, auf welcher Rechtsgrundlage Wearable-Daten im Beschäftigtenkontext verarbeitet werden können. Geprüft wurde zunächst die Einwilligung nach dem TDDDG und anschließend über die Öffnungsklausel des Art. 88 Abs. 1 DSGVO auch die Einwilligung im Beschäftigtenverhältnis nach § 26 Abs. 3 S. 2, Abs. 2 BDSG. Im Rahmen der Einwilligung in die Verarbeitung von Wearable-Daten im Beschäftigtenkontext lag aufgrund des bestehenden Abhängigkeitsverhältnisses zwischen Arbeitgeber und Arbeitnehmer ein besonderes Augenmerkt auf der Freiwilligkeit. Freiwilligkeit liegt dann vor, wenn der Arbeitnehmer echte Wahlfreiheit hat. Der Arbeitnehmer könnte sich allerdings aus Angst vor Nachteilen am Arbeitsplatz bei einer verweigerten Einwilligung in einer Drucksituation befinden, die zu einem inneren

Zwang führt. Auch könnte es zu sozialem Druck kommen, wenn andere Arbeitnehmer der Verarbeitung zugestimmt haben und die Nutzung oder Nichtnutzung aufgrund der Art des Wearables für andere deutlich zu erkennen ist. All dies hätte zur Folge, dass die Einwilligung nicht freiwillig ergeht und somit unwirksam ist. Im Ergebnisberichts D2.1 [10] zur rechtlichen und ethischen Bewertung wurden deshalb mögliche Gegenmaßnahmen gegen sozialen Druck betrachtet.

Neben der Einwilligung als mögliche Rechtsgrundlage wurden zudem die Rechtsgrundlagen des § 26 Abs. 3 S. 1 BDSG, des Art. 9 Abs. 2 lit. h DSGVO und des Art. 6 DSGVO geprüft.

Innerhalb des Projekts galt es sodann zu klären, wer die datenschutzrechtliche Verantwortlichkeit trägt und wer unter Umständen Auftragsverarbeiter ist. Dies ist relevant, da der Verantwortliche die Informationspflichten im Sinne des Art. 13 und 14 DSGVO zu erfüllen hat und als Ansprechpartner für die Ausübung von Betroffenenrechten fungiert. Zusätzlich existiert gemäß Art. 5 Abs. 2 DSGVO die Rechenschaftspflicht, wonach der Verantwortliche die Einhaltung der Grundsätze der Datenverarbeitung nachweisen muss. Zudem treffen ihn auch andere Haftungsrisiken als den Auftragsverarbeiter.

Zudem wurden die Informationspflicht des Verantwortlichen und das Transparenzgebot untersucht. Dabei wurde insbesondere aufgezeigt, welche Auswirkungen die aus der Informationspflicht erwachsenen Anforderungen auf die Gestaltung der Mobil-App haben. Im Anschluss wurden die Rechte der betroffenen Personen beleuchtet.

Darüber hinaus wurden die technischen und organisatorischen Maßnahmen gemäß der DSGVO analysiert. Im Zuge dessen entstand ein Überblick über klassische Maßnahmen zum Schutz der Gewährleistungsziele für die rechtskonforme Verarbeitung von personenbezogenen Daten. Ergänzend wurden die technischen und organisatorischen Vorkehrungen nach § 19 TDDDG dargestellt.

Der Bericht zum datenschutzrechtlichen Rahmen schließt mit einem Überblick über die rechtlichen Anforderungen, der als Orientierungshilfe dient. Die genauen Anforderungen sind allerdings im Lichte des jeweiligen Anwendungsfalls zu betrachten und richten sich auch danach, auf welche Rechtsgrundlagen abgestellt werden soll. Die detaillierte Ausarbeitung der datenschutzrechtlichen und ethischen Rahmenbedingungen ist im Ergebnisbericht D2.1 [10] zu finden.

3.4 Systematische Bedrohungsanalyse zur Ermittlung des Schutzbedarfs

Neben den grundlegenden Anforderungen an Datenschutz, Transparenz und informationelle Selbstbestimmung waren darüber hinaus auch grundlegende IT-Sicherheitsanforderungen zu berücksichtigen, denn:

- Ein Datenschutzkonzept kann nur dann erfolgreich und glaubhaft umgesetzt werden, wenn es nicht durch böswillige Manipulation unterlaufen werden kann.
- Es gibt weitere berechtigte Interessen der Beteiligten, etwa den Schutz des Messprogramms vor manipulierten Messwerten und Sabotage oder die Abwehr von Trittbrettfahrern, die den Analysedienst ohne Vergütung nutzen wollen.

Um auch solche Anforderungen zu erfassen, bedienten wir uns der in [11] und im Ergebnisbericht D1.1 [12] in Abschnitt 8.4 beschriebenen Analysemethode.

Das Verfahren basiert darauf, jede Bedrohung durch ein 3-Tupel (Threat Agent, Asset, Adverse Action) zu charakterisieren: Ein Angreifer (Threat Agent) greift ein bedrohtes Gut des Anwendungsfalls (Asset) mit einer böswilligen Aktion (Adverse Action) an. Die im 3-Tupel-Format erhobenen Bedrohungen werden in einer Bedrohungsmatrix (Abbildung 11) dokumentiert. Die Spalten der Bedrohungsmatrix

repräsentieren je einen Angreifertyp, die Zeilen je ein Asset; im Matrixelement im Schnittpunkt einer Spalte und einer Zeile werden alle identifizierten Schadaktionen[1] vermerkt, die der entsprechende Angreifer auf das entsprechende Asset anwenden kann. Dabei zeichnet sich jeder Angreifertyp durch seine individuellen *Angriffsmotive*, sein spezifisches *Wissen* und seine *Angriffsfähigkeiten* sowie die ihm verfügbaren *Ressourcen* zur Durchführung des Angriffs aus.

Abbildung 11 zeigt einen Ausschnitt der Bedrohungsmatrix des von uns betrachteten Anwendungsfalls (»Kontrolle der physischen und mentalen Belastung am Arbeitsplatz«). Genauere Informationen dazu finden sich in [12].

	Unauthorized Entities			Authorized entities		
	Third Party (TP) unrelated entity that should have no access to WearPrivate solution	**Platform Operator (PO)** Cloud service provider for Analysis Service (if different from AS)	**Acquaintance of Employee (ACQ)** friend, colleague, or relative who is not officially included in the measurement program	**Participant (PRT)** staff member working for EMP using WearPrivate App and participating in Stress Level Monitoring program	**Employer (EMP)** (offering Stress Level Monitoring program)	**Analysis Service (AS)** computing stress level of individual PRT from their vital data
Motivation to attack or manipulate	* May try to **obtain access to personal identifiable data** * May want to **sabotage the monitoring program** as a data privacy activist * May try to **gain acces to the intellectual property of the service providers**	* May want to **exfiltrate personal identifiable data** to interested third parties (or to lauch a blackmailing attack on individual PRT)	* May want to **sneak into the monitoring program** for personal stress-level monitoring without paying (free riding)	* May want do **disguise their true group membership** to increase privacy protection * May want to **only pretend to participate** to evade peer pressure (→ a valid pattern according to our concept) * May want to **sabotage the monitoring program** because of a strong data privacy conviction * May want to **gain acces to personal identifiable data of other participants**	* May want to **re-identify individual employees** to determine their individual stress resilience or their willingness/refusal to participate in group monitoring * May want to **gain access to individual raw data** for unauthorized additional purposes (e.g., performance evaluation of PRTs) * May want to **include more participants** into the program **than paid for** to the service provider (fee fraud)	* May want to **exfiltrate personal identifiable data** to interested third parties * May try to **re-identify individuals** based on their profile and vital raw data * May try to **derive other information from raw data apart from stress levels** * May **charge MS for more analyses than actually performed** (fee fraud)
Information Assets: Spoofing, Tampering, Information Disclosure						
PRT profile data (e.g., age, gender, weight, height)	Tampering with profile data to cause nonsensical analysis results SABOTAGE	Exfiltrating personal identifyable data from PRT profile PRT_RE-IDENT PRT_DATA_DISCLOSURE		Spoofing the profile data on registration to sabotage program SABOTAGE	Disclosing the exact profile of individual participants to more easily re-identify them later on PRT_RE-IDENT Spoofing fake group members to obtain individual measurement results by subtracting the faked data from the group report PRT_DATA_DISCLOSURE ENTITY_SPOOFING	Using "fingerprinting" to find the correct participant matching the profile PRT_RE-IDENT Deriving additional insights into participant's health status and habits based on profile data EXCESSIVE_MONITORING
PRT Vital parameters monitored (e.g., Heart Rate Variability,Acceleration)	Tampering with vital raw data to cause nonsensical analysis results SABOTAGE	Exfiltrating personal identifyable monitoring data of PRT PRT_RE-IDENT PRT_DATA_DISCLOSURE		Forging the vital parameters on registration to sabotage program SABOTAGE	Disclosing the raw vital data measured for the participant PRT_RE-IDENT Spoofing fake group members to obtain individual measurement results by subtracting the faked data from the group report PRT_DATA_DISCLOSURE ENTITY_SPOOFING	Using "fingerprinting" to find the correct participant matching the profile PRT_RE-IDENT Deriving additional insights into participant's health status and habits based on raw data EXCESSIVE_MONITORING
PRT Geo-location (should only be used within Smartphone app but not transmitted to AS)	Tampering with location information (e.g., GPS signal or beacon signal) to cause unintended policy decisions or nonsensical analysis results PRT_DATA_DISCLOSURE SABOTAGE			Tampering with the location data on registration to sabotage program SABOTAGE	Tampering with the definition of relevant geo-information (e.g., to extend monitoring beyond the work place) EXCESSIVE_MONITORING	Tracing back individuals to their homes to re-identify them PRT_RE-IDENT Deriving additional insights into participant's habits EXCESSIVE_MONITORING
PRT credentials ("ticket" for participation, PRT ID, PRT group ID, PRT password)	Spoofing the ID of a PRT IDENTITY_THEFT Registering for the service without proper MS ticket TICKET_FRAUD Tampering with PRT credentials to render PRT account disfunctional SABOTAGE	Disclosing credentials of PRTs Spoofing the ID of a PRT IDENTITY_THEFT	Abusing valid PRT ticket to sneak into the monitoring program IDENTITY_THEFT TICKET_FRAUD	Failing to unregister and unneccessarily occupying an account if leaving the monitoring program SABOTAGE Spoofing group ID to hide in a different group ENTITY_SPOOFING Inflating the size of the own group by inserting fake IDs SABOTAGE Forgetting or compromising one's own password PASSWORD_LOSS IDENTITY_THEFT	Disclosing the participant/ticket relation to re-identify the identity of an AS data record PRT_RE-IDENT Spoofing fake group members to obtain individual measurement results by subtracting the spoofed data from the group report ENTITY_SPOOFING Spoofing tickets to sneak in additional participants (ticket fraud) TICKET_FRAUD	Disclose ID/ticket relationship to EMP or MS to support PRT re-identification PRT_RE-IDENT

Abbildung 11 Ausschnitt der Bedrohungsmatrix

Wiederkehrende, vergleichbare Bedrohungen der Matrix werden zusammengefasst und unter einem gemeinsamen Bedrohungsnamen weiterverarbeitet (in Abbildung 11 in roten Großbuchstaben zu erkennen). Für den in WearPrivate betrachteten Anwendungsfall ergaben sie so unter anderem die Bedrohungen gemäß Abbildung 12.

Der Schutzbedarf des Systems ergibt sich jedoch nicht nur aus den Bedrohungen, denen das System ausgesetzt ist. Darüber hinaus gelten für ein System, das persönliche Daten erfasst und datenschutzrelevante Funktionen bereitstellt, auch allgemeine gesetzliche Vorgaben sowie – im Allgemeinen – auch domänenspezifische Standards, Best Practices oder Qualitätsansprüche des

1 Als Ausgangspunkt für die Ermittlung möglicher Schadwirkungen, auf die ein Angreifer zielen könnte, können zum Beispiel die sogenannten STRIDE-Kategorien [13] dienen: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

Herstellers an die Sicherheit seine Produktpalette. In der von uns angewendeten Analysemethode werden diese Vorgaben zusammenfassend als *Security Policies* bezeichnet.

PRT_DATA_DISCLOSURE	Disclose sensitive personal data of a PRT, such as vital data, individual stress level, general health status, detailed profile data
GROUP_DATA_DISCLOSURE	Disclose group report data to unauthorized parties
EXCESSIVE_MONITORING	Record and analyze wearable data beyond those purposes PRT agreed to or at times or places PRT explicitly excluded from monitoring
PRESSURING_EMPLOYEES	Put pressure on employees to unvoluntarily join the stress monitoring program
PASSWORD_LOSS	Loss of a PRT's login credentials (i.e., ID and password)
IDENTITY_THEFT	Falsely adopt the identity of a PRT or EMP
DISTRACTION	Distract PRT by push notifications in safety-critical situations
TICKET_FRAUD	Use the service without payment or invoice service fees without providing service to the customer

Abbildung 12 Beispielhafte abgeleitete Bedrohungsdefinitionen aus der Bedrohungsmatrix gemäß Abbildung 11

Ergänzend zur Bedrohungsanalyse wurden für die Anforderungsanalyse daher relevante Security Policies ergänzt, die im Rahmen der Literaturrecherche und der Analyse gesetzlicher Vorgaben zuvor ermittelt worden waren. Als Hilfsmittel dient dabei eine sogenannte TPAxO-Matrix[2] (Abbildung 13).

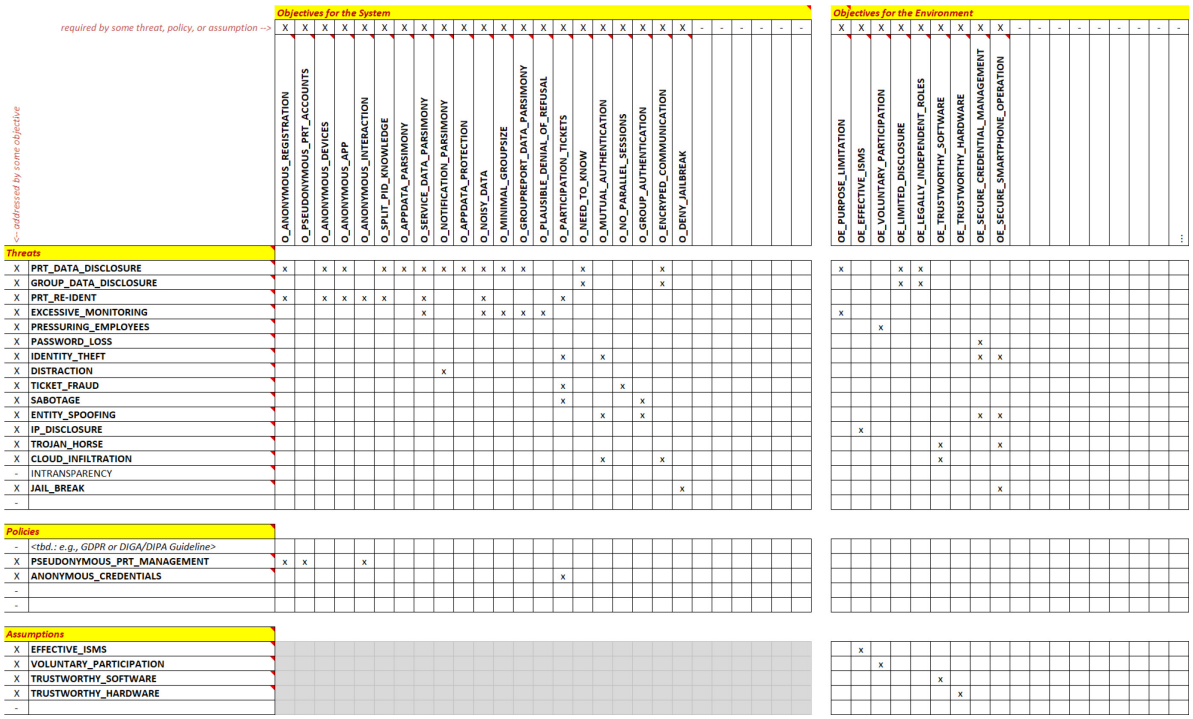


Abbildung 13 Momentaufnahme der TPAxO-Matrix für unseren Anwendungsfall »Belastungsmessung am Arbeitsplatz«

Die Matrix listet in ihren Zeilen alle Bedrohungen (Threats) und Security-Richtlinien (Policies). Diesen Einträgen werden nun in den Matrixspalten geeignete Sicherheitsziele (sogenannte Objectives: O bzw. OE) zugeordnet, die dazu dienen, die Bedrohung zu bekämpfen und die Security Policy durchzusetzen. Dabei bedarf es mitunter mehrerer, sich ergänzender Sicherheitsziele, um einer einzelnen Bedrohung ausreichend zu begegnen oder eine Policy wirksam durchzusetzen. Neben den Abschnitten für Threats und Policies gibt es zusätzlich noch einen Abschnitt für getroffene Annahmen (Assumptions). Annahmen bezeichnen Sachverhalte, die aus Sicht des Analyseteams als gegeben vorausgesetzt

[2] Der Name TPAxO soll an die die Zuordnung der Form {Threats, Policies, Assumptions} × Objectives erinnern.

werden (siehe [11], Abschnitt 5.5). Die Ergebnisse der Analyse und die daraus abgeleitete Sicherheitslösung gelten nur vorbehaltlich dieser Annahmen.

Jeder Bedrohung und jeder geltend gemachten Policy ist eine Reihe von Sicherheitszielen (Objectives) zugeordnet. Dabei bezeichnen *System Objectives* (O) Ziele, die innerhalb des Systems technisch umgesetzt werden sollen. Im Unterschied dazu bezeichnen *Environment Objectives* (OE) Ziele, die außerhalb des Systems realisiert werden sollen, entweder durch nichttechnische organisatorische Prozessvorgaben oder durch technische Lösungen, die von Partnersystemen außerhalb der betrachten Analysegrenzen realisiert werden (z. B. durch eine vorgeschaltete Firewall).

Alle Objectives erhalten einen eindeutigen Namen und eine zugeordnete Zieldefinition, die in der Matrix als Kommentar an die entsprechende Zelle angeheftet wird. Das Analyseteam erstellte und vervollständigte nach dem beschriebenen Verfahren die TPAxO-Matrix. Als Ergebnis entstand so eine Liste von technischen Zielen und nicht-technischen Umgebungszielen. Die technischen Ziele bildeten die Grundlage für die Ableitung detaillierter Systemanforderungen auf der Systementwurfsebene. Tabelle 2 zeigt einen kleinen Ausschnitt der Anforderungen, die nach dem beschriebenen Verfahren systematisch hergeleitet wurden. Ausführlichere Angaben finden sich im Ergebnisbericht D1.1 [12].

Tabelle 1 Bedrohungen, resultierende Ziele und abgeleitete Anforderungen aus Sicht der verschiedenen Rollen

Bedrohung	Ziel	ID	Anforderung
Anforderungen aus Sicht der Arbeitnehmer (AN)			
Re-Identifizierung anhand der App T_PRT_RE-IDENT	Die App wird als generische Software ohne Personalisierung bereitgestellt O_ANONYMOUS_APP	R_AN1	Die App kann anonym über eine öffentlichen App Store bezogen werden
	Zum Betrieb der App ist es nicht erforderlich, seine wahre Identität preiszugeben (z. B. Name, Adresse, Ausweisnummer, ...) O_ANONYMOUS_REGISTRATION O_ABONYMOUS_INTERACTION	R_AN2	Die App-Software fragt niemals Angaben zur Identität des Nutzers (z. B. Name, Adresse, Ausweisnummer) ab und erhält keinen Zugriff auf Adressverzeichnisse oder andere private Daten des Smartphones.
Re-Identifizierung anhand der Kommunikationsbeziehung T_PRT_RE-IDENT	Mit vertretbarem Aufwand kann die Identität eines AN nicht (allein) anhand seiner Kommunikationsbeziehung zum Analysedienst aufgedeckt werden. O_SPLIT_PID_KNOWLEDGE	R_AN3	Der AN gibt sich nur mittels nicht personalisiertem Freischaltcode (Registrierungstoken RT) als autorisierter Nutzer zu erkennen und wird bei AS nur unter Pseudonym PSEU geführt; danach erfolgt die Autorisierung beim Einloggen mittels PSEU + Passwort
	Dienstnutzer müssen keine Kommunikationsbeziehung zum Vertrieb (MV), zum Arbeitgeber (AG) oder zu anderen AN auf digitalem Wege aufbauen. O_SPLIT_PID_KNOWLEDGE	R_AN4	Der Bezug eines Freischaltcodes RT erfolgt außerhalb der WearPrivate App
	AG, MV oder andere AN erhalten keinen Einblick in die Verbindungsdaten zwischen AN und AS O_SPLIT_PID_KNOWLEDGE O_ENCRYPTED_COMMUNICATION	R_AN5	AS und AN kommunizieren über eine verschlüsselte Verbindung, die durch PSEU + Passwort authentisiert wird
	MV und AS erhalten im Rahmen der Registrierung und der Teilnahme an einer Messkampagne keine Auskunft über die Identität der teilnehmenden AN O_ANONYMOUS_REGISTRATION O_ANONYMOUS_INTERACTION O_SPLIT_PID_KNOWLEDGE		*siehe Anforderung R_AN3*
…	…	…	…
Anforderungen aus Sicht des Arbeitgebers (AG)			
Inanspruchnahme des Analysekontingents durch unbefugte Dritte T_TICKET_FRAUD T_IDENTITY_THEFT	Nur Nutzer, die vom AN ausdrücklich autorisiert wurden, können sich beim Dienst registrieren O_PARTICIPATION_TICKETS O_MUTUAL_AUTHENTICATION	R_AG1	Die Nutzerregistrierung erfordert einen fälschungssicheren Freischaltcode RT, den MV generiert und der nur einmal nutzbar ist. Nutzer erhalten ihren Freischaltcode ausschließlich von AG, der seinerseits das

			Kontingent an benötigten Freischaltcodes zuvor mit MV vertraglich geregelt hat.
Verfälschung der Gruppenstatistik durch falsche Gruppenzuordnung der AN T_SABOTAGE T_ENTITY_SPOOFING	Nur jene AN, die AG ausdrücklich für eine Gruppenmitgliedschaft autorisiert hat, können einer Analysegruppe beitreten O_GROUP_AUTHENTICATION	R_AG2	Die Registrierung in einer Analysegruppe erfordert einen entsprechenden Freischaltcode GID. Der AG vergibt fälschungssichere, nicht wiederverwendbare Gruppencodes an die Mitarbeiter, die zu einer Gruppe zusammengefasst werden sollen. Der Gruppencode GID bezeichnet die jeweilige Gruppe.
	Der Dienst bietet dem AN die Möglichkeit, seine Gruppenzugehörigkeit eindeutig nachzuweisen. O_GROUP_AUTHENTICATION		*siehe Anforderung R_AN14*
…	…	…	…

Anforderungen aus Sicht von Marketing & Vertrieb (MV)			
Unentgeltliche Inanspruchnahme des Dienstes durch unbefugte Dritte T_TICKET_FRAUD	Abweisen von Registrierungen, die das vertragliche Mengengerüst überschreiten O_PARTICIPATION_TICKETS	R_MV1	Die Kontrolle des Mengengerüsts erfolgt über fälschungssichere Freischaltcodes zur einmaligen Registrierung (Registrierungstokens RT) und bei Bedarf zur Gruppenmitgliedschaft (GID). MV prüft bei jeder Registrierung die Gültigkeit des entsprechenden Freischaltcodes und invalidiert diesen danach. Die Anzahl der Registrierungen wird dabei mitgezählt und gemäß vertraglich vereinbartem Analysekontingent geeignet reglementiert.
		R_MV2	Je nach Bezahlmodell und Vereinbarung zum Analysekontingent erfolgt eine rechtzeitige Mitteilung an AG, wenn das Analysekontingent ausgeschöpft zu werden droht. In diesem Fall sind Nachverhandlung zwischen MV und AG möglich.
			Ggf. eine Vertragsgestaltung, bei der eine Überschreitung gar nicht eintreten kann, z. B. Flatrate oder Verdrängung durch Least-recently-used-Strategie, siehe R_AG10
…	…	…	…

Anforderungen aus Sicht des Analyseservices (AS)			
Unentgeltliche Inanspruchnahme des Dienstes durch unbefugte Dritte T_TICKET_FRAUD	Abweisen von Registrierungen, die das vertragliche Mengengerüst überschreiten O_PARTICIPATION_TICKETS	R_AS1	AS prüft die Gültigkeit aller Registrierungstickets und weist Registrierungsversuche ohne gültigen Freischaltcode zurück. Für gültige Freischaltcodes ist die Vergütung durch das vertraglich vereinbarte Analysekontingent gesichert.
Ausspähen von geistigem Eigentum T_IP_DISCLOSURE	Sensitive Analysealgorithmen werden nur in Umgebung ausgeführt, die gegen Ausspähen geschützt ist. OE_EFFECTIVE_ISMS	R_AS2	Kritische Teile der Analyselogik werden entweder in der Cloud unter AS-Kontrolle ausgeführt, oder die Smartphone-App stellt dafür eine geeignete gekapselte Ausführungsumgebung zur Verfügung, die gegen Ausspähen gesichert ist.
…	…	…	…

Anforderungen an Entwickler und Tester (E)			
Bedrohung des Datenschutzes durch fremde, nicht selbst entwickelte Software-Komponenten T_TROJAN_HORSE	Fremdsoftware für die Realisierung der Smartphone-App sollte vermieden werden OE_TRUSTWORTHY_SOFTWARE	R_E1	Der Einsatz externer Frameworks zur Implementierung der Smartphone-App ist zu minimieren.
	Fremdkomponenten müssen den Ansprüchen von WearPrivate an Datenschutz, Transparenz und informationelle Selbstbestimmung genügen OE_TRUSTWORTHY_SOFTWARE	R_E2	Eingesetzte Fremdsoftware muss auf Datenschutz- und Sicherheitsmängel überprüft werden, ehe sie für die Realisierung der Smartphone-App genutzt werden.
		R_E3	Eingesetzte Fremdsoftware soll möglichst im Quellcode-Format vorliegen und erst beim Erzeugen des Binaries unter eigener Kontrolle übersetzt werden.

Bedrohung der Datenschutzmechanismen der Smartphone-App durch Jailbreaks T_JAIL_BREAK	Das Betreiben der WearPrivate-App auf einem per Jailbreak modifizierten Smartphone soll unterbunden werden O_JAILBREAK_DENIAL	R_E4	Die Smartphone-App soll einen Mechanismus zur Jailbreak-Erkennung enthalten. Wird ein modifiziertes Betriebssystem erkannt, so muss die App-Software automatisch gestoppt und der Zugriff auf den Dienst muss verweigert werden.
…	…	…	…

4 Datenschutzkonzepte

Ein Wearable-Messprogramm am Arbeitsplatz ist rechtlich und ethisch nur vertretbar, wenn die Vermessung der Belegschaftsangehörigen die Privatsphäre der Belegschaft schützt und gewährleistet, dass die gewonnenen Messdaten nicht zur Leistungs- oder Verhaltenskontrolle der Mitarbeitenden missbraucht werden. Um die erhobenen Stamm- und Wearable-Daten der Betroffenen zu schützen, wurden im Projekt verschiedene Konzepte entwickelt und evaluiert.

4.1 Datenschutzfreundliche Systemarchitektur

Eine datenschutzfreundliche Systemarchitektur kann Datenschutzrisiken bereits wesentlich reduzieren. Je weniger Bedrohungspotenziale die Systemarchitektur und die Prozesskette der Datenverarbeitung aufweisen, umso weniger Schutzmaßnahmen oder vertragliche Regelungen sind erforderlich, um die Privatsphäre der Beteiligten zu wahren.

Ausgangspunkt unserer Überlegungen war ein Gesundheitsdienst nach konventionellem Muster, angelehnt an Geschäftsmodelle, wie sie zum Beispiel bei Fitness-Trackern im Freizeitbereich üblich sind. Hier besteht eine direkte Geschäftsbeziehung zwischen dem Dienstleister und den Dienstnutzern: Weil die private Dienstnutzung den Nutzern selbst in Rechnung gestellt wird, benötigt der Dienstleister auch deren Kontakt- und Bezahldaten.

Eine naheliegende, aus Datenschutzsicht jedoch unbefriedigende Realisierung des Gesundheitsdienstes im betrieblichen Umfeld ist deshalb, die Dienststruktur einfach um eine weitere Rolle – den Arbeitgeber – zu erweitern, im Übrigen aber an der Struktur eines privat genutzten Dienstes festzuhalten. Dies läuft auf eine Realisierung gemäß Abbildung 14 hinaus.

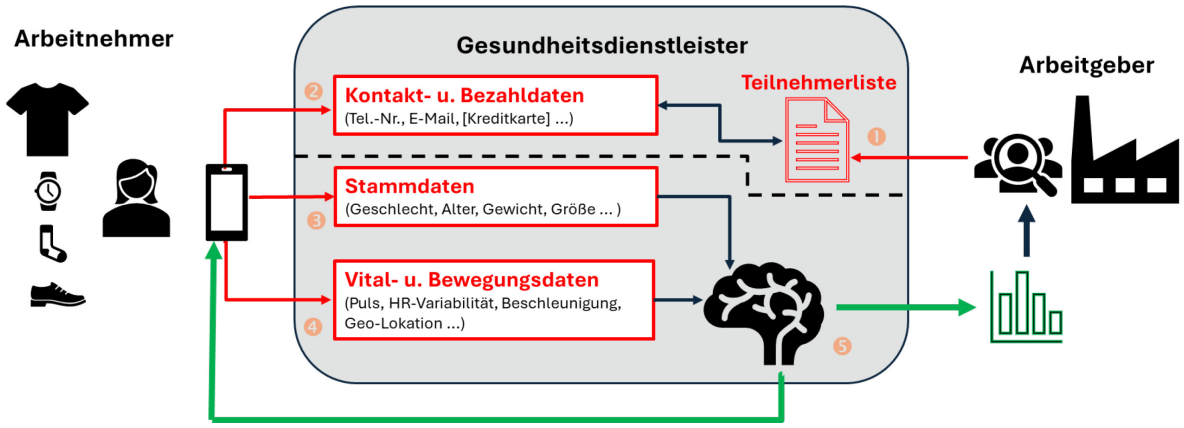


Abbildung 14 Konventionelle, wenig datenschutzfreundliche Struktur eines Wearable-basierten Gesundheitsdienstes: ❶ Der Arbeitgeber beauftragt ein Messpragramm und nominiert die vorgesehenen Teilnehmer. ❷ Die Teilnehmer registrieren sich mit ihren Kontaktdaten, die der Dienstleister anhand der Teilnehmerliste prüft. ❸ Nach erfolgreicher Registrierung teilt der Nutzer seine zur Analyse benötigten Stammdaten mit. ❹ Die Vitaldatenerfassung kann nun beginnen. ❺ Anhand der Stammdaten und den erhobenen Daten der eingesetzten Wearables (z. B. Smart Watch, Smart Shirt, Brustgurt, Schrittzähler ...) berechnet der Dienst individuelles Feedback für den Nutzer und eine Gruppenstatistik für vorgegebene Arbeitnehmer-Teams für den Arbeitgeber. Diese Dienstarchitektur bewirkt eine Anhäufung kritischer persönlicher Daten beim Dienstleister.

Wie aus der Abbildung ersichtlich ist, erhält der Dienstleister bei dieser Lösung umfassende Einblicke in die persönlichen Daten der Teilnehmer. Er kennt nicht nur deren Stamm- und Messdaten, sondern kann diese Daten auch mit den Kontaktdaten verknüpfen. Dieser Personenbezug der angehäuften

persönlichen Daten setzt die Teilnehmer erheblichen Datenschutzrisiken aus, denen der Dienstleister durch aufwändige technische und organisatorische Maßnahmen entgegenwirken muss. Um die Nutzer vom Schutz ihrer Privatsphäre zu überzeugen, sind längliche Datenschutzerklärungen erforderlich.

Gesundheitsdienstleister, die eine Lösung gemäß Abbildung 14 wählen, werden bestrebt sein, innerbetrieblich die Analysedaten von der Kontaktdaten zu trennen und möglichst getrennte IT-Systeme und separate Mitarbeiterteams für die getrennten Bereiche einzusetzen. Kleine Unternehmen verfügen aber mitunter nicht über eine ausreichende Personalstärke (z. B. wenn es die Systemadministration betrifft), um eine solche Trennung vollständig umzusetzen. Für die Nutzer sind solche Maßnahmen zudem schwer nachzuprüfen; sie müssen auf die Datenschutz-Erklärung des Dienstleisters vertrauen und dessen Kompetenz, den erklärten Datenschutz auch korrekt umzusetzen.

Um einen engen Personenbezug der erhobenen Daten und die damit einhergehenden Datenschutzrisiken zu vermeiden, bietet sich eine anonyme Registrierung der Teilnehmer an. Da das Messprogramm vom Arbeitgeber beauftragt und bezahlt wird, ist es grundsätzlich nicht erforderlich, Kontaktdaten der teilnehmenden Arbeitnehmer zu erheben. Stattdessen kann die Autorisierung zur Teilnahme am Messprogramm mittels fälschungssicherer »Eintrittskarten« geregelt werden. Abbildung 15 zeigt einen solchen Lösungsansatz.

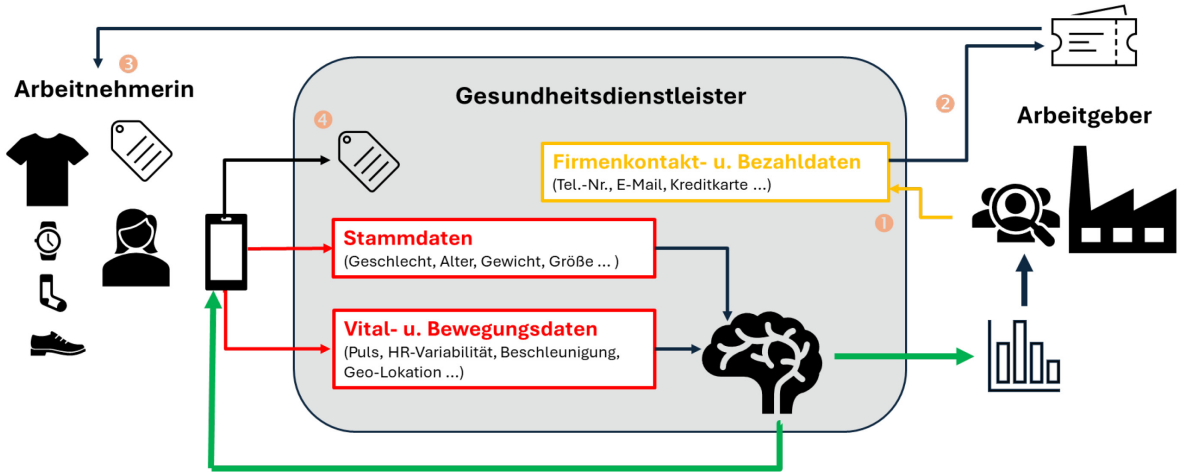


Abbildung 15 Verbesserter Datenschutz durch anonyme Registrierung mittels Teilnehmertickets: ❶ Der Arbeitgeber beauftragt ein Messprogramm für eine bestimmte Anzahl von Teilnehmern. ❷ Der Dienstleister stellt eine hinreichende Zahl von Tickets (digital signierte, fälschungssichere Token) für die Teilnahme aus und übergibt sie dem Arbeitgeber zur Verteilung an seine Belegschaft. ❸ Die Teilnehmer ziehen sich zufällig ein Ticket aus der verfügbaren (am besten überdimensionierten) Ticketmenge des Arbeitgebers. ❹ Die Teilnehmer registrieren sich nun anonym beim Dienstleister und weisen ihre Teilnahmeberechtigung mit ihrem gültigen Ticket nach, das jedoch keinen Personenbezug enthält. Bei erfolgreicher Registrierung entwertet der Dienstleister das Ticket, um eine Wiederverwendung zu unterbinden. Die weiteren Schritte entsprechen dem Ablauf in Abbildung 14

Als fälschungssicheres Ticket kann zum Beispiel ein QR-Code dienen, der neben der Messprogramm-Nummer, für die das Ticket gelten soll, eine digitale Signatur enthält, die der Dienstleister leicht überprüfen kann. Sobald sich der Nutzer mittels seines Tickets als zugelassener Teilnehmer am Messprogramm ausgewiesen hat, wird eine Teilnehmerkennung erstellt und der Nutzer wählt ein Passwort, mit dem er künftig Zugriff auf seine Kennung erhält, ohne seine Identität preisgeben zu müssen. Sein Ticket wird invalidiert, um eine Wiederverwendung zu unterbinden. Im Folgenden dient die Teilnehmerkennung als Pseudonym für den Teilnehmer, und nur der Teilnehmer selbst weiß, welche Identität hinter der Kennung steckt.

Mit der anonymen Registrierung ist ein kleiner Nachteil verbunden: Wenn der Teilnehmer sein Passwort vergisst, gibt es keine Möglichkeit, die Kennung auf ein neues Passwort zurückzusetzen. Der

Teilnehmer kann nämlich nicht beweisen, dass er der authentische Inhaber der Kennung ist. Daher benötigt der Teilnehmer bei Verlust seines Passworts ein neues Ticket, und er muss eine neue Kennung anlegen; seine alte Kennung und die zugeordneten Daten sind verloren.

Auch in Bezug auf den Datenschutz weist die Lösung gemäß Abbildung 15 noch eine Schwäche auf. Der Dienstleister hat noch immer Zugriff auf wichtige Kontextinformationen zum Messprogramm, die eine Identifizierung der Teilnehmer erleichtern könnten, denn er kennt deren Arbeitgeber. Dies ermöglicht unter Umständen Einblicke in die Unternehmensstruktur und hilft so, den Kreis der »Verdächtigen« drastisch einzuschränken bei dem Versuch, die Identität eines Teilnehmers zu entschleiern. Kennt man zum Beispiel die Stammdaten der Person wie Geschlecht, Größe, Körpergewicht und Alter, so lässt sie sich in einer kleinen Gruppe möglicher Kandidaten meist leicht ermitteln.

Um diese Schwäche zu beseitigen, empfiehlt sich eine strikte Rollentrennung, indem man den Gesundheitsdienst in zwei unabhängige Instanzen aufspaltet: Analysedienst und Vertrieb. Abbildung 16 zeigt diesen Lösungsansatz.

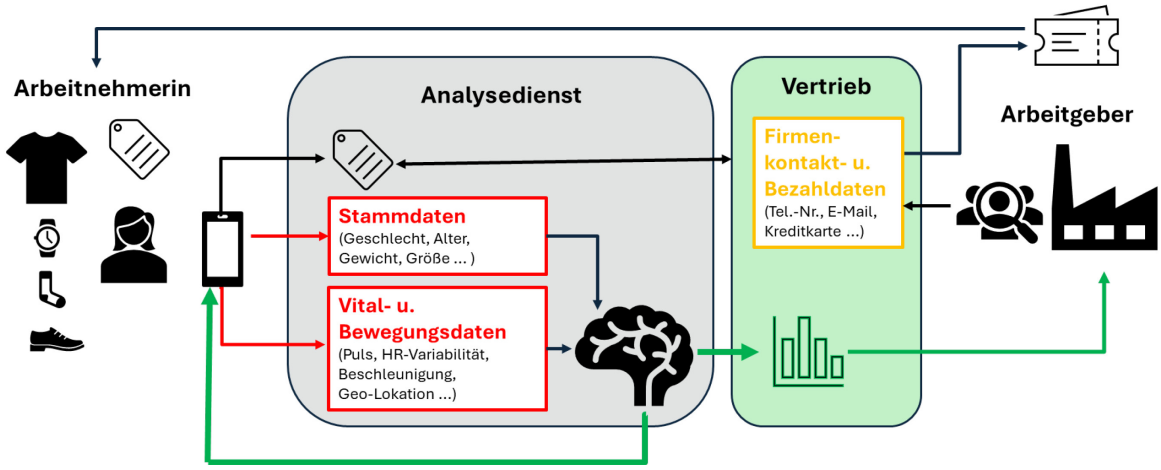


Abbildung 16 Datenschutzfreundliche Rollentrennung zwischen Analysedienst und Vertrieb

Die vorgeschlagene Rollentrennung bewirkt, dass der Analysedient nun keine Kontextinformationen über das Messprogramm erhält; für die Beurteilung der gemessenen Daten ist dies auch nicht erforderlich. Umgekehrt kennt der Vertrieb zwar den Auftraggeber und kann sich so Kontextinformationen zu den Teilnehmern beschaffen, hat allerdings keinerlei Zugriff auf die Stamm- oder Messdaten der Betroffenen, sondern sieht nur aggregierte statistische Auswertungen. Trotz dieser Trennung kann sich der Analysedienst darauf verlassen, dass seine Aufwände vergütet werden, indem er die erhaltenen Tickets mit dem Vertrieb verrechnet.

Die Vision für eine solche datenschutzfreundliche Dienstarchitektur wäre es, dass ein zentraler, auf medizinische Auswertungen spezialisierter Analysedienst Aufträge für möglichst viele Vertriebspartner übernimmt und dadurch sehr viele verschiedene Teilnehmer-Datensätze verwaltet, deren Herkunft sich über das ganze Land erstreckt. Eine solche große Menge von anonymisierten Teilnehmern ermöglicht es dem einzelnen Nutzer, in der Masse unterzutauchen: Zu jedem Stammdatenmerkmal gibt es bei einem hinreichend großen Kundenstamm viele Teilnehmerkennungen mit gleichem oder sehr ähnlichem Attributwert. Dadurch hat ein Angreifer wenig Anhaltspunkte, welche dieser Kennungen einem gesuchten Teilnehmer entspricht.

Vorstellbar wäre etwa, dass ein auf künstliche Intelligenz spezialisierter Anbieter hochpräzise, medizinisch abgesicherte Analysemodelle erstellt und dass zum Beispiel verschiedene Krankenkassen als Vertriebsorganisationen auftreten und Gesundheitslösung in Kooperation mit dem

Analysedienstleister vermarkten. Analysedienst und Vertriebsorganisation wären dann völlig unabhängig agierende Wirtschaftsunternehmen.

Die datenschutzfreundliche Dienstarchitektur gemäß Abbildung 16 zielt darauf ab, dass keine der beteiligten Rollen ohne die Mitwirkung einer anderen Rolle den Datenschutz brechen kann. Selbst wenn sich eine Rolle böswillig nicht an seine Datenschutzerklärung hält, wenn sich ein unzufriedener Mitarbeiter als Innentäter über die geltenden Schutzmaßnahmen hinwegsetzt oder wenn ein Hacker in die Unternehmens-IT eindringt, sind die persönlichen Daten der Teilnehmer noch geschützt und können nicht ohne Weiteres einem konkreten Individuum zugeordnet werden.

Ein großer Vorteil einer datenschutzfreundlichen Architektur wie etwa der in Abbildung 16 ist die leichte Vermittelbarkeit der Schutzwirkung. Man kann dieses Konzept auch IT-Laien recht gut nahebringen und sie so von der Datenschutzwirkung überzeugen. Dies ist gerade in einem Arbeitsplatzumfeld, wo die Teilnahme am Messprogramm nur auf freiwilliger Basis erfolgen darf, ein sehr wichtiger Aspekt. Hier reicht es nicht, faktisch ein hohes Datenschutzniveau zu erzielen: Die Teilnehmer müssen dies auch nachvollziehen können, um Vertrauen in das Messprogramm zu fassen.

4.2 Datennutzungskontrolle

Die datenschutzfreundliche Systemarchitektur gemäß Abschnitt 4.1 bildet die Basis für eine darauf aufsetzende Datennutzungskontrolle. Zu diesem Zweck nutzte das Projekt das modulare MYDATA-Framework [14]. Dieses Rahmenwerk basiert auf den Ergebnissen des Partners IESE im Kontext der IND²UCE-Forschung [15]. Abbildung 17 vermittelt einen Überblick über die MYDATA-Komponenten zur Datennutzungskontrolle. Die MYDATA-Terminologie ist an den XACML-Standard [16] angelehnt.

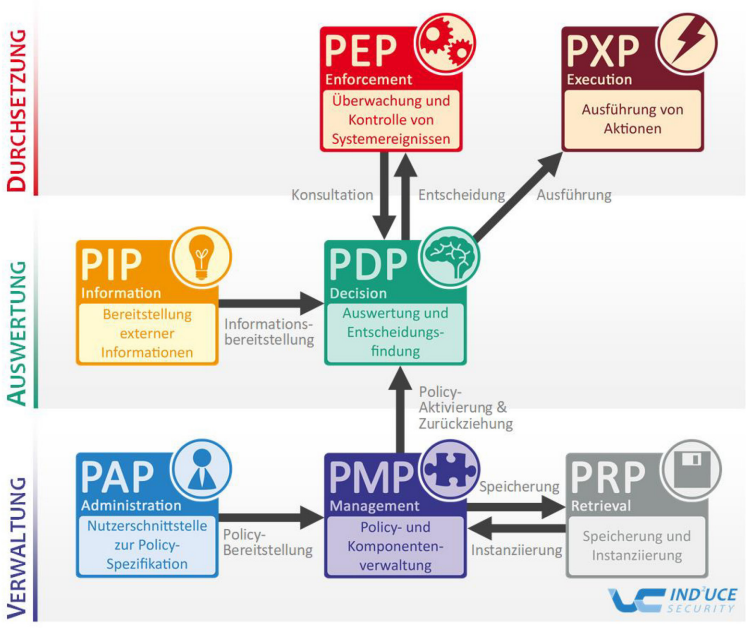


Abbildung 17 Komponenten des MYDATA-Frameworks zur Datennutzungskontrolle (Bildquelle: [17])

Der MYDATA-Ansatz sieht vor, relevante Datenverarbeitungen (z. B. die Verwendung der Daten oder deren Offenlegung durch Übermittlung) einer Menge von Datennutzungsrichtlinien zu unterwerfen. Diese Richtlinien beschreiben, was mit den Daten getan oder nicht getan werden darf. Damit können die beteiligten Stakeholder ihre Datenschutzbedürfnisse, individuelle Präferenzen oder Vorgaben im Zusammenhang mit der Datenverarbeitung ausdrücken. Dies umfasst insbesondere die Datenschutz- und Selbstbestimmungsbedürfnisse der Betroffenen, in unserem Fall also der Wearable-nutzenden

Arbeitnehmer, die ihre persönlichen Vital- und Umgebungsdaten für verschiedene Auswertungen potenziell bereitstellen.

Relevante Datenverarbeitungsversuche (z. B. die Offenlegung der Vitaldaten durch Übermittlung an den Analysedienst oder die Verwendung der Daten zur Erstellung des Gruppenberichts) werden von sogenannten Policy Enforcement Points (PEPs) kontrolliert. Ehe ein PEP die Verarbeitung zulässt, fragt er zunächst bei einem Policy Decision Point (PDP) an, ob die gewünschte Verarbeitung in Einklang mit den zuvor vereinbarten Datennutzungsrichtlinien steht. Der PDP prüft die gewünschte Verarbeitung, wobei er neben den relevanten Datennutzungsrichtlinien auch noch weitere Kontextinformationen (z. B. Ort und Zeitpunkt der gewünschten Verarbeitung oder Identität des Verarbeiters) berücksichtigen kann, die er von Policy Information Points (PIPs) bezieht. Wenn die Richtlinien die gewünschte Verarbeitung erlauben, so autorisiert der PDP den PEP und dieser gibt die Daten für die jeweilige Verarbeitung frei. Untersagt eine Richtlinie die Verarbeitung, so instruiert der PDP den PEP entsprechend und dieser unterbindet die Datenverarbeitung.

Datennutzungsrichtlinien können die Verarbeitung auch an gewisse Auflagen binden, etwa die Maßgabe, dass die Daten vor einer Freigabe anonymisiert werden müssen. Solche Auflagen teilt der PDP dem anfragenden PEP mit, worauf der PEP die erforderlichen Maßnahmen durchführt, ehe er die modifizierten Daten zur Verarbeitung freigibt.

Neben der Freigabeentscheidung und der Anordnung von Modifikationsauflagen kann der PDP auch noch weitere Aktionen anstoßen, die von einem Policy Execution Point (PXP) ausgeführt werden. Eine Datennutzungsrichtlinie kann etwa vorschreiben, für jeden Datenverarbeitungsversuch einen Log-Eintrag zu erstellen oder eine Benachrichtigung an den Betroffenen zu senden.

Die Richtlinie 1 auf Seite 24 zeigt eine exemplarische Datennutzungsrichtlinie, die abhängig davon, ob der Nutzer in seinen Einstellungen der Teilnahme am Gruppenbericht zugestimmt hat, die Verwendung der benötigten Teilnehmerdaten zu diesem Zweck freigibt unter der Maßgabe, dieses Datennutzungsereignis zu protokollieren.

Wie Richtlinie 1 beispielhaft illustriert, verwendet MYDATA für die Spezifikation von Datennutzungsrichtlinien ein XML-Format. Dieses Format eignet sich in der Regel jedoch nicht für Endanwender. Daher sieht das MYDATA-Rahmenwerk einen Policy Administration Point (PAP) vor, um Datennutzungsrichtlinien anwenderfreundlich zu erstellen. Der PAP ist eine Komponente, die dem Nutzer eine auf die jeweilige Nutzergruppe zugeschnittene, in der Regel grafische Schnittstelle bietet, um seine gewünschten Datennutzungsregeln auszudrücken.

Im einfachsten Fall besteht ein PAP lediglich aus einem Auswahlmenü, mit dem vorgefertigte natürlichsprachliche Richtlinien-Klauseln aktiviert oder deaktiviert werden können. Je nach Anwendungsfall und Nutzerexpertise kann ein PAP aber auch parametrisierbare Richtlinienvorlagen liefern, bis hin zu einem freien Zugriff auf den vollständigen Sprachumfang der XML-Richtliniensprache des MYDATA-Frameworks.

Für den WearPrivate-Kontext – d.h. die Erfassung von Wearable-Daten am Arbeitsplatz – war vorgesehen, die Datennutzung mittels des persönlichen Mobilgeräts der Nutzer zu konfigurieren. Daher wurde der PAP in die Mobil-App integriert. Da die App den Nutzer während der Arbeit nicht zu sehr ablenken darf und da voraussichtlich nur wenige Nutzer über besondere IT- oder Datenschutzkenntnisse verfügen, sollte der PAP eine möglichst einfache, leicht zu bedienende Benutzeroberfläche bereitstellen. Die WearPrivate-App beschränkt sich daher im Wesentlichen auf einfache JA/NEIN-Entscheidungen, Auswahlen oder die Angabe von Grenzwerten (z. B. »Datenerfassung nur zwischen 8:00 und 17:00 Uhr«), die mit wenigen Klicks konfigurierbar sind und deren Bedeutung unmittelbar einsichtig ist.

Richtlinie 1 Datennutzung für Gruppenbericht einschränken und protokollieren

```
<policy id='urn:policy:wearprivate:cloud-policy'
        xmlns='http://www.mydata-control.de/4.0/mydataLanguage'
        xmlns:parameter="http://www.mydata-control.de/4.0/parameter"
        xmlns:event="http://www.mydata-control.de/4.0/event"
        xmlns:pip="http://www.mydata-control.de/4.0/pip">
  <mechanism event='urn:action:wearprivate:analytics-svc-uses-data-to-generate-grp-report'>
    <if>
      <pip:boolean method="urn:info:wearprivate:readUserSetting" default="false">
        <parameter:string name="userId">
          <event:string eventParameter="userId" default=""/>
        </parameter:string>
        <parameter:string name="setting"
value="$.analyticsServiceSettings.contributeDataToGroupReport"/>
      </pip:boolean>
      <then>
        <allow/>
        <execute action='urn:action:wearprivate:logEvent'>
          <parameter:string name='userId'>
            <event:string eventParameter="userId" default=""/>
          </parameter:string>
          <parameter:string name='eventType' value="analytics-svc-uses-data-to-generate-grp-
report"/>
          <parameter:string name='entryTitle' value="Teilnahme Gruppenbericht"/>
          <parameter:string name='entryText' value="Der Analysedienst hat Daten für den
Gruppenbericht verwendet."/>
        </execute>
      </then>
    </if>
    <else>
      <inhibit/>
    </else>
  </mechanism>
</policy>
```

Von seiner App aus steuert der Nutzer alle relevanten Datenverarbeitungen. Dazu sind entlang der Verarbeitungskette an verschiedenen Stellen PEPs integriert, um dort über die Datenverarbeitungen zu wachen. Abbildung 18 zeigt die konzeptionelle, vollumfängliche Integration der MYDATA-Komponenten im Gesamtsystem. Gepunktete Linien bezeichnen Informationsflüsse. Hierbei kennzeichnen Linien mit der Farbe Magenta die Informationsflüsse der besonders schützenswerten Gesundheitsdaten des Arbeitnehmers, über die wir ihm Kontrolle ermöglichen möchten. Grüne Linien bezeichnen Informationsflüsse, die der Transparenz und Selbstbestimmung des Arbeitnehmers dienen.

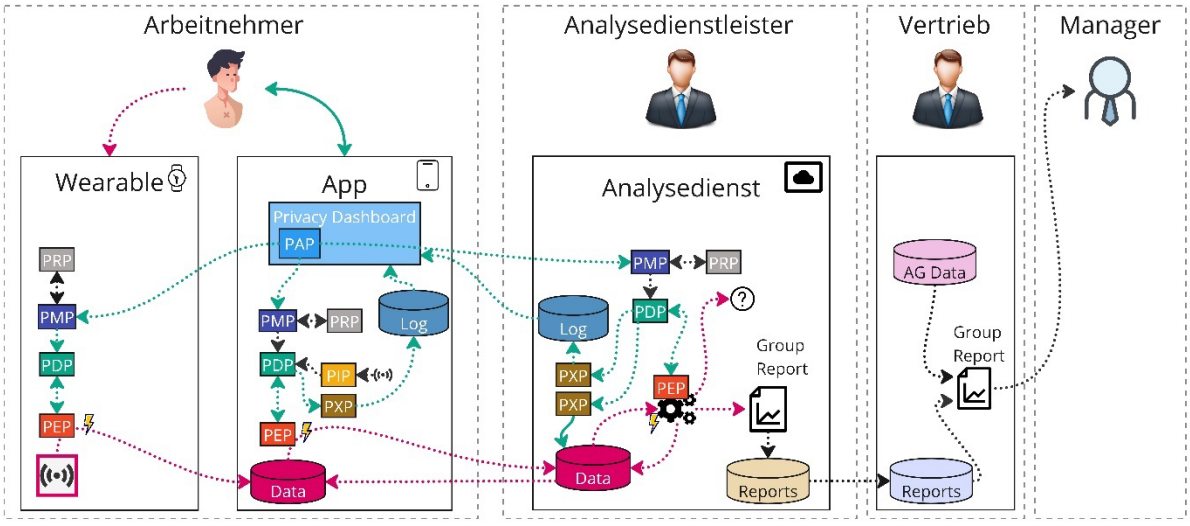


Abbildung 18 Konzeptionelle Integration und Positionierung der MYDATA-Komponenten im Gesamtsystem

Neben der Datennutzungskontrolle durch PEPs sieht das Konzept auch eine Protokollierung mittels PXPs vor. Zur Ermittlung von Kontextinformationen (z. B. Datum, Uhrzeit oder Geo-Lokation) stellt die App einen entsprechenden PIP bereit, der dazu auf die Sensorik des Mobilgeräts zurückgreift. Das Privacy-Dashboard der WearPrivate-App fungiert als PAP, mit dem der Nutzer seine Datennutzungspräferenzen auf einfache Weise ausdrücken kann.

Gemäß Abbildung 18 ist auch das Wearable in die MYDATA-Konfiguration mit einbezogen. Zu diesem Zweck müssen entsprechende MYDATA-Komponenten in der Wearable-Firmware verankert werden. Um einen solch tiefen Eingriff in die Wearable-Steuerung zu ermöglichen, sollten die Wearables für den Demonstrator ursprünglich von einem der Projektpartner bereitgestellt werden, der eigene Smart Shirts mit integrierter Sensorik produziert. Dieser Partner musste jedoch kurzfristig seine Projektteilnahme absagen. Das Projekt musste daher auf Wearables von Fremdherstellern zurückgreifen, bei denen Firmware-Eingriffe nicht mit vertretbarem Aufwand möglich waren.

Im weiteren Projektverlauf zeigte sich jedoch, dass im Wearable auf einen PEP verzichtet werden kann, sofern die Datenverbindung zwischen Wearable und App durch Authentisierung und Verschlüsselung hinreichend geschützt ist. In diesem Fall genügt es, die Datenverarbeitungen erst ab der App zu kontrollieren, da Dritte bis dahin ohnehin keinen Zugriff auf die dynamischen Wearable-Daten oder Einfluss auf deren Verarbeitung haben. Somit entfallen in Abbildung 18 die ursprünglich vorgesehenen MYDATA-Komponenten im Wearable. Diese konzeptionelle Vereinfachung begünstigt die Übertragbarkeit des WearPrivate-Konzepts, da beim Wearable-basierten Arbeits- und Gesundheitsschutz aus Kostengründen in der Regel wohl frei verkäufliche, unmodifizierte Standard-Wearables zum Einsatz kommen werden.

Der Einsatz des MYDATA-Rahmenwerks eröffnet den Entwicklern größere Flexibilität bei der Ausgestaltung der Datenschutzmechanismen. Nachdem die MYDATA-Komponenten entlang der Datenverarbeitungskette verankert sind, lassen sich die Datennutzungsrichtlinien mit vergleichsweise geringem Aufwand erweitern oder modifizieren, um auf geänderte Nutzeranforderungen oder neue Rahmenbedingungen zu reagieren. Äußern die Nutzer zusätzliche Daten- oder Kontext-bezogene Datenschutzpräferenzen und wünschen sich entsprechende Optionen zur Einschränkung der Datenverarbeitung, so lässt sich dies im Privacy-Dashboard schnell anpassen. Der Sprachumfang der MYDATA-Richtliniensprache bietet vielseitige Möglichkeiten, die gewünschten Präferenzen oder andere Vorgaben zu formalisieren und mittels Datennutzungsrichtlinien die Datenverarbeitung entsprechend zu reglementieren.

Eine vertiefende Darstellung der Konzepte zur Datennutzungskontrolle und des MYDATA-Rahmenwerks bietet der Ergebnisbericht D3.2 [18], Kapitel 3. Details zur konzeptionellen Integration von Datennutzungskontrolle in eine Sicherheits-Gesamtarchitektur für einen Wearable-basierten Arbeits- und Gesundheitsschutz beschreibt der Ergebnisbericht D3.1 [19], Kapitel 5. Einblicke in die prototypische Umsetzung der Datennutzungskontrolle im WearPrivate-Demonstrator vermittelt der Ergebnisbericht D3.3 [20], Kapitel 2.

4.3 Anonymisierungskonzepte

Im Verlauf des Projekts wurden vom Partner UdS verschiedene Konzepte erarbeitet, mit denen die erhobenen Daten durch Anonymisierung und Aggregation geschützt werden können. Ziel dieser Konzepte ist es, den Nutzer vor den negativen Folgen eines Verlusts seiner Daten – etwa durch ein Datenleck beim Analysedienstleister – zu schützen. Im Projekt wurden dazu konkret die Profildaten (Geburtsjahr, Geschlecht, Größe, Gewicht) und die Messdaten (Herzratenvariabilität, Herzrate, Beschleunigung) betrachtet. Die erarbeiteten Varianten sind in Abbildung 19 zu sehen.

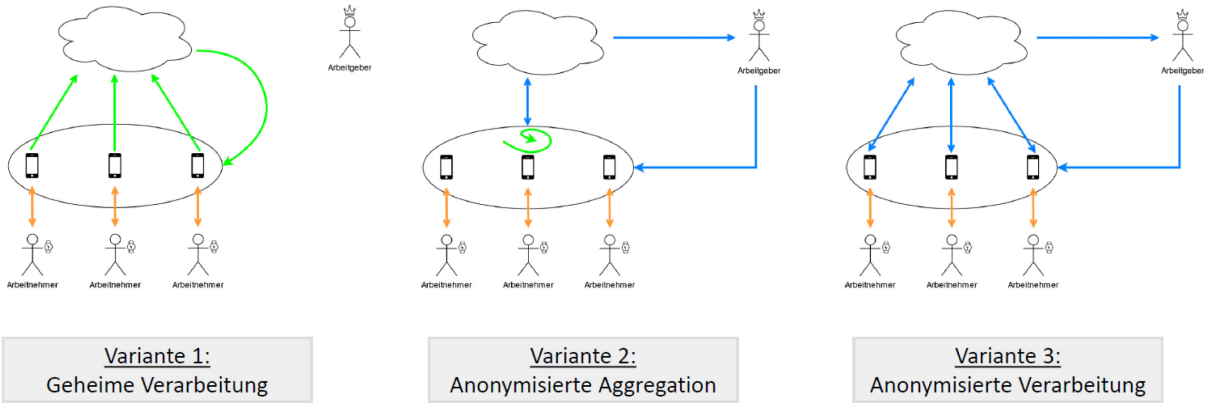


Abbildung 19 Schutzvarianten mithilfe von Anonymisierung und Aggregation

In den Abbildungen befinden sich am unteren Rand die Arbeitnehmer mit ihren Wearables (hier: Smartwatches), deren Daten stets von den Wearables an ihre Smartphones versendet werden. Die Wolke am oberen Rand stellt die Verarbeitungseinheit des Analysedienstes dar (oftmals umgesetzt als ein Cloud-Dienst) und am oberen rechten Rand befindet sich der Arbeitgeber.

Die erste Variante (links) sieht vor, dass die Daten der Arbeitnehmer geheim an den Analysedienst versendet werden und dort auch geheim verarbeitet werden. Dabei ist eine gemeinsame Auswertung der Daten aller Arbeitnehmer möglich, jedoch keine Einzelauswertungen für jeden Arbeitnehmer. Die Ergebnisse dieser Analyse kann der Analysedienst dann der Gruppe mitteilen, ohne selbst jemals die Rohdaten gesehen zu haben oder auch die Ergebnisse der Berechnung zu kennen. Umsetzbar ist dies beispielsweise mithilfe von (Secure) Multiparty-Protokollen oder homomorpher Verschlüsselung. Nachteilig ist hier jedoch, dass die Arbeitnehmer kein individuelles Feedback erhalten und auch der Arbeitgeber in schwierigen Situationen nicht eingreifen kann, sofern sich die Gruppe nicht selbst offenbart. Zudem lassen die möglichen Umsetzungsverfahren nur sehr stark begrenzte Analysen zu.

In der zweiten Variante (Mitte) werden die Daten der Arbeitnehmer in der Gruppe selbst aggregiert (grüner Pfeil) und dann an den Analysedienst versendet. Dieser kann nun die aggregierten Daten einsehen und komplexere Analysen durchführen. Der Analysedienst kann dann die Ergebnisse seiner Datenauswertung sowohl dem Arbeitgeber als auch der Gruppe mitteilen. Für eine Umsetzung können (Secure) Multiparty-Protokolle oder auch Slice-Mix-Aggregate-Verfahren genutzt werden. In dieser Variante können nun komplexe Analysen durchgeführt werden und auch der Arbeitgeber kann schwierige Situationen eigenständig erkennen und diesen entgegenwirken. Die Rohdaten bleiben jedoch stets beim Arbeitnehmer und beim Analysedienst. Arbeitgeber erhalten nur aggregierte Informationen über die gesamte Gruppe, jedoch keine Einsicht in individuelle Rohdaten. Individuelles Feedback für die einzelnen Arbeitnehmer ist daher nicht möglich.

Variante 3 (rechts) ermöglicht hingegen auch individuelles Feedback. Die Daten werden auf den Geräten der Arbeitnehmer anonymisiert und einzeln an den Analysedienst versendet. Dieser kann nun die Analysen auf den anonymisierten Daten durchführen und den Arbeitnehmern individuelle Rückmeldung geben sowie eine aggregierte Version der Einzelergebnisse an den Arbeitgeber weiterleiten. Diese Variante könnte mit Anonymisierungskonzepten wie k-Anonymität oder Differential Privacy umgesetzt werden. Aufgrund der Möglichkeit, einzelne Mitarbeiter auf problematische Messwerte hinzuweisen, hat sich das WearPrivate-Projekt auf diese Schutzvariante fokussiert.

Eine eingehende Darstellung der verschiedenen Anonymisierungsvarianten und ihrer jeweiligen Vorzüge und Nachteile findet sich im Ergebnisbericht D3.2 [18]. Nähere Einzelheiten zu Differential

Privacy und deren Anwendung in WearPrivate zur Datenanonymisierung beschreibt der Ergebnisbericht D6.1 [20].

Konkret wurde im Projekt ein Anonymisierungsmechanismus konzipiert und erprobt, der Differential Privacy (DP) nutzt, um die Urheber von Vitaldaten vor eine Identifizierung zu schützen. Dazu wurden die mit Wearables gemessenen Herzratendaten mittels DP-Techniken verfremdet, so dass sie nicht mehr eindeutig einer Person zuzuordnen sind, zu der man personenbeziehbare Vergleichsmessungen kennt.

Zur Realisierung wurde die Diffprivlib von IBM [22] verwendet. Diese Bibliothek ermöglicht mittels eines Parameters ε die Einstellung, wie stark die Daten verfremdet werden sollen. Ein kleines ε bietet dabei hohen Schutz, während ein großes ε die Daten nur wenig verfremdet und daher nur geringen Schutz vor einer Personenzuschreibung der Wearable-Daten bietet. Im Projekt untersuchten die Verbundpartner, wie stark eine Verfremdung sein muss, um eine Personenidentifizierung signifikant zu erschweren, und wie stark die Wearable-Daten maximal verfremdet werden dürfen, um noch korrekte Befunde daraus ableiten zu können. Näheres zu diesen Sensitivitätsanalysen findet sich in Abschnitt 6.1.

4.4 Darstellungskonzepte für den Gruppenbericht

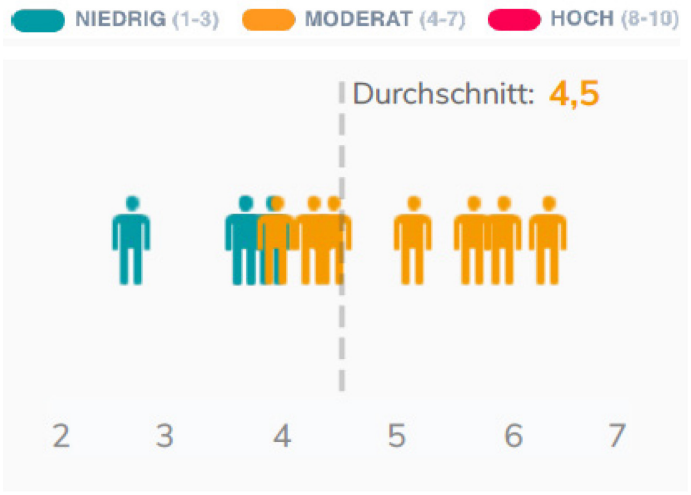
Ziel unseres Demonstrator-Anwendungsfall ist neben einer individuellen Belastungsrückmeldung an die Messprogramm-Teilnehmer in Echtzeit auch die Erstellung von Gruppenberichten für das Gesundheitsmanagement des Arbeitgebers. Während die individuellen Rückmeldungen nur dem jeweiligen Teilnehmer selbst zugänglich gemacht werden, ist der Gruppenbericht allen betroffenen Mitgliedern der jeweiligen Gruppe zugänglich sowie dem Arbeitgeber. Daher müssen die im Gruppenbericht vermittelten Informationen besonders penibel den Datenschutz der Gruppenmitglieder berücksichtigen.

Als grundlegende Datenschutzmaßnahme dürfen solche Gruppenauswertung nur erstellt werden, wenn eine vorgegebene Gruppen-Mindestgröße erreicht wird (typischerweise mindestens 10 Individuen). Finden sich zu wenige Gruppenmitglieder, die ihre persönlichen Befunddaten für eine Gruppenauswertung bereitstellen, so verweigert der Analysedienst für die betreffende Gruppe den Gruppenbericht, weil sich die Gruppendaten als allzu verräterisch für die Individualbefunde erweisen könnten. Dies schützt die Gruppenmitglieder davor, dass der Arbeitgeber die aggregierten Gruppenwerte auf einzelne Personen herunterbricht.

Eine solche Mindestgruppengröße bietet recht guten individuellen Datenschutz, soweit es verdichtete Mittelwerte betrifft und die individuellen Befunde hinreichend streuen. Soll im Gruppenbericht aber auch die Streuung der Werte veranschaulicht werden, kann dies bei größeren Gruppen die Privatsphäre gefährden. Abbildung 20 zeigt einen solchen Fall.

Im Beispiel (a) wird die Streuung durch eine Skala dargestellt, auf der die Messwerte der einzelnen Individuen jeweils durch Personensymbole verortet sind. Stechen in einer solchen Darstellung einzelne Individuen durch besonders hohe oder besonders niedrige Befundwerte heraus, so lassen sich deren Messwerte mitunter recht gut einzelnen Belegschaftsmitgliedern zuordnen: *»Die besonders niedrig belastete Person am linken Skalenende ist mit hoher Wahrscheinlichkeit der Hobby-Rennradfahrer, der sich bei seiner letzten Alpenüberquerung über seine geringe Durchschnittsgeschwindigkeit von nur 26 km/h geärgert hat; die Person am echten Ende der Belastungsskala ist am ehesten der 63-jährige Mitarbeiter, der wegen Herzbeschwerden demnächst in den vorgezogenen Ruhestand gehen wird.«*

(a)



(b)

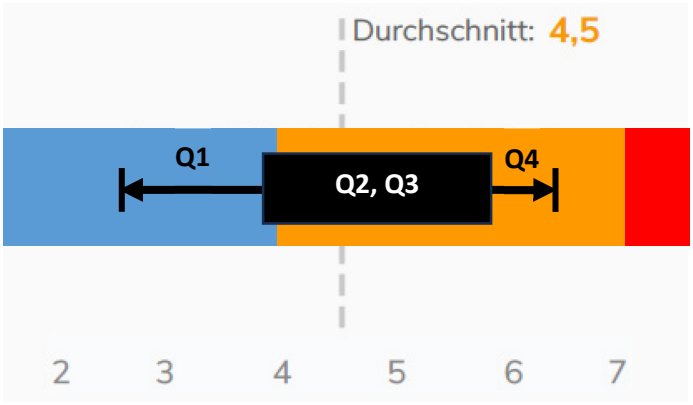


Abbildung 20 (a) Konventionelle, wenig datenschutzfreundliche Gruppenübersicht:
Obwohl die Gruppenmitglieder anonymisiert sind, stechen einzelne Individuen hervor. Eine Führungskraft, die mit der Gruppe und ihrer Zusammensetzung vertraut ist, könnte die gemessenen Werte für diese »Ausreißer« aufgrund solchen Hintergrundwissens mit guter Treffsicherheit bestimmten Personen zuordnen.

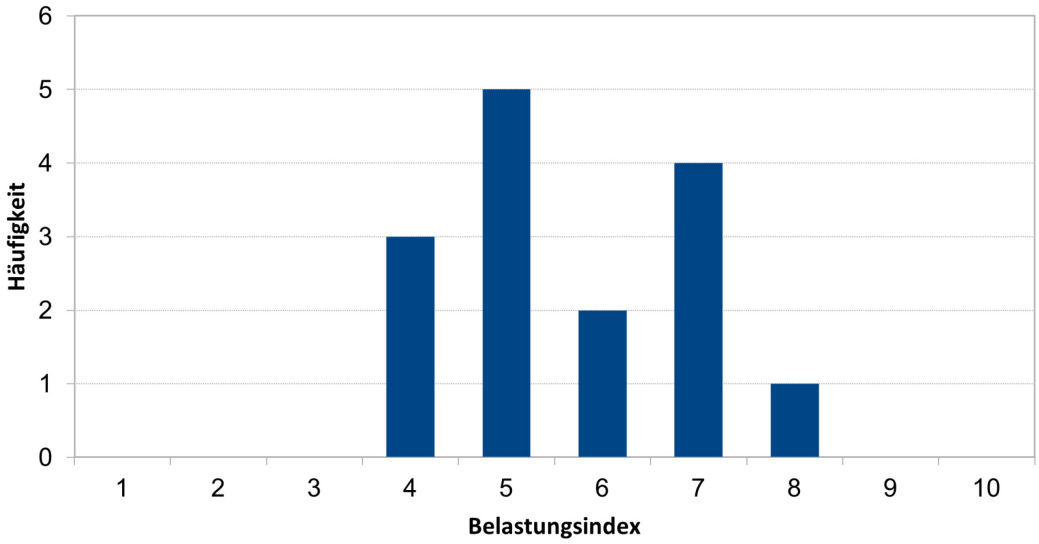
(b) Datenschutzfreundlichere Verschleierung der Individuen:
In dieser Variante sieht der Gesundheitsmanager die Spannweite der Messwerte, kann aber keine Individuen oder Individuen-Anzahlen ablesen. Der Box-Plot zeigt die Quartile der Messwertverteilung an: Q1 – unterste 25% der Messwerte; (Q2, Q3) – mittlere 50% der Messwerte; Q4 – oberste 25% der Messwerte.

Um solche Zusammenhänge zum Schutz der Individuen besser zu verschleiern, sollten die genauen Betroffenenzahlen besser nicht offengelegt werden und es sollte auch unkenntlich bleiben, ob die ermittelten Minima und Maxima durch Ausreißer verursacht wurden oder durch mehrere Individuen mit ganz ähnlichen Befundwerten. Dies lässt sich mit einem Box-Plot erreichen, wie Abbildung 20 (b) illustriert. Die Darstellung zeigt neben der Spannweite der Befundwerte auch die die Quartile Q1 (25 % niedrigste Werte), Q2 und Q3 (mittlere 50% der Messwerte um den Median) und Q4 (25% der höchsten Werte), um annähernd ein Gefühl für die Verteilung der individuellen Befunde zu vermitteln.

Eine gewisse Streuung der individuell gemessenen Werte ist zu erwarten, da physische und mentale Belastungen von vielen verschiedenen Faktoren abhängt – zum Beispiel allgemeiner körperlicher Konstitution, Gesundheitszustand, Trainingszustand, Tätigkeitsprofil, Schlafgewohnheiten oder seelischer Ausgeglichenheit. Unter der Annahme, dass sich die oben genannten zufälligen Faktoren in ihrer Wirkung auf die persönliche Belastung addieren, folgt nach dem Zentralen Grenzwertsatz der Wahrscheinlichkeitsrechnung, dass die Belastungsmessungen annähernd normalverteilt sein sollten. Daher sollte ein Gesundheitsmanager die genaue Lage einzelner Messwerte nicht überbewerten, sondern eher auf die Gesamtverteilung schauen.

Eine mögliche Vorgehensweise ist es daher, die individuellen Belastungswerte durch eine Normalverteilung zu repräsentieren, deren Mittelwert und Standardabweichung identisch mit den entsprechenden Größen der diskreten Verteilung ist. Abbildung 21 zeigt diesen Modellierungsansatz.

(a)



(b)

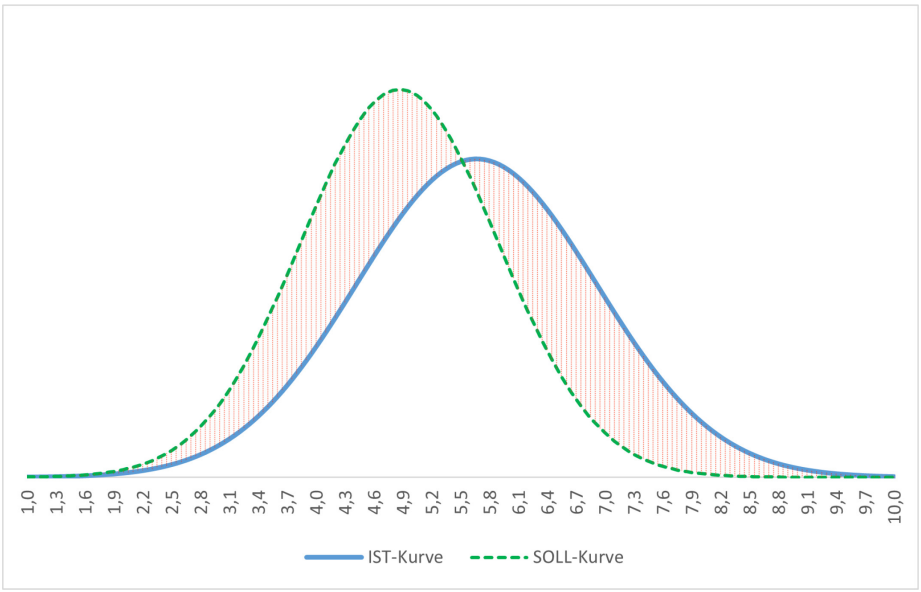


Abbildung 21 (a) Diskrete Häufigkeiten einzelner Messwerte:
Bei einer Darstellung der Häufigkeiten können Individuen – insbesondere Ausreißer – unter Umständen leicht identifiziert werden, wenn man mit den Mitgliedern der vermessenen Gruppe gut vertraut ist.

(b) Datenschutzfreundlichere Alternative: Umwandlung in eine Normalverteilung
Die diskreten Messwerte gemäß (a) werden durch eine Normalverteilung mit dem gleichen Mittelwert und der gleichen Standardabweichung repräsentiert. Der Gesundheitsmanager beurteilt dann nur noch, inwieweit die so erhaltende Normalverteilung (blaue Kurve) einer vorgegebenen idealtypischen Soll-Verteilung (grüne Kurve) entspricht. Im Beispiel ergibt sich ein zu hoher Mittelwert gegenüber einem idealtypischen Befund.

Im Beispiel wurde die diskrete Häufigkeitsverteilung der Belastungsindizes einer 15-köpfigen Gruppe mit einem Mittelwert von 5,8 und einer Standardabweichung von etwa 1,56 (Variante a) in eine entsprechende Normalverteilung umgewandelt (Variante b). Zusätzlich wurde in das Modell (b) noch eine zuvor auf medizinischer Basis bestimmte, (fiktive) idealtypische Soll-Kurve eingezeichnet. Um zu prüfen, ob die Gruppenbelastung dem gewünschten Sollwert entspricht, genügt es nun, die

Überdeckung von Ist- und Soll-Kurve zu beurteilen. Dabei kommt es auf die genauen Zahlenwerte der Wahrscheinlichkeitsverteilung gar nicht an, weil beide Kurven im gleichen Maßstab gemessen werden. Deshalb wurde in Abbildung 21 (b) auf eine Beschriftung der *y*-Achse verzichtet.

Im Vergleich zur diskreten Verteilung gemäß Abbildung 21 (a) oder auch der Box-Plot-Darstellung in Abbildung 20 (b) verwischt die Darstellung in Abbildung 21 (b) die individuellen Messwerte erheblich besser und wahrt damit eher die Privatsphäre der vermessenen Gruppenmitglieder, indem sie die genauen Zahlenverhältnisse verschleiert, aber dennoch die Charakteristika der Gruppe recht gut einfängt.

Wenn die Ist-Kurve gegenüber der Soll-Kurve nach links oder nach rechts verschoben ist, so deutet dies auf eine Unterforderung beziehungsweise Überforderung der Gruppe hin. Sofern die Ist-Kurve wesentlich breiter als die Soll-Kurve ist, so zeigt dies eine sehr inhomogene Belastung innerhalb der Gruppe an. Da zu erwarten ist, dass sich mit zunehmender Gruppengröße die Messwerte immer besser einer Normalverteilung annähern, bietet die vorgeschlagene Befunddarstellung somit einen vielversprechenden Ansatz – zumindest für die Beurteilung größerer Arbeitsteams.

5 Interaktionskonzepte für Transparenz und Selbstbestimmung

Dieses Kapitel beschreibt die in WearPrivate entwickelten Interaktionskonzepte, die darauf abzielen, die informationelle Selbstbestimmung der Nutzer von Wearables zu stärken und eine transparente und anwenderfreundliche Datennutzung zu gewährleisten.

5.1 Anonyme Registrierung

Wie in Abschnitt 4.1 bereits erläutert wurde, beruht der Daten auf einer anonymen Registrierung mittels Teilnehmertickets, die nicht personengebunden sind (vgl. Abbildung 15 auf Seite 20). Damit signalisiert die Anwendung gleich bei der Inbetriebnahme, dass kein Personenbezug beabsichtigt ist.

Dementsprechend sieht unser Interaktionskonzept eine anonyme Registrierung mittels Teilnahmecodes vor. Diese Codes sind fälschungssichere digitale Token, die vom Dienstleister erstellt und vom Arbeitgeber zufällig an die Messprogramm-Teilnehmer ausgegeben werden. Das können etwa QR-Codes sein, die der Teilnehmer zufällig aus einer Lostrommel zieht[3] und unbeobachtet mit seiner App einscannt. Die Wirkungsweise eines Teilnahmecodes entspricht der einer konventionellen Eintrittskarte. Der Teilnehmer weist damit nach, dass sein Arbeitgeber für den Einlösenden des Codes die erforderliche Teilnahmegebühr entrichtet hat. Bei der Registrierung vergibt der Dienst eine anonyme Teilnehmer-ID als Pseudonym für den Nutzer, unter der alle Stamm- und Vitaldaten zu dieser Person gesammelt und die abgeleiteten Analyseergebnisse abgelegt werden. Soweit der Teilnehmer seine ID nicht gegenüber Kollegen, dem Arbeitgeber oder Dritten offenbart, lassen sich seine vom Dienst verwalteten Daten nicht ohne Weiteres[4] zu seiner Person zurückverfolgen.

Bei der Erstbenutzung des Teilnahmecodes wählt der Nutzer ein persönliches, nur ihm bekanntes Passwort, mit dem er sich danach als der rechtmäßige Inhaber seiner Teilnehmer-ID ausweisen kann. Selbst bei Kenntnis der Teilnehmer-ID sind die Daten des Teilnehmers für Dritte nur einsehbar, wenn sie das Passwort des Teilnehmers kennen. Sobald die Registrierung erfolgreich abgeschlossen ist, wird der Code für weitere Registrierungen gesperrt, so wie eine Eintrittskarte nach dem Betreten des Veranstaltungsorts entwertet wird. Abbildung 22 zeigt den Ablauf der anonymen Registrierung.

Auf diese Weise kann der Analysedienst personenbezogene Datenanalysen bereitstellen und korrekt mit dem Arbeitgeber abrechnen, ohne Wissen darüber, um welche Personen es sich handelt. Wann immer sich ein Teilnehmer anonym beim Dienstleister anmeldet und sich per Passwort als rechtmäßiger Inhaber einer Teilnehmer-ID ausweist, kann die Person auf die Konfigurationseinstellungen, Daten und Analyseergebnisse des Nutzerkontos zugreifen, das für diese Teilnehmer-ID eingerichtet wurde. Die Person muss sich dabei jedoch nicht zu erkennen geben.

---

[3] Vor allem in kleineren Betrieben, wo alle Belegschaftsmitglieder an einem gemeinsamen Standort arbeiten, bietet es sich an, die Teilnahmecodes mit einem demonstrativ zufälligen Verfahren auszugeben, bei dem eine Zuordnung zwischen Code und Teilnehmer »offensichtlich« nicht möglich ist. Dies kann erheblich dazu beitragen, das Vertrauen der Betroffenen in den Schutz der Privatsphäre zu stärken.

[4] Manche Daten, die mittels Wearables erhoben werden können, sind charakteristisch für den Wearable-Träger. So sind zum Beispiel bestimmte Bewegungsmuster von Mensch zu Mensch so unterschiedlich, dass eine Wiedererkennung möglich ist, wenn man das Muster einer bekannten Person mit dem einer Reihe von Vergleichsproben aus einem anonymen Datenbestand vergleicht. Das Vitaldatenmuster fungiert hier als eindeutiger »Fingerabdruck« der betreffenden Person. Als Gegenmaßnahme gegen mögliche »Fingerprinting«-Angriffe sieht unser Konzept eine Datenverfremdung vor (siehe Abschnitt 5.7)

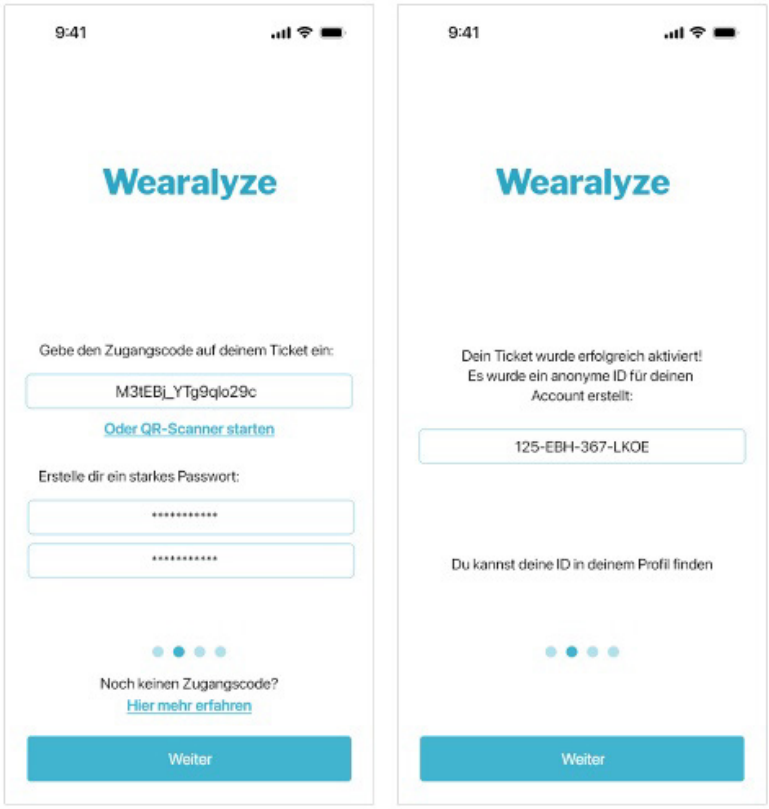


Abbildung 22 Registrierung mittels Teilnehmercode ohne Personenbezug: Im Folgenden kann der Nutzer auf den Dienst mit einer anonymen ID und seinem individuellen Passwort zugreifen, ohne seine wahre Identität zu offenbaren.

5.2 Onboarding

Onboarding bezeichnet den Prozess der schrittweisen Einführung neuer Anwender in die Nutzung einer App. Ziel des Onboardings ist es, die Nutzer mit den wichtigsten Funktionen und der Bedienung der App vertraut zu machen (Abbildung 23), um ihnen den Einstieg zu erleichtern und ein positives erstes Nutzungserlebnis zu schaffen.

Im Kontext datenschutzbezogener Interaktionskonzepte dient das Onboarding insbesondere dazu, neue Nutzer über die Verarbeitung ihrer Daten zu informieren und Vertrauen aufzubauen. Dies soll sicherstellen, dass Nutzer von Anfang an ein klares Verständnis davon haben, welche Daten gesammelt und wie diese von wem verarbeitet werden.

Das Onboarding soll zudem über die verschiedenen Datenschutzoptionen aufklären, damit die Nutzer bewusste Entscheidungen darüber treffen können, welche Daten sie teilen möchten. Dies stärkt die informationelle Selbstbestimmung, da die Anwender die Entscheidung über die Nutzung der App auf Basis von fundiertem Wissen treffen können.

Das Onboarding unterstützt das Recht auf Selbstbestimmung und Transparenz, indem alle notwendigen Einwilligungen eingeholt werden, bevor personenbezogene Daten verarbeitet werden. Die Nutzer können ihre Entscheidungen bewusst treffen und ihre Präferenzen individuell anzupassen.

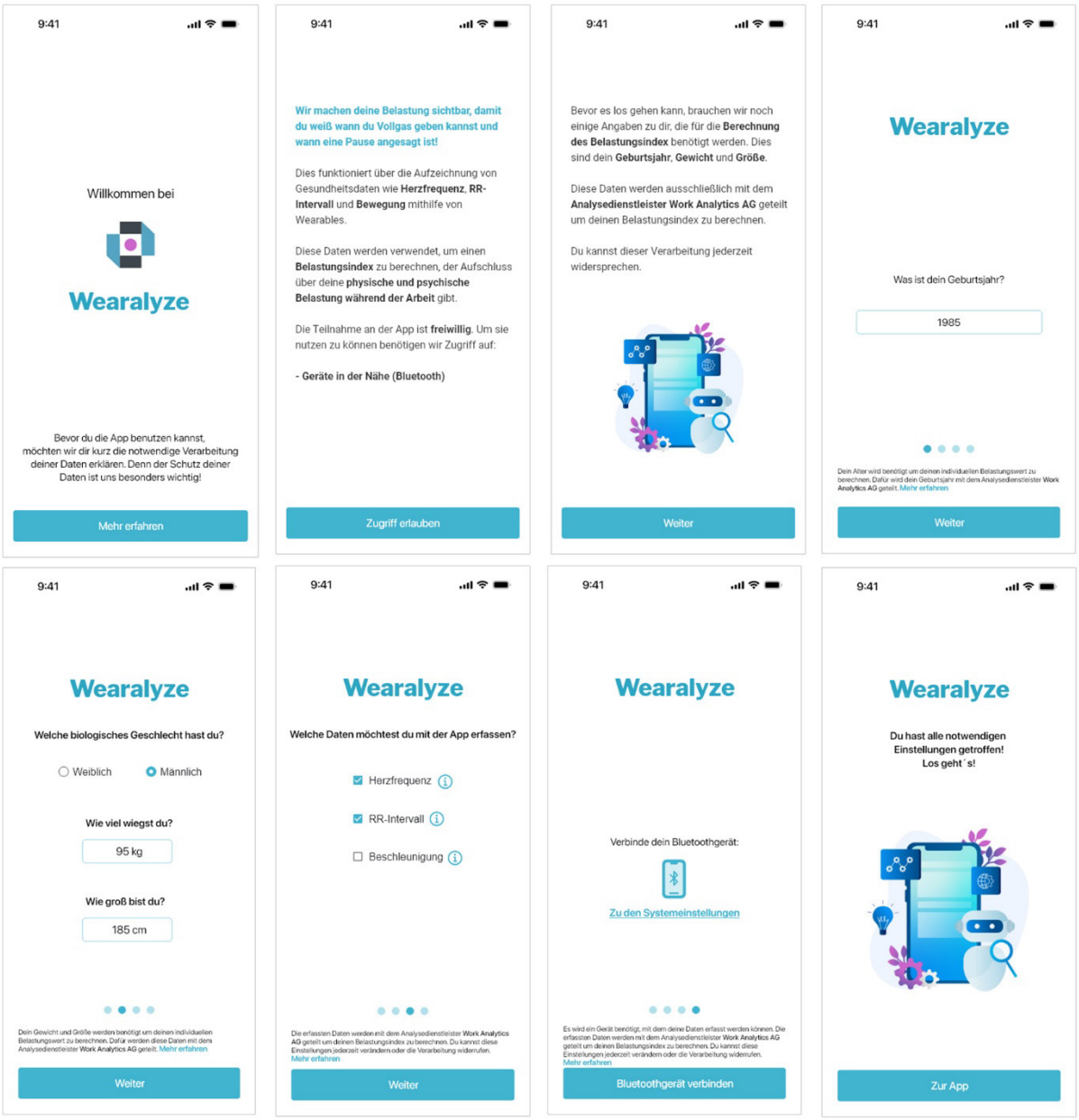


Abbildung 23 Übersicht über die Bildschirmansichten der Onboarding-Sequenz

5.3 Stammdatenerfassung

Neben aufklärenden Aspekten werden im Onboarding auch die benötigten Stammdaten (z. B. Alter, Geschlecht, Größe, Gewicht) abgefragt. Solche Angaben sind notwendig, um den Belastungsindex zu ermitteln, der von verschiedenen persönlichen Merkmalen abhängt. Um auch hier den Nutzern die größtmögliche Sicherheit in Bezug auf ihre Anonymität zu geben, werden die Daten nur in der Granularität abgefragt, die zur Berechnung wirklich benötigt wird. Dazu sind verschiedene Umsetzungen denkbar:

- Die Daten können exakt abgefragt werden.
- Die Daten können exakt abgefragt werden mit anschließender Möglichkeit der Verfremdung.
- Die Daten können in Bereichen (z.B. Alter 20 – 30 Jahre) abgefragt werden.

Die Auswahl des Verfahrens hängt vom jeweiligen Anwendungsfall ab. Insbesondere ist zu berücksichtigen, wie sensitiv die angestrebte Datenanalyse auf die Genauigkeit der verwendeten Rohdaten reagiert und welche Qualitätsansprüche die Nutzer an die Genauigkeit der Datenauswertung haben.

Im WearPrivate-Projekt haben wir uns für dafür entschieden, die Daten genau abzufragen, den Nutzern aber anzubieten, die Daten auf Wunsch vor der Übermittlung zu verfremden. Dieser Ansatz hat den Vorteil, dass die angebotenen Unschärfegrade von den Entwicklern der Anwendung so bemessen werden können, dass je nach Verfremdungsgrad vorgegebene Qualitätsstufen gewahrt bleiben. Würde man den Nutzern freistellen, die Genauigkeit ihrer Angaben nach eigenem Gutdünken zu wählen, wäre bei der Datenauswertung keine klare Abschätzung mehr möglich, wie belastbar die Analyseergebnisse auf der Basis ungenauer Rohdaten sind.[5]

Der Nachteil einer automatischen Verfremdung der exakten Angaben gegenüber einer absichtlich leicht verfälschten Dateneingabe durch den Nutzer ist allerdings, dass der Nutzer sich auf die ordnungsgemäße, ausreichende Datenverfremdung des Systems verlassen muss. Bei manueller Verfremdung ist hingegen sichergestellt, dass dem System zu keiner Zeit die exakten Angaben zur Person zur Verfügung stehen und diese somit auch nicht missbraucht werden können. Das Onboarding-Verfahren muss hier um das Vertrauen der Nutzer werben.

Der mögliche Grad einer Datenverfremdung hängt stark von dem jeweiligen Stammdatenattribut und vom Typ der Analysen ab, in die dieses Attribut einfließen soll. Manche Auswertungen reagieren sensibel auf geänderte Stammdaten, während andere in einem weiten Toleranzbereich stabile Ergebnisse liefern.

5.4 Datenschutz-Profil

Das Datenschutzprofil ist ein zentrales Interaktionskonzept, das den Nutzern eine transparente Übersicht über die Verarbeitung ihrer Daten bietet. Die übersichtliche Darstellung der wesentlichen Informationen und Einstellungsoptionen ermöglicht ihnen, ihre Datenschutz- und Datennutzungseinstellungen effektiv zu überwachen und zu steuern.

Die erfassten Daten, die Zwecke der Datennutzung sowie die aktuellen Einstellungen zur Datenverfremdung und Analysequalität werden als Kacheln übersichtlich dargestellt (Abbildung 24). So können die Nutzer auf einen Blick zu erkennen, ob die bestehenden Einstellungen ihren persönlichen Präferenzen entsprechen und ob sie gegebenenfalls Anpassungen vornehmen sollten.

Ein wichtiger Aspekt des Datenschutzprofils ist die Transparenz. Nutzer können sich jederzeit über die Verarbeitung ihrer Daten und die damit verbundenen Einstellungen informieren. Dies soll gewährleisten, dass die Datennutzung stets den tatsächlichen Wünschen des Nutzers entspricht. Das Dashboard fördert zudem die Selbstbestimmung, da die Nutzer ihre Datenschutzpräferenzen jederzeit anpassen können und somit die Kontrolle über ihre persönlichen Daten behalten.

[5] Will man dem Nutzer freistellen, bei der Angabe seiner Stammdaten ein wenig zu flunkern, so sollte die App zumindest darüber informieren, in welchem Ausmaß die Angabe verfälscht sein darf, um eine gegebene Qualitätsstufe zu garantieren. Da die Genauigkeitstoleranz je nach Wertebereich schwanken kann, erreicht dieser Ansatz schnell seine Grenzen (»Wenn du weniger als 60 kg wiegst, solltest du bei der Angabe deines Körpergewichts um höchstens -7 bis +5 Prozent vom wahren Wert abweichen, bei einem höheren Gewicht um höchstens +/- 4 Prozent.«). Dies gilt insbesondere, wenn neben Gewicht, Körpergröße, Alter und Geschlecht noch weitere Stammdaten benötigt werden, jede mit unterschiedlichen Genauigkeitsanforderungen.

Abbildung 24 Grundansicht der Datenprofileinstellungen mit einer Übersicht über die wichtigsten Konfigurationseinstellungen: Von hier aus kann der Nutzer in die verschiedenen Aspekte verzweigen, die Transparenz und informationelle Selbstbestimmung betreffen, um die Einstellungen seinen Präferenzen anzupassen.

In der Hauptansicht des Dashboards sind weitere Unterbereiche wie Gruppenberichte, Aktivitätenprotokoll und Benachrichtigungseinstellungen zu finden, wodurch die Seite zum Ausgangspunkt aller datenschutzrelevanten Interaktionen wird. Das Privacy-Dashboard ist somit ein zentrales Element zur benutzerzentrierten Gestaltung der Datenschutzfunktionen.

5.5 Vital- und Kontextdatenerfassung

Die Vital- und Kontextdatenerfassung betrifft die vom Wearable dynamisch erhobenen Messdaten. Hierzu zählen Vitaldaten wie beispielsweise die Herzfrequenz, das sogenannte RR-Intervall zur die Berechnung der Herzratenvariabilität oder Beschleunigungsdaten, aber gegebenenfalls auch Kontextinformationen wie zum Beispiel Standort, Temperatur, Luftfeuchte oder Lärmpegel.

Aus Sicht der Datensouveränität gibt es unterschiedliche Ansätze für die Handhabung der Datenerhebung (siehe Abbildung 25): Entweder können die Nutzer selbst entscheiden, welche Daten erfasst werden sollen, oder der Arbeitgeber legt die erforderliche Datenerhebungen verbindlich fest.[6]

[6] Die Zustimmung zu einer Vitaldatenerfassung am Arbeitsplatz muss immer freiwillig erfolgen. Allerdings kann der Arbeitgeber die freiwillige Teilnahme an dem Programm an die Bedingung knüpfen, dass sich die Teilnehmer zur Erhebung und Weiterverarbeitung bestimmter Messwerte bereiterklären, weil sonst die Ziele des Messprogramm nicht erreicht werden können. Es bleibt dann den Betroffenen überlassen, inwieweit sie bereit sind, persönliche Daten preiszugeben, um in den Genuss der Vorteile des Messprogramms zu kommen.

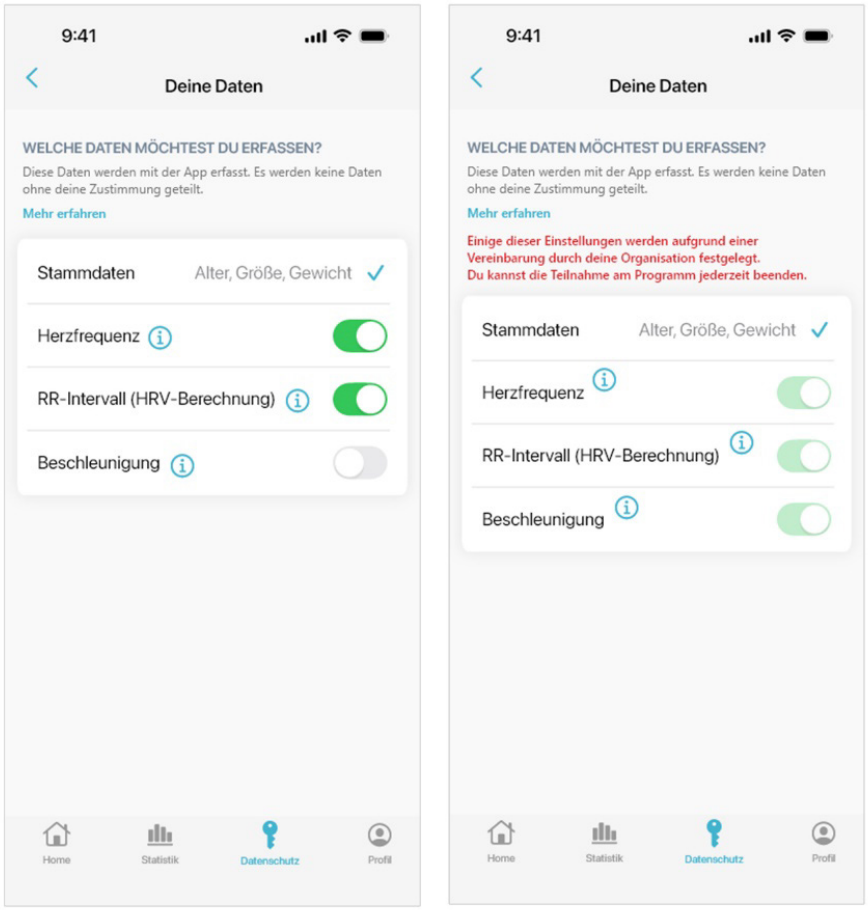


Abbildung 25 Links: Nutzer erhalten eine Übersicht über alle erfassten Rohdaten und können meist selbst bestimmen, welche Daten erfasst werden und welche nicht. Verweigert ein Nutzer die Zustimmung zur Erfassung bestimmter Daten, so weist die App auf mögliche Funktionsbeeinträchtigungen hin.

Rechts: Ist die Auswahl Arbeitgeber-seitig beschränkt und sind gewisse Einstellungen nicht änderbar, verweist die App auf die Freiwilligkeit der Teilnahme und die Möglichkeit, das Messprogramm zu verlassen.

Dürfen die Nutzer selbst auswählen, welche Daten erhoben werden, stärkt dies deren Selbstbestimmung. Sie können die Erfassung von Daten jederzeit deaktivieren, sofern sie keine Erhebung wünschen. Diese Flexibilität verschafft den Nutzern maximale Kontrolle über ihre Daten und ermöglicht es ihnen, eine individuelle Abwägung vorzunehmen.

Die Entscheidung, bestimmte Daten nicht zu erfassen, hat jedoch Auswirkungen auf die Funktionalität der App. Eine zu starke Einschränkung der Datenerhebung kann dazu führen, dass die Berechnung eines aussagekräftigen Belastungsindex nicht mehr möglich ist; der Nutzen der App geht so verloren. Deshalb ist es wichtig, die Nutzer zu informieren, inwieweit die vorgenommenen Einstellungen die Funktionalität der App beeinträchtigen.

Wenn der Arbeitgeber festlegt, welche Daten für die Nutzung der App (mindestens) erhoben werden müssen, haben Nutzer keine oder nur begrenzte Möglichkeiten, die Datenerhebung zu beeinflussen. Da diese Vorgabe den selbstbestimmten Umgang mit den eigenen Daten unter Umständen stark einschränkt, setzt das Interaktionskonzept dem eine transparente Kommunikation entgegen. Dazu liefert die App eine Erläuterung, warum die Einstellungsmöglichkeiten begrenzt sind, und weist noch einmal ausdrücklich darauf hin, dass die Teilnahme freiwillig ist: Ist ein Nutzer nicht bereit, sich auf die geforderte Datenerhebung einzulassen, kann er die Nutzung der App jederzeit beenden.

5.6 Kontrolle über Verarbeitung, Nutzung und Weitergabe der Daten

Datennutzungskontrolle umfasst die Erteilung von Datenzugriffs- und Datenauswertungsrechten sowie der Festlegung des Empfängerkreises, mit dem die Daten und daraus abgeleitete Befunde geteilt werden dürfen. Mittels der Funktionalität *Daten teilen* legt der Nutzer fest, für welche spezifischen Zwecke die Weitergabe der Daten zulässig ist (Abbildung 26).

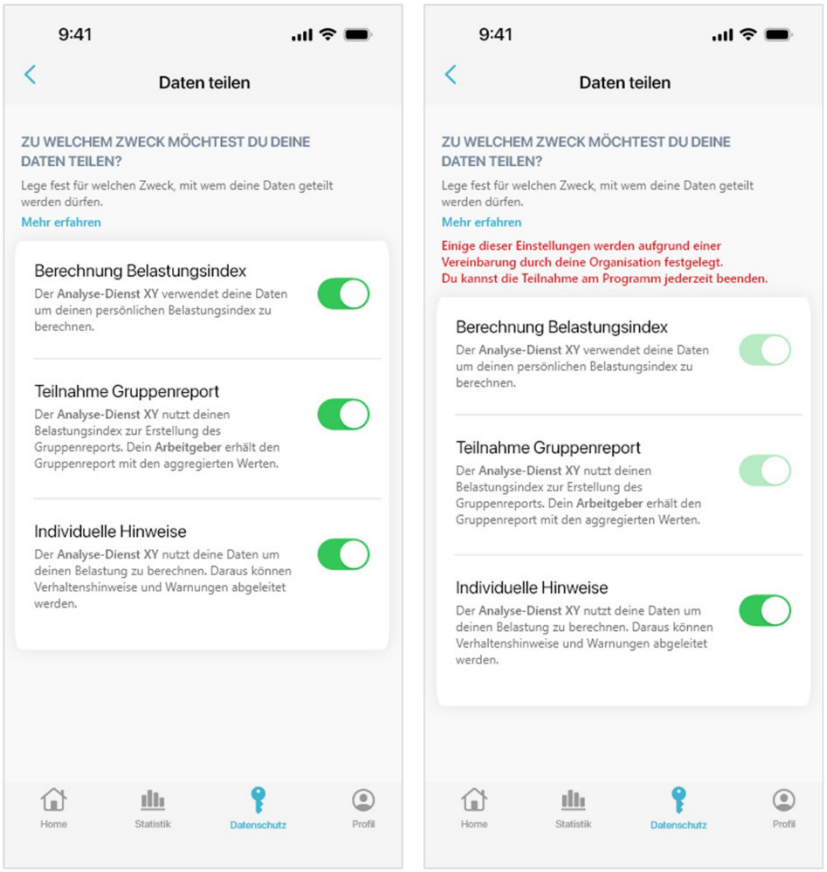


Abbildung 26 Wie bei der Datenerfassung erhalten die Nutzer auch bei der Datennutzung eine vollständige Übersicht über alle möglichen Verwendungszwecke. In der Regel können sie auch selbst bestimmen, welchen dieser Datennutzungen sie zustimmen wollen und welchen nicht. Hat der Arbeitgeber die Auswahlmöglichkeiten aus betrieblichen Gründen beschränkt, so weist die App auf diese Beschränkungen hin sowie auf die Möglichkeit, die freiwillige Teilnahme am Messprogramm jederzeit zu beenden.

In diesem Kontext werden alle verfügbaren Optionen aufgelistet, beispielsweise die Nutzung der Daten zur Berechnung des Belastungsindex, für die Teilnahme am Gruppenbericht, für den Erhalt individueller Hinweise sowie für weitere Verwendungsmöglichkeiten, etwa die freiwillige Datenspende an Forschungseinrichtungen. Jeder dieser Zwecke wird durch eine präzise Erläuterung ergänzt, wem der Zugriff bei Zustimmung zu welchem Zweck gestattet wird. Dies ermöglicht den Nutzern eine informierte Entscheidung, ob und in welchem Umfang sie die betreffenden Daten teilen möchten.

Analog zur Datenerfassung existieren auch in diesem Kontext mehrere Optionen zur Ausgestaltung der Wahlmöglichkeiten:

- Die Nutzer können die volle Kontrolle über die Weitergabe ihrer Daten erhalten und selbstbestimmt entscheiden, für welche Zwecke die Daten verwendet werden dürfen. Dies gewährleistet die größtmögliche Freiheit im Umgang mit den eigenen Daten. Es birgt jedoch für den Arbeitgeber das Risiko, dass sich beispielsweise nicht genügend Mitarbeiter für eine

Teilnahme am Gruppenbericht entscheiden. Daher verliert der Bericht an Aussagekraft oder kann sogar wegen zu geringer Teilnehmerzahl nicht datenschutzkonform erstellt werden.

- Alternativ kann der Arbeitgeber bestimmte Voreinstellungen treffen und damit festlegen, für welche Zwecke die Daten (mindestens) geteilt werden müssen. Ein Beispiel für eine solche Verpflichtung ist die Teilnahme der Mitarbeiter am Gruppenbericht, welcher Analysen zur Arbeitsbelastung für eine bestimmte Mitarbeitergruppe enthält. Da dies jedoch die Selbstbestimmung der Betroffenen einschränkt, wird auch hier eine transparente Kommunikation angestrebt. Den Nutzern wird dabei vermittelt, warum ihre Wahlmöglichkeit eingeschränkt ist und dass sie die Teilnahme am Messprogramm jederzeit beenden können, wenn sie damit nicht einverstanden sind.

Die erklärende Darstellung der jeweiligen Verwendungszwecke und der damit verbundenen Zugriffsrechte ermöglicht den Nutzern eine souveräne Entscheidung bezüglich ihres individuellen Datenschutzbedarfs.

5.7 Datenverfremdung

In unserem Anwendungsfall (vgl. Abschnitt 1.2) streben wir grundsätzlich an, die erfassten Vitaldaten ohne Personenbezug zu verarbeiten. Dazu dient insbesondere das anonyme Registrierungsverfahren (vgl. Abschnitt 5.1), das auf Personenbezüge wie die Angabe von Namen, Adressen oder Telefonnummern verzichtet. Stattdessen werden die Daten einer Person unter einer zufälligen, nutzerspezifischen Teilnehmer-ID verwaltet, also einem Pseudonym, dessen wahre Identität nur dem jeweiligen Nutzer selbst bekannt ist.

Ungeachtet dessen kann man jedoch die Anonymität der Daten nicht unter allen Umständen garantieren. Wenn etwa ein ambitionierter Hobbyradler in seiner Sportgruppe eine Aufzeichnung seiner Herzratenvariabilität in einer Chatgruppe im Internet veröffentlicht, dann besteht die Gefahr, dass ein Angreifer diese Aufzeichnung mit den im Messprogramm erfassten Vitaldaten abgleicht, um sie so wieder dem Chatgruppen-Mitglied zuzuordnen und damit deren Urheber zu ermitteln.

Das Risiko eines solchen Datenabgleichs besteht immer dann,

- wenn erhobene Messdaten sehr charakteristisch für die betreffende Person sind, so wie ein Fingerabdruck, der sich von Person zu Person eindeutig unterscheidet, und
- wenn zusätzlich Vergleichsdaten verfügbar sind, deren Personenbezug bekannt ist.

Um diesem Restrisiko vorzubeugen, sieht das Interaktionskonzept eine Option vor, die übermittelten Stamm- und Vitaldaten durch Verrauschen zu verfremden. Die Datenverfremdung dient dazu, den eindeutigen »Fingerabdruck« des Nutzers so zu verzerren, dass eine eindeutige Personenzuordnung selbst mit präzisen Vergleichsdaten aus anderen Quellen außerhalb des Messprogramms nicht mehr gelingt. Selbst wenn man die Bedrohung in einem konkreten Anwendungsfall als gering einschätzen mag, so dient die Datenverfremdung als vertrauensbildende Maßnahme, um möglichst viele Freiwillige für ein Messprogramm zu gewinnen.

Sowohl die Stammdaten als auch die dynamisch erhobenen Vitaldaten sind potenzielle Kandidaten für eine Datenverfremdung. Es gibt verschiedene Optionen, dem Nutzer Kontrolle über die Art und den Grad der Verfremdung zu ermöglichen. Dabei ist zu berücksichtigen, dass mit einer zunehmenden Datenverfremdung eine zunehmende Einbuße an Analysequalität verbunden ist.

Konkret bietet unser Interaktionskonzept den Nutzern drei Verfremdungsstufen zur Auswahl an. Je nach gewählter Stufe ergibt sich eine entsprechende, gegenläufige Qualität der Analysebefunde: Bei

schwacher Verfremdung erhält der Nutzer eine hohe Analysequalität; während starke Verfremdung eine niedrige Qualität der Befunde bedingt. Dies wird dem Nutzer in der App visuell zurückgespiegelt, wie in Abbildung 27 dargestellt.

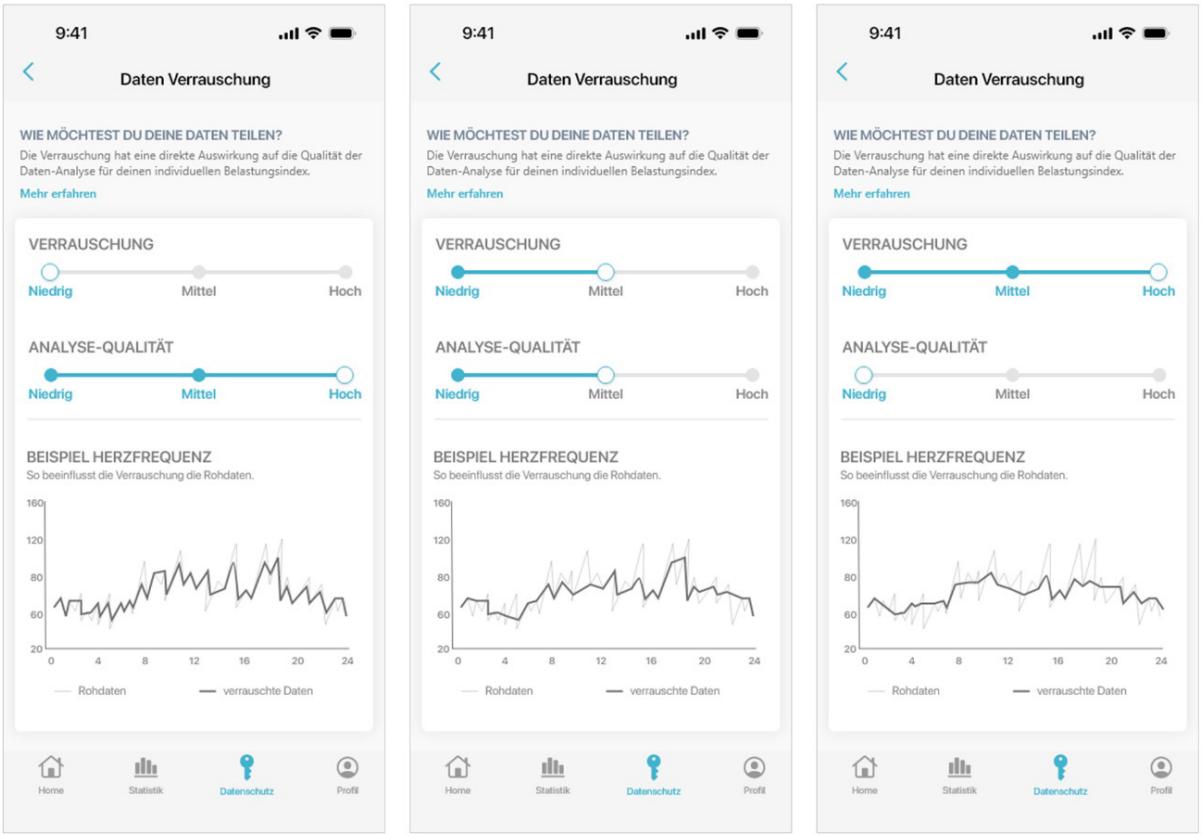


Abbildung 27 Bewusste Verfremdung der gemessenen Stamm- und Vitaldaten, um eine Identifizierung der Person durch einen Datenabgleich mit einer externen personenbezogenen Datenquelle zu erschweren: Da im Allgemeinen die Güte der Analyseergebnisse mit zunehmender Verfremdung der Daten sinkt, bietet die App den Nutzern die Auswahl zwischen drei verschiedenen Verfremdungsstufen und zeigt an, wie die getroffene Wahl die Qualität der Analysen beeinflusst.

Das Interaktionskonzept setzt voraus, dass vom Entwickler der Anwendung eine sinnvolle Abstufung gewählt wurde, die den Nutzen der App nicht ad absurdum führt. Um zu ergründen, wie stark die Nutzerdaten für einen vorgegebenen Privacy-Effekt verfremdet werden müssen, können die Entwickler zum Beispiel auf die in Abschnitt 6.1 beschriebenen Evaluationsverfahren zurückgreifen.

Die Datenverfremdung dient nicht nur einem verbesserten Datenschutz. Das Interaktionskonzept zielt außerdem darauf ab, die Einstiegshürde für datenschutzsensitive Nutzer zu senken. Betroffene, die sich um ihre Privatsphäre sorgen und einem Messprogramm am Arbeitsplatz skeptisch gegenüberstehen, lassen sich eher für eine Teilnahme gewinnen, wenn sie sich zunächst an das Belastungsmonitoring herantasten können, indem sie zu Beginn ihrer Teilnahme nur stark verfremdete Daten bereitstellen. Auch wenn dann die Analysequalität nur begrenzt ist, so lernen die Betroffenen mit der Zeit die Vorzüge des Messprogramms zu schätzen. Mit der Zeit fassen sie – so die Hoffnung – zunehmend Vertrauen in die Datenverarbeitung, so dass sie schließlich eine höherer Analysegenauigkeit anstreben und dafür bereit sind, ihre Stamm- und Vitaldaten in höherer Genauigkeit preiszugeben.

5.8 Zeit- und ortsabhängige Datenerfassung

Um in einem beruflichen Umfeld das Vertrauen der Mitarbeiter zu stärken und so ihre freiwillige Teilnahme an einem Messprogramm zu fördern, sollte die Anwendung sicherstellen, dass keine Daten außerhalb des Arbeitskontexts verarbeitet werden. Eine zeit- und ortsabhängige Datenerfassung knüpft die Erfassung von Vitaldaten an individuelle Vorgaben des Nutzers.

Bei der zeitabhängigen Datenerfassung kann der Nutzer in einem Tages- und Stundenraster festlegen, zu welchen Zeiten die App automatisiert Daten erfassen darf (Abbildung 28 links).

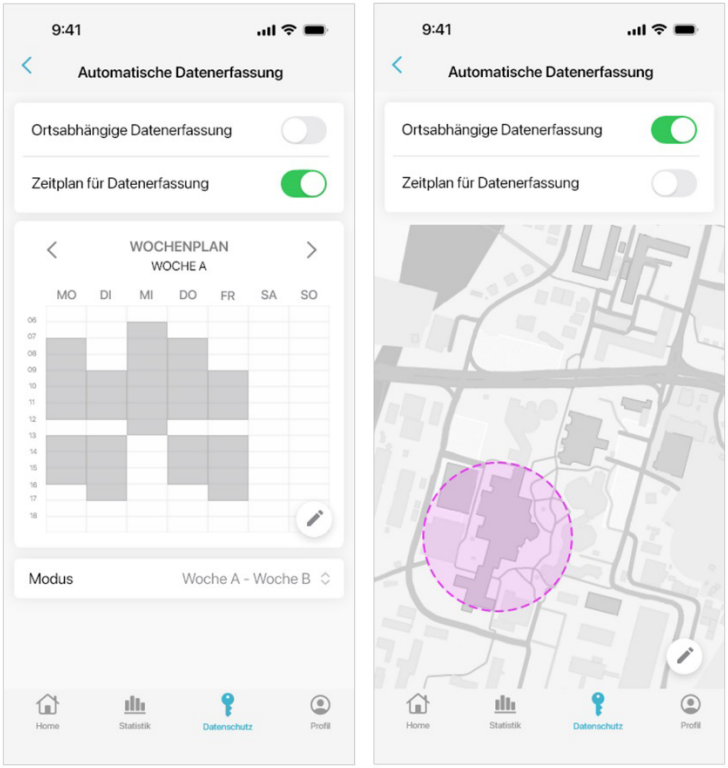


Abbildung 28 Links: Zeitbezogene Einschränkung der Vitaldatenerfassung durch einen individuellen Wochenplan. Rechts: Ortsbezogene Einschränken der Vitaldatenerfassung durch Geo-Fencing.

Die App erfasst die Vitaldaten dann ausschließlich in den vorgegebenen Zeitintervallen und verhindert so, dass die Datenerfassung unbeabsichtigt auch in der Freizeit fortgesetzt wird. Gleichzeitig entfällt das Risiko, das manuelle Starten der Erfassung bei Arbeitsbeginn zu vergessen. Ein solcher Automatismus ist besonders nützlich für den Einsatz von Wearables wie etwa Smart Watches, die kontinuierlich getragen werden, insbesondere auch in der Freizeit. Ist die Nutzung des Wearables hingegen an eine besondere Berufskleidung gebunden, ergibt sich das Arbeitszeitintervall oft schon durch den Kleiderwechsel.

Eine weitere Option ist die ortsabhängige Datenerfassung. Hierbei können Nutzer Orte auf einer Karte definieren, in deren Umkreis die Datenerfassung erfolgen darf (Abbildung 28 rechts). Betritt der Nutzer den Bereich, so startet die Datenerfassung automatisch. Verlässt der Nutzer den Bereich, wird die Datenerfassung automatisch pausiert. Diese Funktion bietet zusätzliche Kontrolle und schützt vor unbeabsichtigter Datenerfassung außerhalb des Arbeitsplatzes.

Die ortsabhängige Erfassung kann auf unterschiedliche Weise kontrolliert werden:

- Geo-Lokations-basiert: Die App kann den genauen (oder zumindest ungefähren) Standort des Nutzers ermitteln, etwa mittels Satelliten-Navigation (GNSS) oder anhand der aktuellen Funkzelle, in dem sich das Mobilgerät gerade befindet. Nachteilig ist, dass ein Satellitenempfang in geschlossenen Gebäuden nicht gewährleistet ist. Daher kann das Verlassen des Aufzeichnungsbereichs oft erst erkannt werden, wenn der Nutzer ins Freie tritt.
- Leitstrahl-basiert: Eine Alternative zur Geo-Lokations-Bestimmung sind Leitstrahlen, wie etwa WLANs oder Bluetooth-Beacons. Der Aufzeichnungsbereich umfasst dann alle Orte, die in der Reichweite dieser Funkquellen liegen. Sobald das Mobilgerät des Nutzers in Reichweite einer konfigurierten Quelle kommt, aktiviert es die Aufzeichnung der Wearable-Daten. Entfernt sich der Nutzer aus der Reichweite der Leitstrahl-Signale, wird die Aufzeichnung automatisch gestoppt. Ein solches Verfahren bietet sich für geschlossene Räume an. Nachteilig ist jedoch, dass die genaue Reichweite eines Leitstrahls mitunter schwer einzuschätzen ist und abhängig von äußeren Faktoren (z. B. Wetter, Störsignalen, baulichen Veränderungen) stärkeren Schwankungen unterliegen kann.

Abbildung 28 (rechts) zeigt, wie sich Erfassungsbeschränkungen auf Basis eines Satellitennavigationssignals einfach als Radius um einen Ortspunkt konfigurieren und anschaulich darstellen lassen.

Mittels Zeit- oder Ortsbeschränkung können Nutzer die Erfassung ihrer Daten flexibel kontrollieren und ihre Privatsphäre in ihrer Freizeit absichern. Je nach beruflicher Situation können die Vorteile des einen oder andere Konzepts überwiegen. Ändern sich zum Beispiel die Arbeitszeiten häufig oder weichen sie aufgrund von Urlaub oder Krankheit vom üblichen Tagesablauf ab, so muss der Nutzer bei der zeitbasierten Erfassung stetige Anpassungen in der App vornehmen. Ein häufiger Wechsel des Arbeitsorts würde dagegen die Nutzung der ortsbeschränkten Erfassung beeinträchtigen.

5.9 Event-Log

Das Event-Log ist ein weiteres Interaktionskonzept zur Erhöhung der Transparenz bei der Datenverarbeitung. Es dient als detailliertes Protokoll, das alle Ereignisse und Aktionen im Zusammenhang mit der Datenerfassung, -verarbeitung und -weitergabe dokumentiert. Diese Ereignisse werden in chronologischer Reihenfolge angezeigt, so dass der Nutzer einen vollständigen Überblick über alle datenschutzrelevanten Vorgänge erhält (Abbildung 29).

Anhand des Ereignisprotokolls können die Nutzer die Erfassung und Verarbeitung ihrer Vitaldaten – wie Puls, RR-Intervall oder Beschleunigungsdaten – jederzeit nachvollziehen. So wird klar ersichtlich, wann Daten erfasst, wie sie verarbeitet und an welche Stellen sie gegebenenfalls weitergeleitet wurden. Die lückenlose Nachvollziehbarkeit gewährleistet ein hohes Maß an Transparenz, was das Vertrauen in die Anwendung stärken soll.

Zudem beugt das Event-Log Missverständnissen oder Unsicherheiten in Bezug auf die persönlichen Datenschutzeinstellungen vor. Wenn der Effekt einer Konfigurationseinstellung sich im Event-Log nicht wie beabsichtigt niederschlägt, ist dies ein Warnzeichen für die Anwender: Gegebenenfalls fehlt noch eine wichtige Einstellung in der persönlichen Datenschutzkonfiguration oder die Wirkung einer Konfigurationsoption wurde falsch eingeschätzt. Dies können die Nutzer zum Anlass nehmen, ihre datenschutzrelevanten Einstellungen noch einmal genauer zu überprüfen und anzupassen.

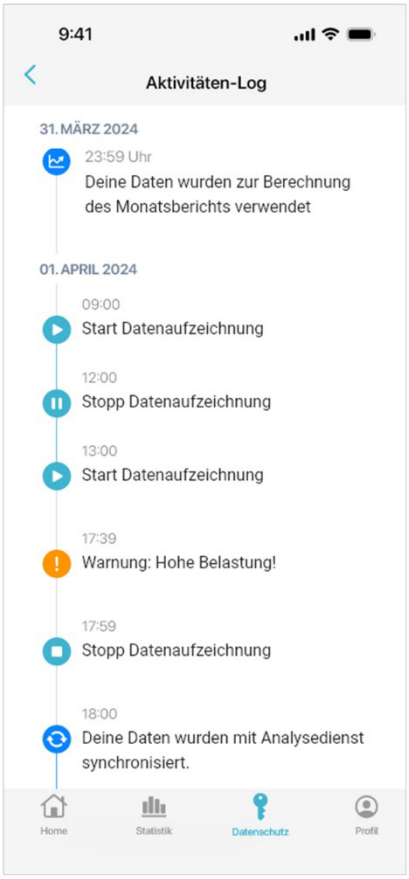


Abbildung 29 Event-Log: Die App erfasst alle Ereignisse, die den Datenschutz und die Privatsphäre betreffen, und zeigt sie in chronologischer Reihenfolge an. Die App-Nutzer können so die Erfassung, Verarbeitung und Weiterleitung ihrer persönlichen Daten nachverfolgen, um volle Transparenz über die Datennutzung zu erhalten.

5.10 Begrenzung der Speicherdauer

Eine vertrauensbildende Maßnahme, die zugleich die Angriffsfläche der erhobenen Daten reduziert, ist die Begrenzung der Speicherdauer von Wearable-Daten und daraus abgeleiteten Analyseergebnissen. Die Benutzer können selbst wählen, wie lange diese Daten auf dem Mobilgerät und in den Systemen des Analysedienstes gespeichert bleiben sollen.

Für ein persönliches, unmittelbares Vitaldaten-Feedback – z. B. die kontinuierliche Ermittlung eines Momentan-Belastungsindex – genügt es im Prinzip, die ermittelten Daten nur für wenige Minuten verfügbar zu halten.[7] Danach können die Roh- und Befunddaten gelöscht werden und sind damit nicht mehr angreifbar.

Sieht das Messprogramm am Arbeitsplatz jedoch einen wöchentlichen oder monatlichen Gruppenbericht vor, dann müssen die Daten der teilnehmenden Gruppenmitglieder mindestens über diesen Zeitraum aggregiert werden, ehe eine Löschung aus Datenschutzgründen erfolgen kann. Ein datenschutzfreundliches Berechnungskonzept sollte allerdings anstreben, die *individuellen* Daten der Gruppenmitglieder sofort zu aggregieren und danach nur die *aggregierten* Werte zu speichern, die

[7] Da der Belastungsindex von der persönlichen körperlichen und geistigen Disposition abhängt, werden für die Berechnung der Momentanbelastung allerdings voraussichtlich einige grundlegende individuelle Merkmale benötigt, wie zum Beispiel der Ruhepuls. Solche Parameter, die zur Kalibrierung der Analysen erforderlich sind, müssen dann über längere Zeiträume verfügbar gehalten werden.

Individualdaten jedoch sofort nach der Aggregierung zu löschen. Die Gangbarkeit dieses Ansatzes hängt jedoch von den Messzielen und dem spezifischen Aggregierungsverfahren ab.

Die erforderliche Mindestspeicherdauer der persönlichen Daten bemisst sich somit danach, welchen Verarbeitungszwecken der Nutzer zugestimmt hat und welche Funktionen der Anwendung er in Anspruch nehmen will. Möchte der Nutzer zum Beispiel auf seine persönliche Belastungshistorie der letzten Tage, Wochen oder Monate zurückgreifen, dann müssen die entsprechenden Daten mindestens über den gewünschten Zeitraum hinweg gespeichert werden. Legt der Nutzer Wert auf eine langfristige Nachvollziehbarkeit aller Ereignisse, dann muss das Event Log entsprechend weit in die Vergangenheit zurückreichen.

Ähnliches gilt für die gewünschte Analysequalität. Wenn sich zum Beispiel die Analysen anhand der Messwert-Trends kontinuierlich neu kalibrieren, um bestmögliche Befunde zu erzielen, dann müssen gegebenenfalls auch ältere Daten für die Trendermittlung und Adaption bereitgehalten werden.

Die Auswahl der Privacy-Einstellungen und der genutzten Funktionen eines Nutzers bestimmt also die minimal mögliche Speicherdauerbegrenzung, die er einstellen kann. Je nach Anwendungsgebiet ist auch der umgekehrte Ansatz möglich: Mit der Wahl einer Höchstspeicherdauer verändert sich die Auswahl an Funktionen, Diensten und Qualitäten, die dem Nutzer danach noch zur Verfügung stehen. Wenn dieser Interaktionsansatz gewählt wird, sollte die Anwendung eine genaue Rückmeldung geben, wie sich eine Speicherdauerbeschränkung auf die Nutzungsmöglichkeiten der App auswirkt.

Um dieses Interaktionskonzept möglichst einfach und nachvollziehbar zu gestalten, empfiehlt es sich meist, den Nutzern nur einige grundlegende Abstufungen der Speicherdauer zur Wahl anzubieten. Anwendungsentwickler können dazu harmonisch abgestufte Speicherdauern festlegen. Das Ziel ist es, möglichst gleitende Übergänge hinsichtlich Datenschutzgewinn und Nutzungseinbußen zu gewährleisten. Zudem kann die Anwendung für fest vorgegebene Stufen maßgeschneiderte Erläuterungen für den Nutzer bereithalten, um die Vorzüge und Nachteile der angebotenen Optionen genau zu beschreiben und die Gründe dafür möglichst transparent zu machen.

Wie bei anderen Einstellungen des Datenschutzprofils kann der Arbeitgeber auch hier die Wahlmöglichkeiten aufgrund betrieblicher oder technischer Gründe einschränken. Die Nutzer müssen sich dann mit beschränkten Selbstbestimmungsoptionen arrangieren oder auf die freiwillige Teilnahme am Messprogramm verzichten.

5.11 Visualisierung der Datenflüsse

Das Interaktionskonzept *Visualisierung der Datenflüsse* soll die Transparenz der Datenverarbeitung erhöhen und den Nutzern eine informierte Entscheidung im Umgang mit ihren Daten zu ermöglichen.

Dazu wird die Übertragungskette durch eine interaktive, animierte Grafik visualisiert, die den realen Fluss der Daten simuliert. Die Grafik stellt die verschiedenen Akteure dar, die an der Datenverarbeitung beteiligt sind. Sie zeigt auf, welche dieser Akteure Zugriff auf welche Daten erhalten (Abbildung 30).

Ein besonderes Merkmal ist die Interaktivität, die es den Nutzern ermöglicht, die Auswirkungen der getroffenen Einstellungen auf spielerische Weise zu testen. So können sie die Datenfreigabe für die Parameter Herzfrequenz, Beschleunigung und RR-Intervall aktivieren oder deaktivieren. Bei jeder Änderung werden die Auswirkungen für den Nutzer sichtbar, indem die App den jeweiligen modifizierten Datenfluss grafisch darstellt. Die Nutzer können sich so unmittelbar darüber informieren, welche Akteure Zugriff auf ihre Daten erhalten und wie die Daten verarbeitet werden. Hierbei werden jedoch keine echten Einstellungen vorgenommen, sondern die Nutzer können in einem sicheren Rahmen verschiedene Einstellungen und deren Konsequenzen durchspielen.

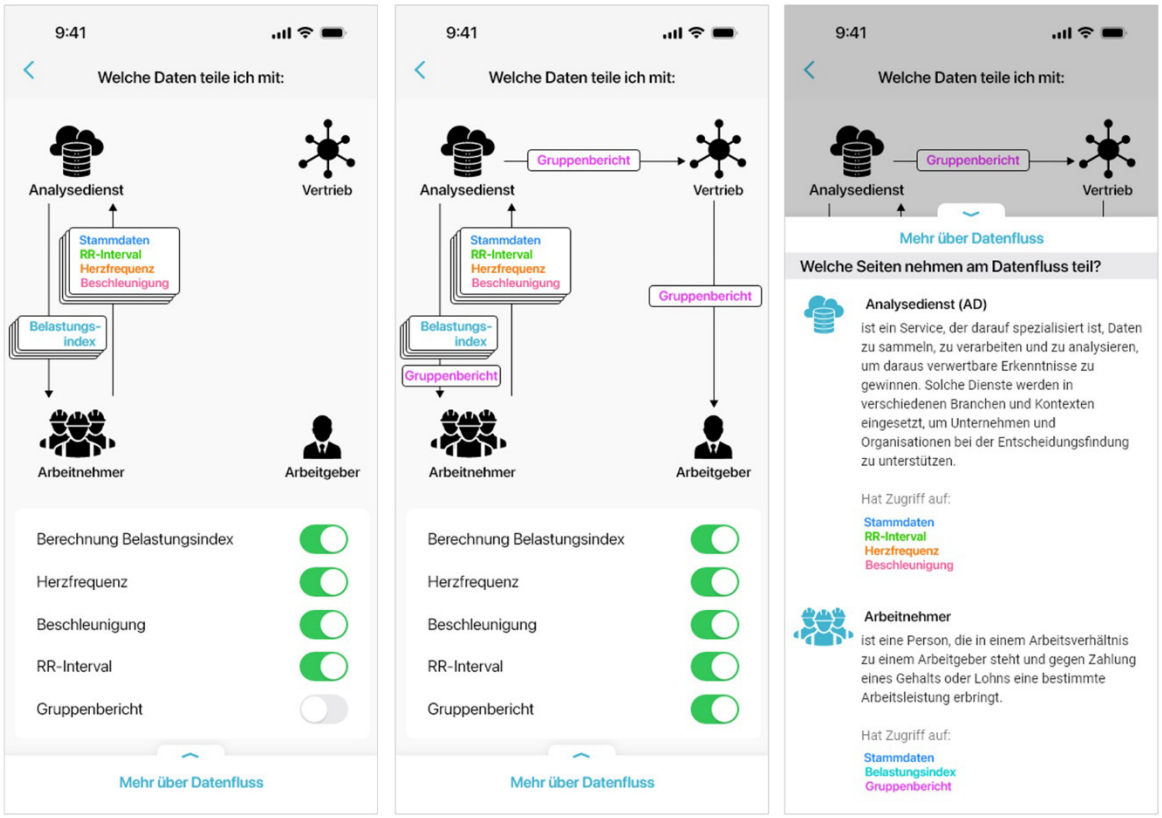


Abbildung 30 Datenfluss-Visualisierung: Je nach der Auswahl der Daten, die ein Nutzer mit dem Analysedienst oder seinem Arbeitgeber teilt, ergeben sich unterschiedliche Datenflüsse. Um den Nutzern zu verdeutlichen, wie sich ihre Einstellungen auf ihre Privatsphäre auswirken, stellt die App dar, welche Datenflüsse sich aus den gewählten Einstellungen jeweils ergeben.

Dies gilt gleichermaßen für die Zustimmung zur Berechnung des Belastungsindex wie für die Teilnahme am Gruppenbericht. Auch diese Funktionen können in der interaktiven Darstellung an- oder ausgeschaltet werden, woraufhin die Auswirkungen visualisiert werden. So wird den Nutzern in unserem Beispiel verdeutlicht, dass der Arbeitnehmer nie Zugriff auf die sensiblen Gesundheitsdaten erhält, sondern nur – nach Zustimmung – den Gruppenbericht mit aggregierten Werten bekommt.

Dieses Interaktionskonzept fördert das Vertrauen der Nutzer, da sie die Auswirkungen ihrer Entscheidungen sofort sehen und so die Kontrolle über die Datenflüsse behalten. Es ermöglicht eine selbstbestimmte Entscheidung über die Datenweitergabe und fördert die Datensouveränität.

6 Evaluation

Die Evaluation der Konzepte, die im Projekt entwickelt wurden, stützte sich zum einen auf die Analyse von Messwerten, die empirisch mit den realisierten Komponenten des WearPrivate-Demonstrators gewonnen wurden. Zum anderen nutzten die Projektpartner Interviews, um qualitative Aussagen über die Nutzerfreundlichkeit und Akzeptanz der im Projekt entwickelten Lösungsbausteine zu erhalten.

6.1 Sensitivität bezüglich Differential Privacy

Um zu prüfen, wie sehr Differential-Privacy-Techniken (siehe Abschnitt 4.3) die Analyseergebnisse beeinflussen, hat der Partner WH die Klassifizierung der unveränderten Rohdaten mit ihrer Klassifizierung nach einer Verfremdung mittels DP verglichen. Abbildung 31 zeigt ein Beispiel einer solchen Analyse, bei der die ursprünglich zugewiesene Beanspruchungsklasse (MENTAL, MIXED, PHYSICAL, RECOVERY) der neu ermittelten Klasse nach Datenverfremdung gegenübergestellt ist.

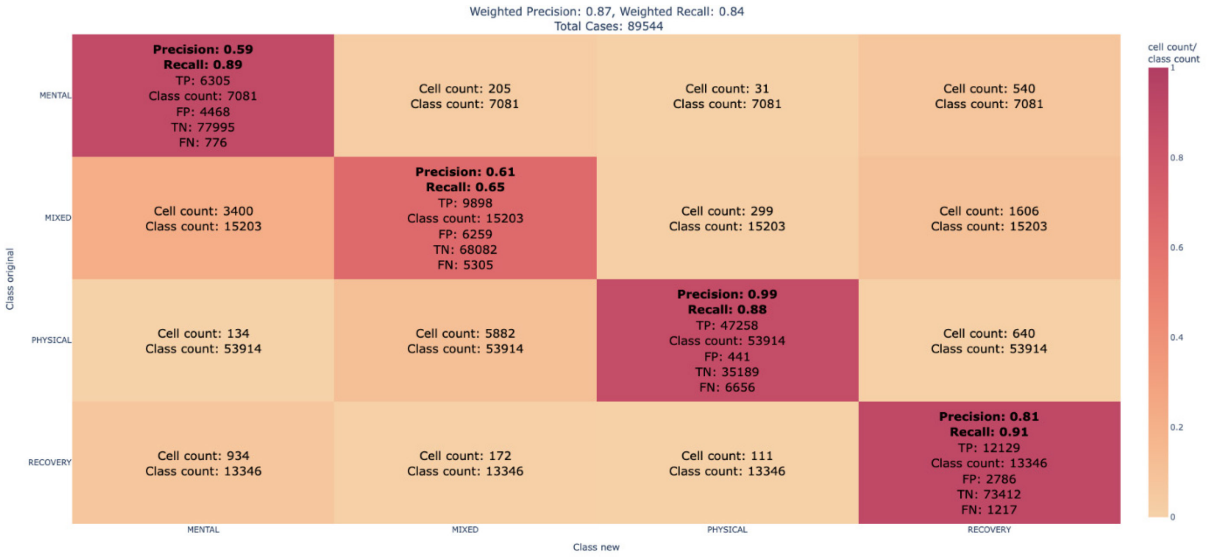


Abbildung 31 Beispiel für die Wirkung einer Datenverfremdung der gemessenen Herzratendaten auf die Klassifizierung der persönlichen Workload von Wearable-Trägern: Die Auswertung zeigt, wie die unveränderten Vitaldatenproben (89544 Fälle) ursprünglich klassifiziert wurden (vertikale Achse) und wie sich deren Klassifizierung nach Anwendung von Differential-Privacy-Techniken geändert hat (horizontale Achse).

Im Diagramm kann man für jede Klasse die Anzahl der korrekten positiven (True Positives, TP) und negativen (True Negatives, TN) Klassenzuordnungen sowie die Anzahl der falsch-positiven (False Positives, FP) und falsch-negativen (False Negatives, FN) Zuordnungen – verglichen mit der ursprünglichen Klassifizierung der unveränderten Rohdaten – ablesen. Daraus lässt sich für jede Klasse die Precision und der Recall der Klassenzuordnung berechnen:

$$Precision = \frac{TP}{TP+FP}$$ *Wie viele der als X klassifizierten Proben sind tatsächlich vom Typ X?*

$$Recall = \frac{TP}{TP+FN}$$ *Wie viele Proben des Typs X werden auch als X klassifiziert?*

Precision und Recall sind Werte zwischen 0 und 1, wobei 1 eine fehlerfreie Klassifizierung anzeigt.

Solche Messungen wurden im Projekt für verschiedene Verfremdungsstärken – charakterisiert durch die Wahl des DP-Parameters ε – vorgenommen. Abbildung 32 zeigt eine Übersicht der Befunde für die Klassifizierungsaufgabe gemäß Abbildung 31.

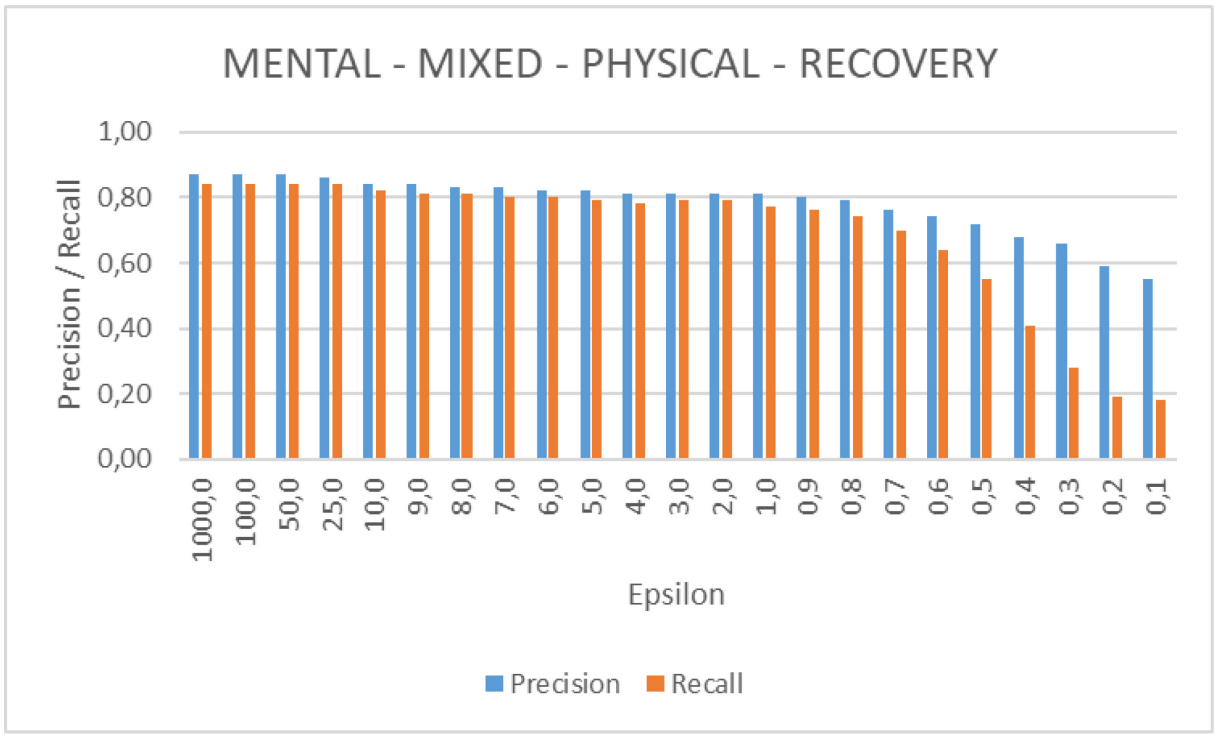


Abbildung 32 Effekt einer Datenverfremdung der gemessenen Herzratendaten auf die Klassifizierung der persönlichen Workload von Wearable-Trägern nach Belastungsart: Die Darstellung zeigt die erzielte Precision und den erzielten Recall der Klassifizierung – gewichtet nach der relativen Häufigkeit der einzelnen Klassen – gemäß der Klasseneinteilung aus Abbildung 31 für verschiedene Werte von ε im Bereich zwischen 0,1 und 1000.

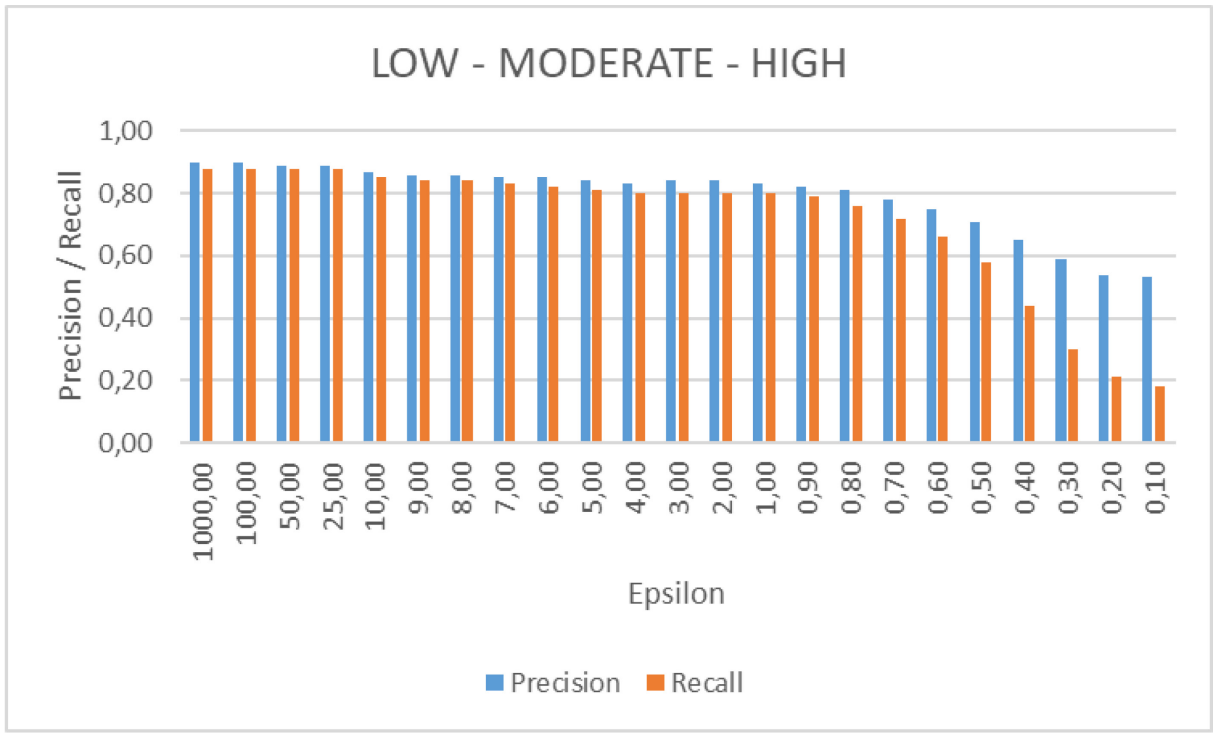


Abbildung 33 Effekt einer Datenverfremdung der gemessenen Herzratenvariabilitätsdaten auf die Bewertung der persönlichen Belastungsstärke als LOW, MODERTE oder HIGH: Für starke Datenverfremdung ($\varepsilon \leq 0{,}8$) nehmen die Fehleinschätzung merklich zu; wie in Abbildung 32 bricht vor allem der Recall rapide ein.

Schon bei milder Datenverfremdung mit ε-Werten zwischen 10 und 1000 sinken Precision und Recall der für unveränderte Rohdaten ermittelten Workload-Klassen merklich; ab $\varepsilon \leq 0{,}9$ nehmen die Klassifizierungsfehler rapide zu.

Auch die Wirkung einer DP-Verfremdung auf die Bewertung einer Belastungsstärke als LOW, MODERATE oder HIGH wurde für unsere Demonstratoranwendung ermittelt. Abbildung 33 zeigt das Ergebnis unserer Messungen. In diesem Fall ist eine Verfremdung mit einem $\varepsilon \leq 0{,}8$ noch vertretbar. Danach beginnt die Analysequalität merklich zu sinken.

Für unsere Demonstratoranwendung ergibt sich somit, dass für die Verfremdung der Herzraten-variabilitätsdaten ein $\varepsilon \geq 0{,}9$ gewählt werden sollte, um die Analysequalität in Bezug auf die Belastungsklassifizierung nicht allzu sehr zu beeinträchtigen. Die Beurteilung der Belastungsstärke reagiert nur geringfügig besser auf eine ε-Verfremdung der Daten als die Workload-Klassifizierung.

Nachdem so die Spielräume für eine DP-Datenverfremdung ausgelotet waren, untersuchte der Partner UdS den damit erzielbaren Anonymisierungsgewinn. Als Datenbasis dienten dabei zwei Datensätze, die Daten in Ruhephasen sowie auch in unterschiedlichen Stressphasen umfassen. Der erste Datensatz von Irurzun et al. [23] umfasst 147 Personen im Alter von einem Monat bis 55 Jahren. Da diese Alterspanne nicht unserem Anwendungsfall »Messprogramm für Arbeitnehmer« entspricht, wurden für die folgende Analyse nur die Personen zwischen 18 und 55 Jahren berücksichtigt (33 Personen). Im zweiten Datensatz von Koldijk et al. [24] sind 25 Personen vertreten.

Im Experiment wurde nun geprüft, inwieweit es gelingt, die oben beschriebenen Herzratendaten der insgesamt 58 Probanden einem vorgegebenen Vergleichsdatensatz einer bestimmten Person zuzuordnen und damit die Identität des Probanden zu bestimmen, dem die Herzratendaten jeweils zuzurechnen sind. Als Gütemaß für den Identifizierungserfolg diente der sogenannte F1-Score, also das harmonische Mittel aus Precision und Recall. Das harmonische Mittel lässt sich auch als der Quotient von Produkt und arithmetischem Mittel der beiden Größen darstellen:

$$F1 = \frac{Precision * Recall}{½ * (Precision + Recall)}$$

Wie man leicht sieht, gilt $Minimum(Precision, Recall) \leq F1 \leq Maximum(Precision, Recall)$, wobei der F1-Score immer zum niedrigeren der beiden Werte tendiert, also kleiner oder gleich dem arithmetischen Mittel von Precision und Recall ist.

Um eine hohe Datenschutzwirkung nachzuweisen, sollte der F1-Score für das oben beschriebene Identifizierungsproblem möglichst *gering* sein und damit bei einem Angriff auf die Anonymität der Daten möglichst schlechte Wiedererkennungsgüte liefern. Abbildung 34 zeigt, wie die Identifizierungs-leistung mit zunehmender Verfremdung der Herzratendaten (also sinkendem DP-Parameter ε) immer mehr abnimmt.

Wie sich zeigt, sind Herzratendaten recht charakteristisch für jede Person. Sie eignen sich daher als biologischer »Fingerabdruck«, um den Urheber der Daten zu identifizieren. Im Experiment gelang dies bei unveränderten Rohdaten mit einem F1-Score von etwa 0,9, also mit einer Precision und einem Recall in ähnlicher Höhe, wie in Abbildung 34 dargestellt. Mit zunehmender Datenverfremdung sinkt der Identifizierungserfolg zwar, aber die Verfremdung bietet in unserem Experiment nur einen geringen zusätzlichen Schutz vor einer Identifizierung der Probanden. Für den zuvor in unserer Demonstratoranwendung ermittelten Schwellenwert für ε von etwa 0,8 bis 0,9 (vgl. Abbildung 32 und Abbildung 33 auf Seite 46) ergibt sich gemäß Abbildung 34 ein F1-Score in der Größenordnung von 0,85. Dies liefert nur eine geringe Verbesserung gegenüber dem F1-Score für unveränderte Rohdaten.

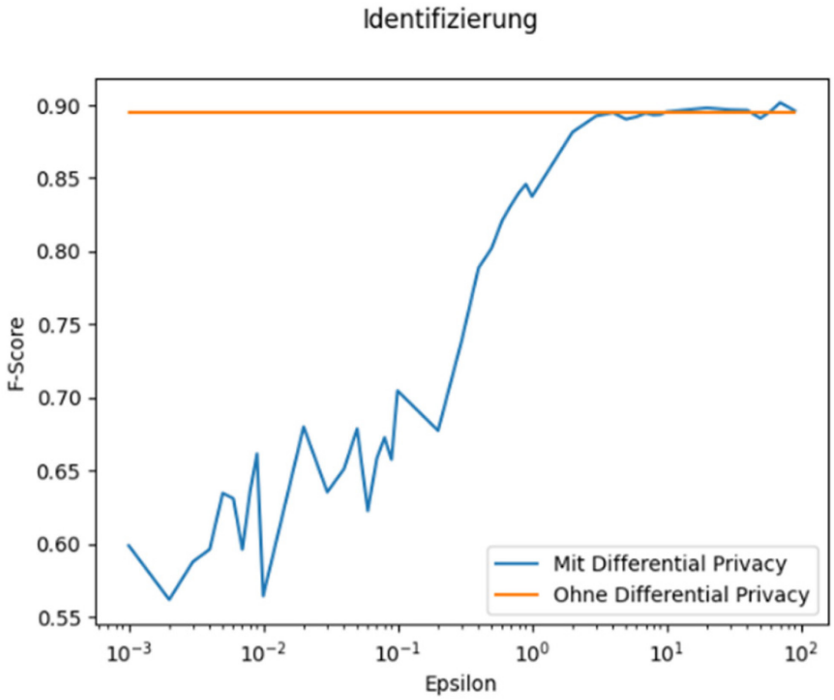


Abbildung 34 F1-Score des Identifizierungsexperiments in Abhängigkeit von der Verfremdungsstärke mittels Differential-Privacy-Techniken, charakterisiert durch den Parameter ε.

Bei diesem Befund ist allerdings zu berücksichtigen, dass gerade die Bestimmung der Herzratenvariabilität sehr empfindlich auf die Änderung von RR-Intervalllängen reagiert. Dies lässt für eine HRV-Bestimmung erwarten, dass überlagertes Rauschen schnell zu Fehleinschätzungen führt. Daher bieten Analysen, die auf den HRV-Wert zurückgreifen, generell nur wenig Spielraum für Anonymisierung durch Datenverfremdung.

Zudem ist bei unseren Experimenten zu berücksichtigen, dass mit dem DP-Parameter ε zwar die Stärke der Datenverfremdung charakterisiert wird, nicht aber das genaue Verfremdungsverfahren. Das von uns verwendete Verfahren ist im Ergebnisbericht D3.3 [20] genauer beschrieben. Bei diesem Verfahren mussten im Experiment zur Konsistenzwahrung verschiedene kleinere Anpassungen an den Daten vorgenommen werden, etwa, damit der übermittelte Puls-Wert noch zu den gemessenen Herzraten-Intervallen passt. Es gibt verschiedene Möglichkeiten, die Konsistenz der verfremdeten Daten zu gewährleisten, so zum Beispiel das Weglassen bzw. Einfügen von Messwerten oder das Stauchen beziehungsweise Strecken der zuvor verfremdeten Intervalle. Daher ist es denkbar, dass mit einem anderen als dem von uns implementierten Verfremdungsverfahren die Analysequalität besser gewahrt werden kann, was eine stärkere Datenverfremdung und damit einen stärkeren Schutz gegen die Identifizierung von Probanden ermöglichen würde.

Die ermittelten Spielräume für die Anwendung von Differential Privacy als Anonymisierungsmaßnahme bei HRV-Messungen sind darüber hinaus auch insoweit eine eher konservative Schätzung, als der Anonymisierungseffekt gemäß Abbildung 34 auf Auswertungen über einer nur geringen Probandenanzahl (58 Personen) beruht. Es ist naturgemäß leichter, ein HRV-Profil in einer kleinen Menge möglicher Kandidaten wiederzufinden als in einer sehr großen Grundgesamtheit. Wenn also ein Analysedienstleister HRV-Messungen von sehr vielen Kunden verarbeitet, sollte es einem Angreifer erheblich schwerer fallen als in unserem Experiment, einen Vergleichsdatensatz eindeutig einem bestimmten Probanden zuzuordnen. In diesem Fall ist bereits bei einer Datenverfremdung mit $\varepsilon \approx 1$ voraussichtlich mit einem deutlich besseren Anonymisierungseffekt zu rechnen.

Die Analysekomponente des WearPrivate-Demonstrators basiert auf künstlicher Intelligenz (KI). Um den Analysedienst robuster gegenüber Datenverfremdungen zu machen und damit eine stärkere Verfremdung ermöglichen, könnte man die KI gezielt mit verfremdeten Daten zu trainieren. In unseren Experimenten zeigte sich nämlich, dass die Verfremdung durch Differential-Privacy-Techniken die Herzraten-Variabilität tendenziell erhöht, was von dem Analyseverfahren meist als »geringere Belastung« interpretiert wird. Das bedeutet, dass der vom Demonstrator berechnete Belastungsindex bei verfremdeten Daten systematisch etwas zu gering eingeschätzt wird, wie die Beispielmessung in Abbildung 35 illustriert. Teilt man der Analysekomponente also mit, in welchem Maße die Messdaten verfremdet sind, so kann das KI-Verfahren die dadurch verursachte Fehlertendenz bei geeignetem Training zumindest teilweise kompensieren. Im Projekt fehlte leider die Zeit, diese Idee weiterzuverfolgen. Die vorläufigen Messungen weisen jedoch darauf hin, dass hier noch zusätzliche Verbesserungspotenziale erschlossen werden können.

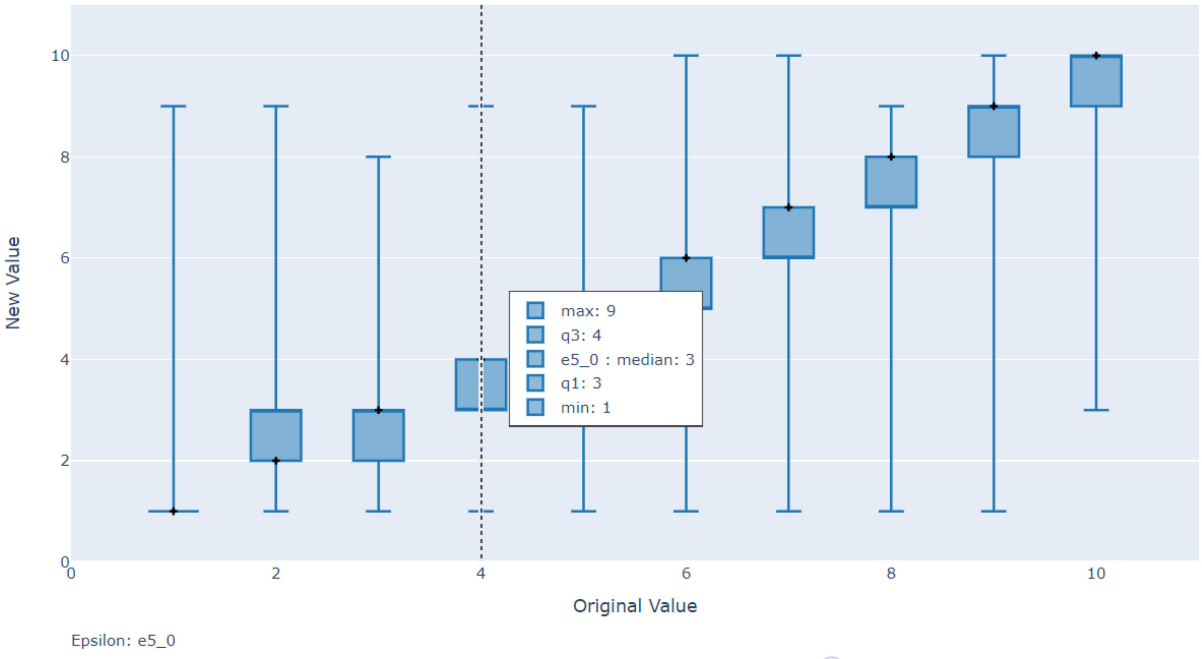


Abbildung 35 Beispiel für die systematische Verschiebung des ermittelten Belastungsindex [1 … 10] bei Verfremdung der Daten (Im Beispiel: ε = 5): Ähnliche Verschiebungen wurden im Projekt für unterschiedliche Werte von ε ermittelt.

Einschränkend ist noch anzumerken, dass unsere Versuchsreihen auf der Annahme basieren, dass unser Demonstrator die unveränderten Rohdaten korrekt klassifiziert. Unsere Vergleichsmessungen prüfen nur, wie sehr die Klassifizierung nach einer Datenverfremdung von der ursprünglichen Klassifizierung abweicht. Ob diese Abweichung aus medizinischer Sicht eine Verschlechterung oder eine Verbesserung des Befunds darstellt, ist damit genau genommen noch nicht erwiesen.

Während der Praxiserprobung der Anwendung und auch bei der Analyse der Effekte von Datenverfremdungen der statischen Profildaten von Probanden gab es Anhaltspunkte, dass die verwendete Analysekomponente zum Teil fehlerhafte Einschätzungen der tatsächlichen Belastungssituation vornimmt. Sollte sich dieser Verdacht erhärten, so mindert dies die Validität unserer Evaluationsergebnisse. Wichtiger als die an unserem eingeschränkten Demonstrator ermittelten Messergebnisse ist jedoch der hier beschriebene Evaluationsprozess, der valide ist, solange man die zugrunde gelegten Annahmen zuvor empirisch absichert.

6.2 Interviews bezüglich Interaktions- und Datenschutzkonzepten und Erprobung

Um die Interaktionskonzepte und Nutzerfreundlichkeit unseres Demonstrators zu evaluieren und zu prüfen, inwieweit die entwickelten Datenschutzkonzepte potenzielle Nutzer überzeugen und zur Teilnahme an einem Wearable-Messprogramm bewegen können, führten die Projektpartner WH, NMS und IESE qualitative Interviews mit Arbeitnehmern aus unterschiedlichen Berufsfeldern. Außerdem rekrutierte der Projektpartner NMS einen Probanden für eine Praxiserprobung, um Nutzererfahrung zu sammeln und Rückmeldungen zur Alltagstauglichkeit der Datenschutzkonzepte und zur Nutzerakzeptanz unserer Lösungsbausteine zu erhalten.

Die Interviews wurden mit vier männlichen Teilnehmern im Alter von 20 bis 50 Jahren aus unterschiedlichen Branchen durchgeführt: einem Arbeitssicherheitsexperten (Person A), einem Health & Safety Manager aus dem Bereich Seeschifffahrt (Person B), einem Industriearbeiter (Person C) sowie einer Krankenhaus-Pflegefachkraft (Person D). Den Interviewpartnern wurde ein Klick-Dummy unseres Demonstrators gezeigt, der das Interaktionskonzept veranschaulicht, und es wurde ihnen die grundlegende Prozesskette des Messprogramms erläutert. Sie hatten jedoch keinen Zugriff auf den funktionsfähigen Demonstrator im Praxisbetrieb, sondern mussten ihre Einschätzungen anhand der abstrakten Darstellung unserer Lösungskonzepte vornehmen. Im Interview wurden insbesondere Einschätzungen zu den folgenden Aspekten abgefragt:

- Vertrauen in die Lösung und deren Datenschutz:
  Person A (Arbeitssicherheitsexperte) und Person D (Pflegefachkraft) betonten beide die Bedeutung von Datenschutz und Kontrolle über ihre persönlichen Daten. Beide gaben hohe Bewertungen für die Möglichkeit, selbst zu entscheiden, welche Daten erfasst und weitergegeben werden dürfen.
  Person C (Industriearbeiter) teilte ebenfalls diese Bedenken in Bezug auf Datenschutzkontrolle, war jedoch grundsätzlich offen für die Nutzung der App, insbesondere durch den anonymisierten Anmeldeprozess und die Möglichkeit, die Datenerfassung zu steuern.
  ⇨ *Diese Aussagen lassen darauf schließen, dass Datenschutz eine entscheidende Rolle bei der Akzeptanz solcher Technologien spielt, da die Nutzer vor allem aufgrund der Anonymität und der Kontrolle über ihre Daten Vertrauen schöpften.*
- Genauigkeit und Funktionalität der Messungen:
  Person B (Health & Safety Manager) äußerte Skepsis gegenüber der Genauigkeit der Wearable-Technologie, insbesondere in Bezug auf seine spezifische Arbeitsumgebung. Er gab an, dass er die Technologie zwar als nützlich ansieht, aber Zweifel an der praktischen Umsetzung in seinem maritimen Arbeitsumfeld hat.
  Person C (Industriearbeiter) betonte, dass er die Verrauschung der Daten zum Schutz der Privatsphäre positiv bewertet, dass dies jedoch auch Unsicherheit hinsichtlich der Genauigkeit der Analysen auslöst.
  ⇨ *Diese Bedenken zur Genauigkeit spiegeln sich auch in den Bewertungen Praxiserprobung (siehe unten) wider. Es wird deutlich, dass die App hier noch Optimierungspotenzial aufweist, um das Vertrauen in die erfassten Daten zu steigern.*
- Anwendungspotenzial und Nutzerfreundlichkeit:
  Person A und C betonten, dass die App gut gestaltet und einfach zu bedienen sei. Sie empfanden die Transparenz bei der Datenverarbeitung als positiv und vertrauten der Technologie stärker aufgrund der die Möglichkeit, den Gruppenbericht selbst einzusehen, den ihre Vorgesetzten erhalten.
  ⇨ *Diese Einschätzungen korrelieren mit den hohen Bewertungen zur Benutzerfreundlichkeit in*

der Praxiserprobung (siehe unten). Die einfache Bedienung der App wurde von den meisten Teilnehmern als eine ihrer Stärken hervorgehoben.

Außerdem wurden die Interviewpartner gebeten, einige Aussagen auf einer Skala von 1 (»stimme überhaupt nicht zu«) bis 5 (»stimme vollkommen zu«) zu bewerten. Tabelle 2 zeigt die Einschätzungen der vier befragten Personen.

Tabelle 2 Einschätzung verschiedener Aussagen durch die Interviewpartner auf einer Skala von 1 (»stimme ich überhaupt nicht zu«) bis 5 (»stimme ich vollkommen zu«)

	Person A	Person B	Person C	Person D
[Vor Erläuterung der WearPrivate-Lösungsbausteine und Demonstration mittels Klick-Prototyp] ***Ich bin offen dafür, Wearable-Lösungen für Sicherheit und Gesundheit am Arbeitsplatz einzusetzen.***	4	2,5	4	5
Die Registrierung über einen zufälligen QR-Code anstelle meiner persönlichen E-Mail-Adresse hat mein Vertrauen in den Wearable-Service gestärkt.	4	4	5	5
Das Feature der Datenverwaltung hat mein Vertrauen in den Wearable-Service gestärkt.	5	4	4	5
Die Verrauschung der Daten hat mein Vertrauen in den Wearable-Service gestärkt.	4	4	4	5
Die Option zu entscheiden, für was meine Daten verarbeitet werden dürfen, hat mein Vertrauen gestärkt.	5	5	5	5
Die Option zu entscheiden, welche Daten erfasst werden dürfen, hat mein Vertrauen gestärkt.	5	5	5	4
Dass ich denselben Bericht einsehen kann wie mein Manager, hat mein Vertrauen in den Wearable-Service gestärkt.	5	5	5	5
[Nach Erläuterung der WearPrivate-Lösungsbausteine und Demonstration mittels Klick-Prototyp] ***Ich bin offen dafür, Wearable-Lösungen für Sicherheit und Gesundheit mit den vorgestellten Datenschutzfunktionen am Arbeitsplatz einzusetzen***	4	4	4	5

Alle Befragten zeigten sich gegenüber Wearable-Lösungen sehr aufgeschlossen. Im Vergleich zur Eingangsbefragung (vgl. Abschnitt 3.2) waren die Vorbehalte der Interviewpartner deutlich weniger ausgeprägt. Dies mag unter anderem damit zu tun haben, dass die Befragten in ihren Berufen stärkeren körperlichen Belastungen ausgesetzt sind und daher dem Gesundheits- und Arbeitsschutz einen höheren Stellenwert einräumen als die Teilnehmer der Eingangsbefragung aus einem IT-nahen Umfeld; eventuell waren sie sich auch der Datenschutzgefahren weniger bewusst als die mit IT-Problemen besser vertrauten Personen der ersten Befragung.

In einem zweiten Evaluationsschritt wurde unser Demonstrator im Praxistest erprobt. Als Proband diente ein männlicher Mitarbeiter des Partners NMS in der Alterskohorte 40 bis 45 Jahre, der überwiegend Bürotätigkeiten verrichtet und nicht in das WearPrivate-Projekt involviert war. Der Demonstrator wurde einem Probanden zunächst als Klick-Dummy vorgestellt. Dabei wurde ihm die grundlegende Funktionsweise der App veranschaulicht. Nach dieser Vorstellung beantwortete der Proband Fragen zur Benutzerfreundlichkeit und zum Datenschutz. Diese Fragen wurden später erneut aufgegriffen, um Veränderungen in den Einschätzungen nach der Praxiserprobung zu erfassen und zu evaluieren, wie der Prototyp das Vertrauen des Probanden in die Technologie beeinflusst hat.

Danach benutzte der Proband die im Projekt entwickelte Wearable-Lösung über einen längeren Zeitraum am Arbeitsplatz. Durch die direkte Interaktion mit dem Demonstrator in seinem Arbeitsumfeld konnte die Versuchsperson spezifische Aspekte der App nachvollziehen und im Gespräch mit den Entwicklern detailliert erläutern, welche Funktionen für sie besonders wichtig oder problematisch waren.

Der Proband bewertete die nachfolgenden Aspekte jeweils auf einer Skala von 1 (»stimme überhaupt nicht zu«) bis 5 (»stimme vollkommen zu«):

- Benutzerfreundlichkeit und Effizienz
  - □ *»Das System war einfach zu bedienen«*
    ⇨ Bewertung: 5/5
  - □ *»Ich konnte die Aufgaben effizient und ohne größere Schwierigkeiten bewältigen«*
    ⇨ Bewertung: 5/5
- Genauigkeit der Belastungsmessung
  - □ *»Die App hat meine Stresslevels präzise erfasst«*
    ⇨ Bewertung: 3/5
- Verständlichkeit der Benutzeroberfläche
  - □ *»Die Benutzeroberfläche der App war klar und verständlich«*
    ⇨ Bewertung: 4/5
- Alltagstauglichkeit
  - □ *»Ich würde das System auch in meinem Alltag zur Stressbewertung verwenden«*
    ⇨ Bewertung: 3/5
- Erkennen und Verständnis der Belastung
  - □ *»Das System half mir, meinen Stress besser zu erkennen und zu verstehen«*
    ⇨ Bewertung: 2/5
- Allgemeine Zufriedenheit mit der Lösung
  - □ *»Insgesamt war ich zufrieden mit meiner Erfahrung mit dem System«*
    ⇨ Bewertung: 3/5

Die Usability-Studie – ergänzt durch qualitative Interviews – zeigt, dass die App eine solide Grundlage hinsichtlich Benutzerfreundlichkeit und Effizienz bietet. Gleichzeitig wurde deutlich, dass die Genauigkeit der Belastungsmessungen sowie der Mehrwert der App für den Alltag weiter verbessert werden müssen. Der Datenschutz und die Kontrolle über die eigenen Daten erwiesen sich als zentrale Faktoren, die das Vertrauen der Befragten maßgeblich beeinflussten.

Besonders auffällig war, dass der Klick-Dummy von den Teilnehmern etwas besser bewertet wurde als die voll funktionsfähige Version der App. Die reduzierte Interaktion und klar strukturierte Darstellung im Klick-Dummy hatten eine positive Wirkung, da sie es den Befragten ermöglichten, sich auf die Benutzeroberfläche, die Navigation und vor allem auf das Datenschutzkonzept zu konzentrieren. Dieser Fokus auf die Interaktion mit den Datenschutzfunktionen, wie etwa die individuelle Kontrolle und die Transparenz bei der Datenerfassung, deutet darauf hin, dass der Datenschutz ein entscheidender Erfolgsfaktor für die Nutzerakzeptanz ist.

Ein weiterer Grund für die bessere Bewertung des Klick-Dummies könnte sein, dass die bewertenden Teilnehmer in diesem keine Erfahrungen mit Belastungshinweisen machen konnten, die zu einem mehr oder weniger nachvollziehbaren Zeitpunkt eintrafen, wie es beim Gebrauch der App geschah. Es ist vorstellbar, dass dieser technische Aspekt in der Vorstellung der Interview-Teilnehmer beim Klick-Dummy einfach »perfekt« funktionierte. In der praktischen Nutzung waren insbesondere der Messwert der mentalen Belastung sowie die zugehörigen Warnungen nicht immer intuitiv zu den aktuell durchgeführten Aktivitäten zuzuordnen.

Zusammenfassend lässt sich erkennen, dass die für die Anwender am deutlichsten sichtbare Komponente des WearPrivate-Gesamtsystems – die Smartphone-App – durch ihre als ansprechend und gut bedienbar bewertete Oberfläche eine wichtige Rolle darin spielt, den Nutzern einen selbstbestimmten Umgang mit ihren Daten zu ermöglichen. Gleichzeitig zeigen die Bewertungen der Messgenauigkeit sowie der Nachvollziehbarkeit der gemeldeten Belastungen, dass das WearPrivate-System in diesen Bereichen noch verbessert werden kann.

Es ist empfehlenswert, zu diesen Themen weitergehende Untersuchungen durchzuführen, um die Gründe für die hier beobachteten Probleme genauer zu identifizieren. Beispielsweise ist aktuell unklar, ob die empfundene Ungenauigkeit in der Belastungsmessung eine tatsächliche Ungenauigkeit ist, die durch technische Maßnahmen verbessert werden könnte, oder nur eine empfundene Ungenauigkeit. Insbesondere mentale Belastungen könnten für die betroffenen Personen in dem Moment des Geschehens gar nicht als solche wahrgenommen werden. Die genauere Analyse solcher Situationen in weiteren Studien sowie die differenziertere Formulierung der Warntexte würde von der Hinzunahme psychologischer und medizinischer Kompetenzen profitieren, die im WearPrivate-Projekt jedoch nicht zur Verfügung standen.

7 Voraussichtlicher Nutzen und Verwertbarkeit der Projektergebnisse

Die Projektpartner sehen für die erzielten Projektergebnisse verschiedene Verwertungsmöglichkeiten. Darüber hinaus hat das Projekt eine Reihe weiterführender Forschungsfragestellungen aufgeworfen, die im begrenzten Rahmen des WearPrivate-Projekts nicht mehr weiterverfolgt werden konnten, aber lohnende Ziele für Anschlussprojekte sein könnten.

7.1 Wirtschaftliche Verwertbarkeit

Der Projektpartner WearHealth (WH) ist darauf spezialisiert, Industrieunternehmen mithilfe von KI und Wearables dabei zu unterstützen, die Sicherheit und Gesundheit ihrer Mitarbeiter zu verbessern. Da die Lösungen mit sensiblen Daten arbeiten, ist Datenschutz ein entscheidender Aspekt, der adressiert werden muss.

Die Ergebnisse des WearPrivate-Projekts werden in verschiedene Teile der WH-Services integriert, wie zum Beispiel in die Benutzer-Apps, das Analyse-Dashboard und den Cloud-Service, um für die Kunden und deren Arbeitnehmer bestmöglichen Datenschutz zu gewährleisten.

Der Projektpartner neusta mobile solutions (NMS) wird die Tätigkeiten in WearPrivate als Referenz für seine Kompetenz in den Bereichen Wearable Computing, App-Entwicklung sowie Datenschutz und Datensicherheit im Rahmen seiner vertrieblichen Aktivitäten nutzen. Dabei soll der im Projekt entwickelte Demonstrator als Showcase genutzt werden. Damit soll die Kompetenz der NMS im Bereich Datenschutz und Datensicherheit als wesentliches Unterscheidungsmerkmal gegenüber dem Wettbewerb ausgebaut werden, damit NMS neben Software-Projekten zukünftig auch spezialisierte Beratungsleistungen anbieten kann.

7.2 Wissenschaftlich-technische Verwertbarkeit

Die Projektergebnisse aus WearPrivate ergänzen das Wissensportfolio des IESE und der UdS im Bereich Datenschutz, das mit den Projekten TrUSD [1], D'Accord [2] und KickStartTrustee [37] systematisch aufgebaut und mit WearPrivate nun erweitert wurde. Im Kern handelt es sich um Lösungsbausteine für die unterschiedlichen Aspekte einer angestrebten künftigen Datenökonomie, wie zum Beispiel Vertrauensbildung unter den Beteiligten, Einblick in alle datenschutzrelevanten Vorgänge und vorgehaltenen persönlichen Daten (Transparenz), Datennutzungskontrolle über bereitgestellte Daten sowie Wahrnehmung und Durchsetzung der Betroffenenrechte (informationelle Selbstbestimmung). Diese Aspekte wurden in den genannten Projekten in unterschiedlichen Kontexten (z. B. Arbeitsplatz, Digitales Ökosystem), in Bezug auf unterschiedliche Anforderungen (z. B. Datenschutz, IT-Sicherheit, Rechtssicherheit, Nutzerfreundlichkeit) und aus verschiedenen Blickwinkeln (z. B. Arbeitnehmer, Geschäftspartner, Datentreuhänder) beleuchtet.

Anders als zuvor lag der Schwerpunkt des WearPrivate-Projekts nicht auf klassischer Informationsverarbeitung im Rahmen von Geschäftsprozessen, sondern auf kontinuierlich erhobenen Vitaldaten. Hier erfolgt die Erfassung und Analyse der Daten unterschwellig, ohne dass die Beteiligten ausdrücklich IT-Transaktionen anstoßen müssen wie in konventionellen Geschäftsanwendungen. Wie wichtig solche Wearable- oder Sensor-Daten zukünftig sein werden, zeigt neben der zunehmenden Verbreitung von Fitnesstrackern (z. B. Smart-Watches, Brustgurte, Fahrrad-Trittfrequenz- und -Drehmoment-Sensoren) im privaten Freizeitbereich zum Beispiel auch die Ausstattung moderner

Fahrzeuge mit immer umfassenderer Verkehrstelematik. Ein anderes Einsatzfeld ist die Hausautomatisierung, die Sensor-gesteuert Aspekte wie Schließung, Klimatisierung, Belüftung und Beleuchtung automatisch an die Bedürfnisse der Bewohner anpasst und dabei durch intelligentes Energiemanagement den Energieverbrauch minimiert. In all diesen Anwendungsfeldern fallen im Zuge der Sensorüberwachung zahlreiche schützenswerte persönliche Daten an.

Während die ausgeklügelte Vermessung aller Lebensbereiche große Potentiale hat, Prozesse effizienter, nutzerfreundlicher und sicherer zu machen oder Forschungsdaten für eine bessere medizinische Versorgung der Menschen zu liefern, birgt sie auch viele Datenschutzherausforderungen. Hier setzt WearPrivate an und entwirft Konzepte, Sensordaten nutzbar zu machen, ohne die Anonymität der Datengeber zu gefährden. Konkret liefern die Arbeiten im Projekt unter anderem folgende Beiträge:

- ein Verfahren für eine systematische Bedrohungsanalyse, die ausgehend von den schützenswerten Gütern einer Anwendung, den Motiven potenzieller Angreifer, den geltenden rechtlichen Bestimmungen und Normen sowie der anerkannten guten Praxis die Anforderungen an eine sichere, datenschutzfreundliche Gestaltung des Systems Schritt für Schritt herleitet;
- einen Anforderungskatalog für Wearable-basierte Gesundheitslösungen mit konkreten Vorschlägen für Maßnahmen, um die Transparenz der Datenverarbeitung und die informationelle Selbstbestimmung der Betroffenen zu stärken und die Interessen der verschiedenen Beteiligten zu schützen;
- einen Architekturvorschlag, um personenbezogene Daten am Arbeitsplatz vollständig anonym zu erheben und zu analysieren, ohne dass die Nutzer der Anwendung ihre Identität preisgeben müssen;
- eine beispielhafte Implementierung von Messdatenanonymisierung auf der Basis von Differential-Privacy-Techniken und Verfahren zur Beurteilung der damit einhergehenden Qualitätseinbußen in Bezug auf die erzielten Analysebefunde;
- einen beispielhaften Einsatz des von IESE entwickelten MYDATA-Frameworks in einem neuen Anwendungskontext, um für das Rahmenwerk zur Datennutzungskontrolle, das bereits von Industriekunden des Instituts lizenziert wurde, neue Einsatzfelder zu erschließen;
- Interaktionsmechanismen für eine mobile Anwendung, um die Transparenz- und Selbstbestimmungsansprüche von Arbeitnehmern zu befriedigen und ihr Vertrauen für eine freiwillige Teilnahme an einem Messprogramm zum Arbeits- und Gesundheitsschutz zu gewinnen durch offensichtliche, auch einem IT-Laien vermittelbare Datenschutzmaßnahmen.

Als Forschungseinrichtungen streben IESE und UdS im Gegensatz zu den Industriepartnern keine kommerzielle Nutzung entsprechender Wearable-Lösungen an, beraten aber interessierte Industriekunden bei der Gestaltung und Entwicklung solcher Systeme. Die oben beschrieben Lösungsbausteine können so oder so ähnlich auch in verwandten Anwendungsfeldern nutzbringend eingesetzt werden.

Im Projektkonsortium des WearPrivate-Projekts bleibt es vor allem dem Industriepartner WH als einem Domänenspezialist vorbehalten, die Ergebnisse des Projekts unmittelbar in eigenen konkreten Dienstleistungen zu vermarkten. Aber auch der Entwicklungs- und Evaluationspartner NMS konnte im Zuge des Projekts sein Profil als Entwickler mobiler Lösungen glaubhaft um Kompetenzen im Bereich von Gesundheits- und Arbeitsschutzanwendungen erweitern.

7.3 Wissenschaftliche Anschlussfähigkeit

Im Projekt haben die Partner unter anderem die Datennutzungskontrolltechnologie MYDATA eingesetzt, um die vom Nutzer gewünschten Datennutzungsregeln entlang der Messdatenverarbeitungskette durchzusetzen. Forschungsbedarf in Bezug auf Datennutzungskontrolle besteht bei der Attestierung von MYDATA-Komponenten, die auf entfernten Plattformen Datennutzungsrichtlinien überwachen und notfalls erzwingen sollen.

Bisher geschieht die Attestierung überwiegend durch manuelle Audits und vertragliche Regelungen. Dies erschwert eine Zertifizierung und kontinuierliche Aufrechterhaltung der Datenschutzeigenschaften eines Analysedienstes. Die Forschung hat zwar die kryptografischen Grundlagen für eine sogenannte Remote Attestation erarbeitet – also den formalen Nachweis, dass eine Software-Komponente authentisch ist und auf einer definierten, unveränderten Betriebssystemplattform ausgeführt wird. Allerdings sind die vorgeschlagenen Verfahren recht aufwändig und wenig anwendungsfreundlich. Zusammen mit anderen Fraunhofer-Instituten war das IESE an der Erforschung praktikabler Lösungen im Kontext von Industrial Data Spaces beteiligt [25][26][27]. Eine bequeme Möglichkeit, die Datenschutzqualitäten eines Cloud-Dienstes technisch, ohne manuelle Inspektionen vor Ort oder allein anhand vertraglicher Gewährleistungspflichten gegenüber den Dienstnutzern sicher nachzuweisen, fehlt jedoch noch immer und muss weiter erforscht werden.

Der im WearPrivate-Projekt entwickelte Demonstrator nutzt für die Analyse der Messdaten Techniken der Künstlichen Intelligenz (KI). Während der Evaluation der Datenverfremdung als Mittel zur Anonymisierung der Messdaten ergaben sich im Projekt Anhaltspunkte dafür, dass die KI-Komponente womöglich übertrainiert war, also Anzeichen von sogenanntem *Overfitting* aufwies. Overfitting tritt auf, wenn ein KI-System zu intensiv auf einen bestimmten Trainingsdatensatz optimiert wurde. Das System erzielt dann zwar überdurchschnittliche gute Ergebnisse für die Trainingsbeispiele, büßt dadurch aber seine Fähigkeit zum Generalisieren der Trainingsdaten ein: Weichen die Messwerte nur geringfügig von den Trainingsbeispielen ein, so erkennt die KI diese Ähnlichkeit nicht mehr und liefert dann trotz der Ähnlichkeit der Daten unangemessen stark abweichende Befunde. Im Projekt fehlte leider die Zeit und das medizinische Fachwissen, um solchen Indizien genauer nachzugehen. Für den praktischen Einsatz von Wearables im Gesundheitsschutz wäre es aber lohnend, KI-Systeme zu diesem Zweck auch mit verrauschten Daten zu trainieren. Dies würde nicht nur den Spielraum für verfremdungsbasierte Datenanonymisierung vergrößern, sondern es könnte auch die Fähigkeit der Analysekomponenten zum Generalisieren von Messergebnissen verbessern.

Neben domänenspezifischen inhaltlichen Arbeiten hat WearPrivate auch Beiträge zur Entwicklungsmethodik datenschutzkritischer Systeme geliefert. Dazu wurde ein am IESE entwickeltes Verfahren zur systematischen Bedrohungs- und Sicherheitsanforderungsanalyse [28] über die Jahre weiterentwickelt [11]. Inzwischen wurde der Analyseansatz in unterschiedlichen Anwendungsdomänen wie Medizingerätetechnik, Avionik, Automotive, Gesundheitswesen und nun auch Wearable-Lösungen angewendet und dabei um weitere Prozesselemente für Datenschutz ergänzt. Dadurch eröffnen sich neue Forschungsperspektiven im Bereich der IT-Sicherheit (Security) und des Datenschutzes (Privacy), aber auch im Bereich der funktionalen Sicherheit (Safety) und angrenzenden Themengebieten rund um die Verlässlichkeit (Dependability) und Resilienz von Systemen. Hier besteht noch erheblicher Forschungsbedarf, weil in der industriellen Praxis die Aspekte Security und Safety derzeit oft noch von unabhängigen Teams mit unterschiedlichen Methoden und Werkzeugen bearbeitet werden. Aufgrund der zunehmenden Abhängigkeit der Gesellschaft von IT-Systemen, dem immer weiteren Vordringen von IT in sicherheitskritische Anwendungsfelder sowie der zunehmenden Vernetzung von IT-Systemen über offene Kommunikationsstandards wachsen beide Aspekte der Sicherheit – Safety und Security – immer mehr zusammen und sollten in der Systementwicklung ganzheitlich betrachtet werden.

8 Dissemination der Projektergebnisse

Die Projektpartner nutzten verschiedene Disseminationsmaßnahmen, um ihre Projektergebnisse der Öffentlichkeit vorzustellen und in die aktuelle Forschung einzubringen.

8.1 Projektwebseite

Die UdS hat für das Projekt eine Projektwebseite [29] eingerichtet. Diese informierte die Öffentlichkeit über Projektdetails, die Projektpartner sowie über aktuelle Entwicklungen. Hierzu gehörten auch Berichte zu Veröffentlichungen, Konferenzen und Workshops sowie zu durchgeführten Konsortialtreffen.

Die Partner werden die Ergebnisberichte des Verbundvorhabens nach Fertigstellung auf der Projektwebseite veröffentlichen und zum Herunterladen bereitstellen.

8.2 Erfolgte oder geplante Veröffentlichungen

Im engeren Kontext des Projekts sind folgende Veröffentlichung entstanden.

- B. Steffes et al. (2022). Einwilligung oder Anonymisierung? Rechtliche Implikationen der Datenverarbeitung im Beschäftigungskontext [30]
- Simone Salemi, Nils Wiedemann (2023): Die europäische Datenstrategie und das Datenschutzrecht: Abgrenzungsschwierigkeiten Data Act und Data Governance Act zur DSGVO [31]
- Simone Salemi, Nils Wiedemann: Die europäische Datenstrategie und das Datenschutzrecht: Das Verhältnis von Daten-Governance-Gesetz und Datengesetz zur DSGVO [32]
- Ajla Hajric und Simone Salemi (2024): Können Datenschützer aus Konzepten des sexuellen Konsenses lernen? [33]

Darüber hinaus wird jedes der vier Teilprojekte des WearPrivate-Verbundvorhabens einen Abschlussbericht publizieren. Diese Berichte sind über die Technische Informationsbibliothek (TIB) [34] in Hannover oder direkt von den Verbundpartnern beziehbar.

8.3 Vorträge

Die Projektpartner nahmen an folgenden Veranstaltungen als Vortragende teil oder organisierten selbst die entsprechenden Events:

- Forum Privatheit (2023): Data Sharing – Datenkapitalismus by Default? Jahreskonferenz 2023 der Plattform Privatheit, Berlin [35]:
  Am 5. und 6. Oktober 2023 fand im Umweltforum Berlin die Jahreskonferenz »Forum Privatheit 2023: Data Sharing – Datenkapitalismus by Default?« statt. Das Projekt WearPrivate war mit einem Poster zum Thema »Data Sharing im Kontext digitaler Selbstvermessung« vertreten. Beleuchtet wurde dabei das Spannungsfeld zwischen dem Wunsch, vorhandene Daten möglichst umfassend nutzbar zu machen – also auch für Forschungszwecke und für die Allgemeinheit – andererseits aber die berechtigten Datenschutzinteressen der Betroffenen zu wahren. Dies hat in einem Arbeitsplatzumfeld, wie es von WearPrivate postuliert wird und wo

ein Abhängigkeitsverhältnis zwischen den Beschäftigten und ihrem Arbeitgeber besteht, eine besondere Brisanz. Der Beitrag beleuchtete dazu auch technische Maßnahmen zum Wearable-Datenschutz, die im Projekt entwickelt wurden.

- Fraunhofer IESE und Fraunhofer IAO (2023): Datenökonomie trifft Datenschutz. Berlin, Fraunhofer-Forum [36]:
  Am 10. Oktober 2023 fand im Fraunhofer-Forum in Berlin eine gemeinsame Veranstaltung der Fraunhofer-Institute IESE und IAO »Datenökonomie trifft Datenschutz« vor interessierten Gästen aus Forschung, Wirtschaft und Politik statt. Dabei stellten fünf Projekte im Rahmen der BMBF-Ausschreibung »Selbstvermessung und digitale Selbstbestimmung« ihre Forschungsarbeiten vor, darunter D'Accord [2], PERISCOPE [3], TESTER [4], KickStartTrustee [37] und WearPrivate. Die Projekte präsentierten ihre Zielsetzung sowie den Stand ihrer Arbeiten und stellten sich der Diskussion.
- Fraunhofer IESE, Universität des Saarlands, neusta mobile solutions GmbH, WearHealth (2024): Abschlusspräsentation des Projekts WearPrivate [Online-Veranstaltung]:
  Am 12. November 2024 präsentierten die Projektpartner ihre Projektergebnisse im Rahmen eines öffentlichen halbtägigen Online-Events und luden zur Diskussion ein. An der Veranstaltung nahmen auch Vertreter angrenzender Forschungsprojekte (z. B. D'Accord, PERISCOPE, TESTER, GameUp) und des »Forum Privatheit« teil sowie der für WearPrivate zuständige Projektbetreuer des Projektträgers VDI/VDE. Eingeladen waren auch Repräsentanten verschiedener einschlägiger GI-Arbeitsgruppen (z. B. aus den Bereichen Digital Health, Consumer Health Informatics, Usable Safety and Security, Privacy Enhancing Technologies).

8.4 Messebesuche

Um die Fortschritte, Erkenntnisse und Ergebnisse des WearPrivate-Projekts zu präsentieren, nahm der Verbundprojektpartner WH aktiv an einschlägigen Kongressen und Messen teil, die gezielt von potenziellen Kunden aus den Bereichen Arbeitssicherheit und Gesundheitslösungen besucht werden. Auf diesen Veranstaltungen stellte WH sein Portfolio an Wearable-basierten Lösungen zur Verbesserung von Sicherheit und Gesundheit am Arbeitsplatz vor und demonstrierte die im Rahmen des WearPrivate-Projekts entwickelten Datenschutzstrategien.

In Gesprächen mit Fachleuten aus verschiedenen Branchen – darunter Energie, Logistik, Fertigung, Automobil und Bau – tauschte sich WH über aktuelle Herausforderungen und Bedürfnisse aus. Zu den Gesprächspartnern zählten Betriebsleiter, Teamleiter sowie Fachkräfte für Arbeitssicherheit und Gesundheitsschutz. Datenschutz war ein zentrales Thema in allen Diskussionen und WH erhielt durchweg positive Rückmeldungen zu den im WearPrivate-Projekt entwickelten Lösungen.

Besuchte Veranstaltungen:

- A+A 2023, Düsseldorf (24.–27. Oktober 2023):
  Die A+A ist eine weltweit führende Messe für Arbeitssicherheit, Gesundheitsschutz und Security. Sie präsentiert die neuesten Innovationen in den Bereichen Persönliche Schutzausrüstung, Sicherheitstechnologien und Gesundheitslösungen. Neben einer umfangreichen Ausstellung bietet die Messe Expertenvorträge und Seminare und dient als wichtige Networking-Plattform für Fachleute und Branchenführer.
- BVL Supply Chain CX 2024, Berlin (23.–25. Oktober 2024):
  Diese Kongress-Expo-Kombination konzentriert sich auf Logistik- und Lieferketten-

management und behandelt Themen wie Nachhaltigkeit, Digitalisierung, KI und Innovation. Mit über 160 Expertenvorträgen und 120 Ausstellern bietet die Veranstaltung Einblicke in die Zukunft von Lieferketten. Netzwerkveranstaltungen und interaktive Workshops ergänzen das Programm

- ARBEITSSCHUTZ AKTUELL 2024, Stuttgart (5.–7. November 2024):
  Diese bedeutende Fachmesse für Arbeitssicherheit und Gesundheitsschutz präsentiert 250 Aussteller mit Innovationen in den Bereichen Persönliche Schutzausrüstung, Arbeitssicherheit und Gesundheitsmanagement. Das begleitende Konferenzprogramm behandelt Themen wie die Auswirkungen des Klimawandels, neue Arbeitsmodelle und Maschinensicherheit, und es bietet zahlreiche Networking-Möglichkeiten.

8.5 Master- und Bachelorarbeiten

Beim Partner NMS haben zwei studentische Mitarbeitende des WearPrivate-Projekts auf Grundlage der dort gewonnenen Kenntnisse über Technik und Usability von Wearables ihre gemeinsame Masterarbeit konzipiert:

- Jule Marie Hucke, Jan-Niclas de Vries (2025): *Asana Ai Swift & Sense – A System to Support Yoga Practitioners by Using Machine Learning Algorithms and Feasible Feedback Channels* [38]

Die Arbeit wird voraussichtlich im Februar 2025 abgeschlossen sein und nimmt Bezug auf Ergebnisse des WearPrivate-Projekts.

An der Universität des Saarlandes wurden im Verlauf des Projekts eine Reihe an Bachelorarbeiten angefertigt, deren Ergebnisse in die Arbeiten der UdS im Projekt eingeflossen sind. Die folgende Auflistung zeigt die Titel der Arbeiten:

- An analysis of data transfer and comparison using secure multiparty computation in the area of wearables and quantified self (2022)
- Implementierung einer anonymen Systemarchitektur zur Übermittlung von Gesundheitsdaten im Beschäftigungsverhältnis (2022)
- Privacy-Preserving Step Data Collection: A Comparison of Differential Privacy Implementations for Wearables (2023)
- Datenschutzkonforme Stresserkennung mit Hilfe der Herzfrequenzvariabilität (2024)
- Accelerating Towards Precision: Identifying Position Segments Using Acceleration Data (2024)

9 Zusammenfassung und Ausblick

Im Rahmen des WearPrivate-Projekts haben die Projektpartner verschiedene Lösungsbausteine entwickelt, um Wearable-basierte Anwendungen in einem beruflichen Umfeld datenschutzfreundlich zu realisieren. Damit lässt sich die immer ausgefeiltere Wearable-Sensorik, die im privaten Freizeit- und Sportbereich inzwischen gut etabliert ist, auch für den betrieblichen Gesundheits- und Arbeitsschutz erschließen.

Der vorliegende Bericht dokumentiert die zugrundeliegenden Konzepte und Realisierungsansätze, um die Privatsphäre der Wearable-Nutzer zu schützen, zugleich aber auch deren kontinuierlich erhobenen Vital- und Umgebungsdaten nutzbar zu machen. Dabei muss einerseits eine ausreichende Datenvielfalt und Datenqualität erzielt werden, die medizinisch fundierte Erkenntnisse liefert; andererseits dürfen die Wearable-Daten nicht zu einer Leistungs- oder Verhaltenskontrolle missbraucht werden.

Da die Teilnahme an einem betrieblichen Wearable-Messprogramm nach geltendem Recht nur auf freiwilliger Basis erfolgen kann, genügt es nicht, einen rechtskonformen Datenschutz technisch zu gewährleisten: Die Datenschutzeigenschaften einer Wearable-Lösungen müssen den Betroffenen auch nachvollziehbar vermittelt werden, um sie für eine freiwillige Teilnahme am Messprogramm zu gewinnen. Sofern man Datenschutzvorbehalte der Betriebsangehörigen nicht ausräumen oder ihnen den Mehrwert eines Gesundheits- und Arbeitsschutz-Monitorings nicht überzeugend darlegen kann, wird der Arbeitgeber mit der Einführung einer solchen Lösung scheitern. Ein wichtiges Ziel des Projekts war es daher, Lösungsbausteine zu finden, deren Wirkungsweise sich auch IT-Laien leicht vermitteln lässt und die »offensichtlich« die Privatsphäre schützen, den Nutzer umfassend über alle datenschutzrelevanten Vorgänge informieren (Transparenz) und ihm ein Höchstmaß an Mitbestimmung über die Verwendung seiner persönlichen Daten bieten (informationelle Selbstbestimmung).

Im Zuge der Forschungs- und Entwicklungsarbeiten und der Praxistests mit dem im Projekt entwickelten Demonstrator sind allerdings auch einige Grenzen des Wearable-basierten Arbeits- und Gesundheitsschutzes deutlich geworden. So lässt die Messgenauigkeit und Zuverlässigkeit der heute marktgängigen Wearables oft noch zu wünschen übrig. Dies ist nicht ganz überraschend, denn die Hersteller privat genutzter Wearables müssen einen Kompromiss finden, indem sie verschiedene Anforderungen gegeneinander abwägen, wie zum Beispiel das Preis-Leistungsverhältnis, den Energieverbrauch oder den Bedien- und Tragekomfort des Wearables. Hinzu kommt, dass eine präzise Messung generell schwierig ist, wenn der Wearable-Gebrauch nicht von fachlich geschultem Personal überwacht wird, um Anwendungsfehler auszuschließen. Je nachdem, wie locker oder wie fest ein Brustgurt oder eine Smartwatch am Körper fixiert wird und wie genau der korrekte Sitz des Geräts kontrolliert wird, können sich deutliche Datenverluste oder Messwertverfälschungen ergeben. Hier fehlt es an Studien, die genauer ergründen, welche Messgenauigkeit sich im unüberwachten Eigengebrauch überhaupt erzielen lässt.

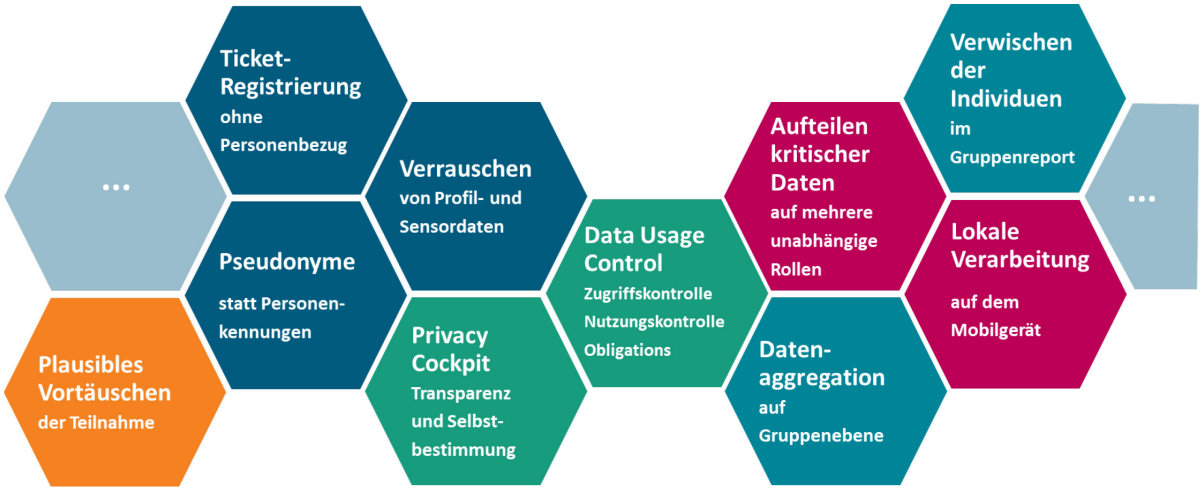
Problemtisch ist auch die Beurteilung der Auswertungsgüte von Wearable-Messdaten. Da wir im WearPrivate-Projekt nicht auf medizinische Experten zurückgreifen konnten, war es mitunter schwer zu beurteilen, ob die ermittelten Befunde valide sind oder auf Fehleinschätzungen der Analyselogik beruhen. Eine Beurteilung fällt allein deshalb schwer, weil die Verarbeitung der Rohdaten oft mittels KI-Systemen erfolgt: Die Konstruktion nachvollziehbarer KI – zum Beispiel *Explainable Neural Networks* – ist derzeit noch Gegenstand intensiver Forschung. In unseren Praxiserprobungen fanden sich Hinweise, dass die im Projekt verwendete Analysekomponente mitunter zu Fehlschlüssen neigt. Um

hier belastbare Aussagen zu False Positives und False Negatives zu ermitteln, bedarf es weiterer klinischer Studien.

Was schließlich die Freiwilligkeit einer Teilnahme an einem Wearable-Messprogramm betrifft, sind zwei grundlegende Hürden zu überwinden: nachvollziehbarer Nutzen und grundlegendes Vertrauen. Unabhängig davon, ob potenzielle Teilnehmer eines Messprogramm Datenschutzvorbehalte haben oder nicht, ist die Wearable-Nutzung immer mit gewissen Mühen und Einschränkungen verbunden. Diese werden die Betroffenen nur auf sich nehmen, wenn sie einen entsprechenden Gewinn für ihre Arbeitssicherheit und Gesundheit erkennen können. Die Kosten-Nutzen-Abwägung fällt am ehesten in gefahrengeneigten Tätigkeitsfeldern positiv aus – etwa im Bergbau, in der Forstwirtschaft oder in der Seeschifffahrt. In Berufen, die eher durch mentale Belastungen als durch offensichtliche körperliche Beanspruchung geprägt sind, wird daher die Zustimmung zu einer Selbstvermessung geringer ausfallen. Wie die Ergebnisse unserer Umfragen nahelegen, gilt dies insbesondere für Berufszweige, die eng mit der Datenschutzproblematik von IT-Lösungen befasst sind. Um auch Datenschutzskeptiker oder Arbeitnehmer für ein Messprogramm zu gewinnen, die keinen ganz offensichtlichen körperlichen Gesundheitsrisiken ausgesetzt sind, bedarf es daher überzeugender Nachweise, dass die mittels Wearables erzielbare Vitalüberwachung einen signifikanten gesundheitlichen Mehrwert bietet.

In Bezug auf das Vertrauen der Betroffenen, dass die erhobenen Daten nicht missbräuchlich verwendet werden, stehen betriebliche Wearable-Messprogramme vor einem Dilemma: Wenn die Belegschaft dem Arbeitgeber nicht vertraut, so wird sie sich auch durch ausgefeilte Datenschutzlösungen nur schwer zu einer Teilnahme bewegen lassen; ist das Vertrauensverhältnis jedoch gut, dann sollte der Arbeitgeber ein offenes Ohr für die Belange der Beschäftigten haben, so dass es oft keiner Wearable-Messungen bedarf, um die (Über-)Belastung von Arbeitsgruppen oder einzelner Betroffener zu erkennen und direkt anzusprechen. In diesem Fall bleibt dem Wearable nur die Aufgabe, solche Belastungen aufzuspüren, die den Betroffenen selbst gar nicht bewusst sind – was aber sehr hohe Anforderungen an die Validität der arbeitsmedizinischen Analysen von Wearable-Rohdaten stellt und erhebliche Überzeugungsarbeit erfordert, dies der Belegschaft auch zu vermitteln.

Die hier beschriebenen Einschränkungen begrenzen derzeit noch die Möglichkeiten, dauerhaft tragfähige Geschäftsmodelle für Wearable-basierten Arbeits- und Gesundheitsschutz auf breiter Front zu etablieren.



Quellenverzeichnis

[1] TrUSD (2018–2021): Projektwebseite. HK Business Solutions GmbH https://www.trusd-projekt.de/ [zuletzt besucht am 25.10.2024]

[2] D'Accord (2021–2024): Projektwebseite. HK Business Solutions GmbH https://daccord-projekt.de/ [zuletzt besucht am 25.10.2024]

[3] PERISCOPE (2021–2024): Projektwebseite. Fraunhofer-Institut für Arbeitswirtschaft und Organisation http://periscope-projekt.de/ [zuletzt besucht am 13.11.2024]

[4] TESTER (2021–2024): Projektwebseite. Fraunhofer-Institut Arbeitswirtschaft und Organisation https://www.tester-projekt.de/ [zuletzt besucht am 13.11.2024]

[5] InviDas (2020–2023): Projektwebseite. Gesellschaft für Informatik e.V. https://invidas.gi.de/ [zuletzt besucht am 25.10.2024]

[6] Pantelopoulos, Alexandros & Bourbakis, Nikolaos G. (2010): A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis. IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews 40(1), pp. 1–12 https://doi.org/10.1109/TSMCC.2009.2032660 [zuletzt besucht am 25.11.2024]

[7] Svertoka, Ekaterina & Saafi, Salwa & Rusu, Alexandru & Burget, Radim & Ion, Marghescu & Hosek, Jiri & Ometov, Aleksandr (2021). Wearables for Industrial Work Safety: A Survey. Sensors 21(11) https://doi.org/10.3390/s21113844 [zuletzt besucht am 25.11.2024]

[8] Tindale, Lauren & Chiu, Derek & Minielly, Nicole & Hrincu, Viorica & Talhouk, Aline & Illes, Judy (2022). Wearable Biosensors in the Workplace: Perceptions and Perspectives. Frontiers in Digital Health 4 https://doi.org/10.3389/fdgth.2022.800367 [zuletzt besucht am 25.11.2024]

[9] Jannis von Albedyll, Reinhard Schwarz (2022): State-of-the-Art-Bericht zu Privacy-UIs. Ergebnisbericht D4.1, Projekt WearPrivate, Fraunhofer IESE, Kaiserslautern https://www.wearprivate.de/deliverables.html [zuletzt besucht am 17.12.2024]

[10] Simone Salemi (2024): Bericht über ethische, rechtliche und soziale Implikationen der Projektergebnisse. Ergebnisbericht D2.1, Projekt WearPrivate, Universität des Saarlandes, Saarbrücken

[11] Reinhard Schwarz (2022): Threat Analysis and Security Requirements Elicitation. IESE-Report Nr. 009.22/E, Fraunhofer IESE, Kaiserslautern

[12] Svenja Polst, Philipp Neuschwander, Reinhard Schwarz, Bianca Steffes, Simone Salemi (2024): Anforderungsdokument. Ergebnisbericht D1.1, Projekt WearPrivate, Kaiserslautern – Saarbrücken https://www.wearprivate.de/deliverables.html [zuletzt besucht am 17.12.2024]

[13] Loren Kohnfelder and Praerit Garg (1999): The threats to our products. Microsoft Interface https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx [zuletzt besucht am 10.06.2024]

[14] MYDATA Control Technologies (2024): Projektwebseite. Fraunhofer IESE, Kaiserslautern https://www.mydata-control.de [zuletzt besucht am 02.01.2025]

[15] MYDATA Control Technologies (2024): IND²UCE vs. MYDATA Control Technologies. Projektwebseite, Fraunhofer IESE, Kaiserslautern https://developer.mydata-control.de/release-notes/mydata-branding.html [zuletzt besucht am 02.01.2025]

[16] Erik Rissanen (editor) (2013): eXtensible Access Control Markup Language (XACML) Version 3.0. OASIS Standard https://www.oasis-open.org/standard/xacmlv3-0/ [zuletzt besucht am 02.01.2025]

[17] Feth, D., Jung, C. (2019): 10 Jahre Forschung zu Datennutzungskontrolle am Fraunhofer IESE. https://www.iese.fraunhofer.de/blog/10-jahre-datennutzungskontrolle-am-fraunhofer-iese/ [zuletzt besucht am 08.01.2025]

[18] Bianca Steffes, Philipp Neuschwander, Marcus-Sebastian Schröder (2024): Konzepte für Anonymisierung und Datennutzungskontrolle. Ergebnisbericht D3.2, Projekt WearPrivate, Saarbrücken – Kaiserslautern – Bremen
https://www.wearprivate.de/deliverables.html [zuletzt besucht am 17.12.2024]

[19] Marcus-Sebastian Schröder, Reinhard Schwarz, Philipp Neuschwander, Bianca Steffes, Ajla Hajric, Esteban Bayro-Kaiser (2024): IT-Sicherheitsarchitektur und Datenschutzkonzept. Ergebnisbericht D3.1, Projekt WearPrivate, Bremen – Kaiserslautern – Saarbrücken
https://www.wearprivate.de/deliverables.html [zuletzt besucht am 17.12.2024]

[20] Marcus-Sebastian Schröder, Philipp Neuschwander (2024): Konzeption des Hauptdemonstrators. Ergebnisbericht D3.3, Projekt WearPrivate, Bremen – Kaiserslautern
https://www.wearprivate.de/deliverables.html [zuletzt besucht am 17.12.2024]

[21] Bianca Steffes, Reinhard Schwarz, Marcus Schröder, Jule Marie Hucke (2024): Evaluationsbericht. Ergebnisbericht D6.1, Projekt WearPrivate, Saarbrücken –Kaiserslautern – Bremen
https://www.wearprivate.de/deliverables.html [zuletzt besucht am 17.12.2024]

[22] Holohan, Naoise; Braghin, Stefano; Mac Aonghusa, Pol and Levacher, Killian (2019): Diffprivlib: the IBM differential privacy library
https://arxiv.org/abs/1907.02444 [zuletzt besucht am 25.11.2024]

[23] Irurzun, I. M., Garavaglia, L., Defeo, M. M., & Thomas Mailland, J. (2021): RR interval time series from healthy subjects (version 1.0.0). *PhysioNet*
https://doi.org/10.13026/51yd-d219 [zuletzt besucht am 25.11.2024]

[24] Saskia Koldijk, Maya Sappelli, Suzan Verberne, Mark A. Neerincx, and Wessel Kraaij (2014): The SWELL Knowledge Work Dataset for Stress and User Modeling Research. In: Proceedings of the 16th International Conference on Multimodal Interaction (ICMI '14). Association for Computing Machinery, New York, NY, USA, pp. 291–298
https://doi.org/10.1145/2663204.2663257 [zuletzt besucht am 25.11.2024]

[25] Boris Otto et al. (2016): Industrial Data Space. White Paper, Fraunhofer-Gesellschaft, München
https://www.dataspaces.fraunhofer.de/content/dam/isst/publikationen/StudienundWhitePaper/Industrial-Data-Space_whitepaper.pdf [zuletzt besucht am 31.11.2024]

[26] Internation Data Spaces (2024): Home-Page, Fraunhofer-Gesellschaft, München
https://www.dataspaces.fraunhofer.de/de/InternationalDataSpaces.html [zuletzt besucht am 31.11.2024]

[27] Sebastian Steinbuss (ed.) (2019): Reference Architecture Model, Version 3.0. International Data Spaces Association, Dortmund
https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf [zuletzt besucht am 31.11.2024]

[28] K. Müller, M. Paulitsch, R. Schwarz, S. Tverdyshev und H. Blasum (2012): MILS-based information flow control in the avionic domain: A case study on compositional architecture and verification. In: Proceedings 31st Digital Avionics Systems Conference (DASC), Williamsburg, Virginia, October 2012, pp. 7B1-1–7B1-13
https://doi.org/10.1109/DASC.2012.6382411 [zuletzt besucht am 31.11.2024]

[29] WearPrivate (2021–2024): Projektwebseite. Universität des Saarlandes, Saarbrücken
https://www.wearprivate.de/ [zuletzt besucht am 31.11.2024]

[30] Bianca Steffes, Christian K. Bosse, Aljoscha Dietrich, Hartmut Schmitt (2022). Einwilligung oder Anonymisierung? Rechtliche Implikationen der Datenverarbeitung im Beschäftigungskontext. In: Recht DIGITAL – 25 Jahre IRIS: Tagungsband Internationales Rechtsinformatik Symposion (IRIS 2022), Österreichische Computer Gesellschaft https://www.uni-saarland.de/fileadmin/upload/lehrstuhl/sorge/Paper-Downloads/IRIS22_Steffes.pdf [zuletzt besucht am 25.10.2024]

[31] Simone Salemi, Nils Wiedemann (2023): Die europäische Datenstrategie und das Datenschutzrecht: Abgrenzungsschwierigkeiten Data Act und Data Governance Act zur DSGVO. In: Tagungsband des 26. Internationalen Rechtsinformatik Symposions (IRIS 2023), Österreichische Computer Gesellschaft https://www.uni-saarland.de/fileadmin/upload/lehrstuhl/sorge/Paper-Downloads/47_iris_2023_Salemi_Wiedemann.pdf [zuletzt besucht am 25.10.2024]

[32] Simone Salemi, Nils Wiedemann (2023): Die europäische Datenstrategie und das Datenschutzrecht: Das Verhältnis von Daten-Governance-Gesetz und Datengesetz zur DSGVO. Tagungsband Internationales Rechtsinformatik Symposion (IRIS 2023), Jusletter IT, 27. April 2023 https://jusletter-it.weblaw.ch/en/issues/2023/27-April-2023/die-europaische-date_6b6d92be07.html__ONCE [zuletzt besucht am 19.11.2024]

[33] Ajla Hajric und Simone Salemi (2023): Können Datenschützer aus Konzepten des sexuellen Konsenses lernen? Datenschutz und Datensicherheit - DuD, 48/3, pp. 177–182 https://doi.org/10.1007/s11623-023-1903-9 [zuletzt besucht am 19.11.2024]

[34] Technische Informationsbibliothek (TIB). Hannover https://www.tib.eu/ [zuletzt besucht am 19.11.2024]

[35] Simone Salemi, Bianca Steffes und Nils Wiedemann (2023): Data Sharing im Kontext digitaler Selbstvermessung. Poster Präsentation, Jahreskonferenz Forum Privatheit 2023: Data Sharing – Datenkapitalismus by Default? https://plattform-privatheit.de/p-prv/jahreskonferenzen/jahreskonferenz-2023.php [zuletzt besucht am 19.11.2024]

[36] Fraunhofer IESE und Fraunhofer IAO (2023): Datenökonomie trifft Datenschutz. Berlin, Fraunhofer-Forum https://www.iese.fraunhofer.de/de/veranstaltungen_messen/2023/datenschutzoekonomie2023.html [zuletzt besucht am 25.10.2024]

[37] KickStartTrustee (2022–2023): Projektwebseite. Fraunhofer IESE https://www.kickstarttrustee.de/ [zuletzt besucht am 25.10.2024]

[38] Jule Marie Hucke, Jan-Niclas de Vries (2025): Asana Ai Swift & Sense – A System to Support Yoga Practitioners by Using Machine Learning Algorithms and Feasible Feedback Channels. Masterarbeit, Bremen [in Vorbereitung]