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

Ergebnisbericht D1.1

Anforderungsdokument

Version	2.0
Datum	19.07.2024
Verfasser	Svenja Polst (IESE) Philipp Neuschwander (IESE) Reinhard Schwarz (IESE) Bianca Steffes (UdS) Simone Salemi (UdS)

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KIS1511K gefördert.

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

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Ansprechperson

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

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

Inhaltsverzeichnis

Liste der Abkürzungen

BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
DiGA	Digitale Gesundheitsanwendungen
DiPA	Digitale Pflegeanwendungen
DSGVO	Datenschutzgrundverordnung
HR	Herzrate
HRV	Herzratenvariabilität
HSE	Health, Safety & Environment
KI	Künstliche Intelligenz
SMART	Specific, Measurable, Attainable, Result-Based, and Time-Bound
TARA	Threat Analysis and Risk Assessment

1 Über dieses Dokument

Dieses Dokument gibt einen Überblick über die Anforderungsanalyse-Aktivitäten im WearPrivate-Vorhaben, um am Beispiel des ausgewählten Hauptdemonstrators den Weg vom Wearable-Anwendungsfall zu einer entsprechenden Anforderungsspezifikation für eine Wearable-Anwendung im Arbeitsplatzkontext zu skizzieren. Das Dokument wurde von Projektsprint zu Projektsprint fortgeschrieben, um den Erkenntnisgewinn und den Projektfortschritt von Iteration zu Iteration widerzuspiegeln.

Kapitel 2 vermittelt Hintergrundinformationen zu Wearables und ihrem Einsatz am Arbeitsplatz in bestehenden Geschäftsmodellen.

Kapitel 3 beschreibt die Anwendungsfälle, die im Projekt genauer betrachtet wurden. Diese stammen vom Projektpartner WearHealth.

In Kapitel 4 werden die relevanten Stakeholder vorgestellt, die zusammen mit den Anwendungspartnern WearHealth und Ambiotex erhoben wurden.

Kapitel 5 verweist auf die rechtlichen Rahmenbedingungen des Wearable-Einsatzes am Arbeitsplatz und umreißt wesentliche Anforderungen an solche Systeme. Eine detailliertere Analyse dazu findet sich im Ergebnisbericht D 2.1.

Kapitel 6 widmet sich ausführlich möglichen Datenschutzproblemen und skizziert dazu Lösungsideen. Diese Problemfälle, deren Lösungsanforderungen und Lösungsideen wurden im Konsortium erarbeitet.

Einige der Probleme wurden bereits vom Anwendungspartner WearHealth validiert, andere jedoch noch nicht. Die Validierung sollen im Rahmen des Vorhabens durch Befragungen der Stakeholder ergänzt werden. Dabei sollen weitere Anforderungen verschiedener Stakeholder erhoben werden.

Kapitel 7 beschreibt, welche Informationen von welchem Stakeholder erhoben werden sollten, um die Anforderungsspezifikation für die gewählte Demonstratoranwendung zu vervollständigen und zu verfeinern.

Kapitel 8 fasst die verdichteten Anforderungen für den Anwendungsfall »Belastungsmessung« zusammen. Dieser Anwendungsfall wurde von den Projektpartnern als Demonstrator-Anwendungsfall ausgewählt. Das Kapitel beschreibt eine Vorgehensweise, um Datenschutz- und Sicherheitsanforderungen an den Anwendungsfall oder ähnliche Wearable-Anwendungen systematisch zu ermitteln und deren Stimmigkeit und Vollständigkeit zu überwachen. Die mit dieser Vorgehensweise erhobenen Bedrohungen, Ziele und Anforderungen werden tabellarisch aufgelistet und miteinander in Beziehung gesetzt.

2 Wearables im Kontext Arbeitssicherheit

Dieses Kapitel liefert Hintergrundinformationen bezüglich Wearables im Arbeitssicherheitskontext. Diese Informationen sollen zu einem gemeinsamen Verständnis des Projektkontexts im Projektkonsortium beitragen. Ein gemeinsames Verständnis des Kontexts ist Voraussetzung, um die Besonderheiten des Datenschutzes in diesem Kontext herausarbeiten zu können.

Zunächst gehen wir auf Wearables im Allgemeinen ein und dann spezifisch auf die Eigenschaften der Wearables des Projektpartners WearHealth und des ausgeschiedenen Projektpartners Ambiotex.

2.1 Definition und Beschreibung

Wearables lassen sich in etwa wie folgt charakterisieren:

> „Wearables sind Computertechnologien, die man am Körper oder am Kopf trägt. Sie sind eine Konkretisierung des Ubiquitous Computing, der Allgegenwart der Datenverarbeitung, und ein Teil des Internets der Dinge. Man spricht auch von Wearable Technology und vom Wearable Computer. Sinn und Zweck ist meist die Unterstützung einer Tätigkeit in der realen Welt, etwa durch (Zusatz-)Informationen, Auswertungen und Anweisungen. Wearable Computing ist das entsprechende Gebiet, mit dem sich die gleichnamige Disziplin der Informatik zusammen mit der Mensch-Maschine-Interaktion befasst. Elektrotechnik, Designtheorie und Künstliche Intelligenz (KI) spielen ebenfalls eine Rolle. Wesentlich für Wearables sind eine hochentwickelte Sensorik, eine permanente Verarbeitung von Daten und ein akuter Support des Benutzers.“ [1]

Bei der Nutzung von Wearables im Arbeitskontext werden personenbezogene Daten erfasst, was mögliche Datenschutzimplikationen zur Folge hat.

Wearables können auf verschiedene Weisen getragen werden:

- Gebrauchsgegenstand mit integrierter Sensorik: Die Sensorik kann zum Beispiel in eine Armbanduhr integriert sein. Man spricht dann von sogenannten Smartwatches.
- Dediziertes Gerät: Die Sensorik wird über ein extra dafür entwickeltes Gerät verfügbar gemacht. Das Gerät kann zum Beispiel über Druckknöpfe an einem Brustgurt oder einem speziellen T-Shirt angebracht werden. Auch eine Art Pflaster kann zum Befestigen am Körper verwendet werden. Die Wahl der Befestigung hängt vom Körperbau ab. Bei Frauen mit viel Oberweite hält der Gurt vermutlich besser die Position als ein T-Shirt. Älteren Menschen ist dagegen ein Shirt vermutlich zu eng.

2.2 Messgrößen und Datenauswertung

Typische Messgrößen, die durch die Sensorik erfasst werden, sind:

- Herzratenvariabilität (HRV)
- Beschleunigung
- Aufenthaltsort (meist GPS)

Aus der Herzratenvariabilität und der Beschleunigung können Erkenntnisse gewonnen werden über:

- Art der Aktivität (z. B. Laufen, Klettern)

[1] Quelle: https://wirtschaftslexikon.gabler.de/definition/wearables-54088

- Atemfrequenz
- Belastungslevel / Stresslevel
- Herzfrequenz
- Schlafphasen
- Schrittanzahl
- Trainingsbereitschaft des Körpers
- Vorhofflimmern (Voraussetzung: Sensorik, die als Medizingerät zugelassen ist)

Die meisten Wearables bieten nicht genug Rechenleistung, um komplexe Datenauswertungen durchzuführen. Die Daten müssen daher für die Auswertung auf ein anderes Gerät übertragen werden, zum Beispiel auf Server-Systeme in einer Cloud. Da die Wearables zudem nur über begrenzte Batteriekapazität verfügen, übermitteln sie ihre Daten in der Regel mittels eines energieeffizienten Übermittlungsstandards wie etwa Bluetooth Low Energy (BLE). Da solche Standards nur eine begrenzte Sendereichweite ermöglichen, muss oft noch ein Zwischengerät zum Auslesen der Daten und zu deren Übermittlung mit einem Weitbereichs-Kommunikationsstandard genutzt werden, zum Beispiel ein Smartphone oder eine Basisstation mit einer Verbindung zu einem lokalen Netz oder zum Internet.

Eine Datenverarbeitung im Projektkontext könnte also wie folgt aussehen: Die Daten werden vom Wearable erhoben. Danach werden sie drahtlos an eine Smartphone-App übertragen. Von dort werden sie in die Cloud übermittelt, wo eine detaillierte Auswertung erfolgt, etwa mittels KI-Methoden. Die Ergebnisse der Auswertung gehen zurück an den Arbeitnehmer. Möglicherweise erhält auch der Arbeitgeber Ergebnisdaten.

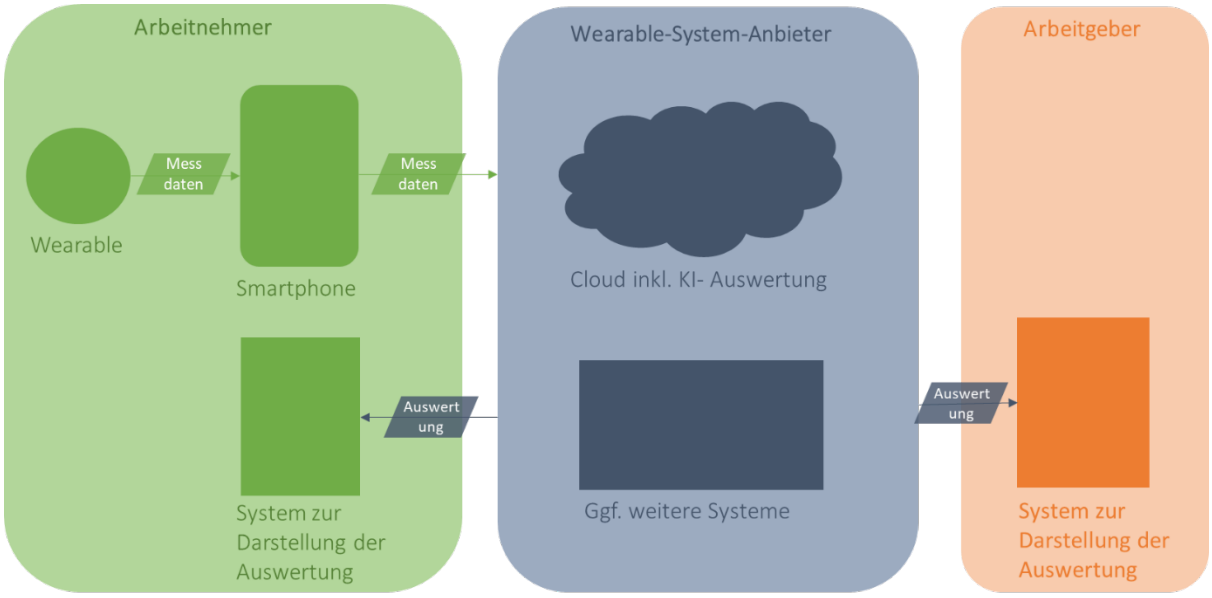

Abbildung 1 Abstrakte Darstellung eines Wearable-Systems

2.3 Geschäftsmodell

Das Geschäftsmodell kann je nach Wearables-System-Anbieter unterschiedlich gestaltet sein. Daher wird an dieser Stelle nur auf die Value Proposition eingegangen, die nach aktuellem Kenntnisstand bei den meisten Systemanbietern ähnlich gestaltet ist. Die Value Proposition ist sozusagen die Sammlung der Mehrwerte für die Kunden. Als Kunden kann man sowohl die Arbeitgeber als auch seine Beschäftigten betrachten.

Mehrwerte für den Arbeitgeber:

- Sicherstellung der Arbeitssicherheit:
    - Prävention von Überbelastung
    - Prävention von Verletzungen
    - Hilferuf bei Notfall
- Effizienzsteigerung der Prozesse

Mehrwerte für die Beschäftigten:

- Früherkennung von Erkrankungen und gegebenenfalls Vorschlag von Präventivmaßnahmen zur Verhinderung von Erkrankungen durch dauerhafte Fehlbelastung
- Prävention von Überlastung
- Prävention von Verletzungen

Daneben wären grundsätzlich noch weitere Mehrwerte vorstellbar, die aber derzeit noch kaum kommerziell ausgeschöpft werden, etwa

- Gutschriften für gesundheitsförderliches und gefahrenbewusstes Verhalten, zum Beispiel im Rahmen eines Bonus-Programms des Arbeitsgebers oder einer Krankenkasse.
- Beweissicherung im Falle eines Arbeitsunfalls, um zu belegen, dass eine Schädigung tatsächlich im Kontext des Arbeitsverhältnisses eingetreten ist.

2.4 Wearables beim Anwendungspartner WearHealth

WearHealth setzt Smartwatches und Gurte von Polar ein. Ob ein Gurt oder eine Smartwatch eingesetzt wird, hängt vom Anwendungsfall und vom Auftraggeber ab. So zählen etwa Armbanduhren bei einigen Unternehmen als Schmuck und sind daher aus Sicherheitsgründen nicht zugelassen.

Die Daten werden durch die Sensoren im Wearable erfasst und auf ein Smartphone übertragen. Vom Smartphone werden sie in eine Cloud geladen, wo Machine-Learning-Algorithmen die Daten analysieren. Die erste Version des Algorithmus wurde in Bremen im Labor entwickelt. Später wurde der Algorithmus auf die Industrie angepasst und verbessert.

Der Algorithmus wurde darauf trainiert, die Muster der HRV zu bewerten hinsichtlich des "fight or flight"-Modus. Anhand der Muster lässt sich die Art der Belastung – kognitiv oder physisch – ablesen.

2.4.1 Messgrößen & Messungen

Die Messgrößen sind:

- Herzratenvariabilität
- Körperbeschleunigung

Location Tracking wird in den meisten Fällen nicht verwendet.

Die Daten aus den Wearables werden kontinuierlich erfasst (z. B. mit einer Abtastrate von100Hz). Die Cloud liefert alle 30 Sekunden einen Belastungswert auf Basis von 5-Minuten-Datenpaketen.

Um bestmögliche Ergebnisse zu erzielen, sollte das System auf die spezifische Konstitution der Person eingemessen werden. Für diese Baseline-Messung gilt idealerweise:

- Sie sollte mehrere Male durchgeführt werden (morgens früh).
- Die Baseline wird über den Tag optimiert

Das Problem bei einer solchenKalibrierung außerhalb eines klinischen Umfelds besteht darin, dass manche Nutzer den Test beim Autofahren durchführen oder Randfälle beim Schlafen wählen. Das verfälscht das Ergebnis. Daher ist der Nutzen einer Kalibrierung, die nicht medizinisch überwacht wird, umstritten und manche Anbieter verzichten darauf.

2.4.2 Datenauswertung

Trainingsdaten:

- Die verwendeten Machine-Learning-Modelle wurden zunächst von WearHealth selbst trainiert.
- Durch Nutzer werden weitere Trainingsdaten erzeugt. Nutzer bewerten dazu subjektiv ihren Zustand.

Die Aufbereitung der Daten liefert Ergebnisse über die physische und mentale Belastung auf einer Skala von 1 bis 10 in Form einer PDF-Datei, die vom Betroffenen heruntergeladen und geteilt werden kann. Die Daten sind grafisch aufbereitet. Die genaue Aufbereitung wird auf das Unternehmen und den Anwendungsfall angepasst. Zum Beispiel wird angepasst, ob die Ergebnisse für eine Einzelperson oder für eine Gruppe von Personen wiedergegeben werden. Eine Entscheidung für Gruppen fällt unter anderem, um die Daten zu anonymisieren. Die Mindestgrenze zur Aggregation von Daten hängt von den Unternehmen ab. Sie beruht derzeit nicht auf einer strengen wissenschaftlichen Grundlage. Bei einigen Auftraggebern gilt eine Aggregation ab 5 Personen als anonym, bei anderen eher ab 10 Personen.

2.4.3 Einführung beim Auftraggeber

Jemand im Unternehmen muss für den Aufnahmeprozess zuständig sein, also dafür, den Wearable-Einsatz zu organisieren, ihn mit den Nutzern abzusprechen und die Nutzungszeiträume mit den Betroffenen zu klären. Diese Person ist *nicht* für Datenschutzfragen zuständig.

Seit Corona werden die Wearables von WearHealth nur noch zugesendet. Die Einrichtung für die Betroffenen ist einfach: Es genügt, die zugehörige App auf das Smartphone herunterzuladen.

2.4.4 Geschäftsmodell

Der Kern des Geschäftsmodells von WearHealth liegt in der Datenauswertung, also in der Bereitstellung der Machine-Learning-Modelle. WearHealth kauft die Wearables ein und stellt sie dem Auftraggeber zur Verfügung. Zudem berät WearHealth den Auftraggeber bezüglich der durchzuführenden Messungen und passt die Datenauswertung und Ergebnisdarstellung an die Bedürfnisse des Auftraggebers an.

2.5 Wearables beim Anwendungspartner Ambiotex

Da Ambiotex aus dem Projektkonsortium ausgeschieden ist, ist die Beschreibung des Wearable-Systems weniger umfangreich als beim verbleibenden Projektpartner WearHealth.

Ambiotex war Anbieter von einem Wearable, das an einem Gurt oder einem speziellen Shirt in der Nähe des Herzens angebracht werden konnte. Die Herzratenvariabilität (HRV) war die wichtigste Messgröße für Ambiotex. Mittels HRV konnten folgende Informationen ermittelt werden:

- Genereller Verfassungszustand des Nervensystems (ermittelt durch HRV Snapshot)
- Stress
- Vorhofflimmern
- Trainingsbereitschaft des Körpers
- Evtl. auch weitere abgeleitete Informationen, die heute noch nicht bekannt sind

HRV kann mit dem Sensor durchgehend im Alltag gemessen werden. Daher lassen die Daten bessere Interpretationen zu als ab und zu ein EKG durchzuführen, wie es im medizinischen Kontext üblich ist.

Die Daten wurden von einer KI analysiert. Die Trainingsmodelle wurden mit öffentlich verfügbaren Daten gefüttert. Ambiotex plante eine eigene Studie durchzuführen, bei der Daten erhoben und von Kardiologen bewertet werden. Die Daten lagen auf eigenen Servern.

Abbildung 2 Wearable-System von Ambiotex

3 Anwendungsfälle

Im Projekt wurden vier Anwendungsfälle ausgewählt, die als Grundlage dienen, um praxisnahe Datenschutzmaßnahmen zu entwickeln. Die Anwendungsfälle stammen von WearHealth.

3.1 Belastung im Manufacturing-Bereich

ID	AF1
Name	Belastung im Manufacturing-Bereich
Beschreibung	**Analyse Teil 1:** • Identifizieren der belastendsten Arbeitsstationen • »Profil« pro Arbeitsstation in einer Art Ampelbewertung **Analyse Teil 2:** • wie performen die jeweiligen MA unter der jeweiligen Belastung • der Einzelscore der Mitarbeitenden kann betrachtet werden, um deren Einsatz im Unternehmen zu optimieren (z. B.: MA1 passt nicht so gut zu Station1 aber dafür sehr gut an Station4). • Mitarbeiter können auch selbst auf Basis der Daten sagen, dass sie gerne woanders eingesetzt werden möchten.
Daten	HRV/HR/Bewegungsdaten
Auswertung	Teil 1: Individuelle Auswertung Teil 2: aggregierte Auswertung
Verwendungszweck	Belastung messen Überbelastung vermeiden
Datennutzer	Arbeitnehmer, Teamleiter, Manager
Messzeitraum für Auswertung	Über mehrere Tage
Baseline-Messung	Nach Möglichkeit gleich nach dem Aufwachen.
Feedback	Auswertung nach Ende des Messzeitraums
Wearable	Gurt oder Smartwatch
Umgebung	Werksgelände, bisher Tests nur außerhalb von Deutschland. Realistisch in DE, wird hier jedoch aus Datenschutzgründen nicht gemacht
Mehrwert für Arbeitnehmer	Bessere Arbeitsbedingungen, sichereres und gesünderes Arbeiten
Mehrwert für Arbeitgeber	Engagement der Belegschaft, weniger Ausfallzeiten, Steigerung der Produktivität

3.2 Belastung in Risikosituation

ID	AF2
Name	Belastung in Risikosituation
Beschreibung	System analysiert Belastung (kognitiv und physisch). Bei hoher Belastung bekommt der Nutzer eine Mitteilung darüber, dass eine hohe Belastung vorliegt → Awareness schaffen, dass aktuell ein höheres Sicherheitsrisiko besteht. Betroffene entscheiden selbst, wie sie vorgehen. Mögliche Reaktion ist ein eine kurze Reflektion der Situation oder eine kurze Pause, um der Belastung entgegenzuwirken.
Daten	HRV/HR/Bewegungsdaten
Auswertung	individuelle Auswertung
Verwendungszweck	• Awareness für hohe Belastung • Prävention von Gefahrensituationen
Datennutzer	Arbeitnehmer, Teamleiter
Messzeitraum für Auswertung	Kontinuierlich bei der Arbeit (Bei risikoreichen Tätigkeiten)
Baseline-Messung	Nach Möglichkeit gleich nach dem Aufwachen.
Feedback	Direktes Feedback bei hoher Belastung
Wearable	Gurt (Uhr ist nicht zugelassen in dieser Umgebung)
Umgebung	Hochspannungsanlagen z. B. von EON Deutschland
Mehrwert für Arbeitnehmer	Sichereres und gesünderes Arbeiten
Mehrwert für Arbeitgeber	Engagement der Belegschaft, verbesserte Sicherheit, weniger Ausfallzeiten, höhere Produktivität

3.3 Lokalisierung

ID	AF3
Name	Lokalisierung
Beschreibung	Lokalisierung für Routenoptimierung; Tracking von Aktivitäten für Methods-Time Measurement; Zugangskontrolle und Nachverfolgbarkeit von Aufgaben
Daten	GPS
Auswertung	individuelle Auswertung

Verwendungszweck	• Routenoptimierung • Zugangskontrolle • Prävention von Gefahrensituationen
Datennutzer	Teamleiter, Manager
Messzeitraum für Auswertung	Kontinuierlich
Baseline-Messung	— keine —
Feedback	beim Betreten von Risikozonen
Wearable	Smartwatch oder Smartphone
Umgebung	Werksgelände (irgendwo, wo Arbeitnehmer überhaupt nicht oder nicht zu einer gewissen Zeit sein sollte). zB. ABB Deutschland
Mehrwert für Arbeitnehmer	Sichereres Arbeiten
Mehrwert für Arbeitgeber	Verbesserte Sicherheit, höhere Produktivität

3.4 Ermüdungsmessung

ID	AF4
Name	Ermüdungsmessung
Beschreibung	Ermüdungserscheinungen von LKW-Fahrern werden gemessen, so dass schon vor Eintreten starker Müdigkeit eine Prognose über die Einsatzfähigkeit gegeben werden kann. Der Teamleiter kann präventive Maßnahmen ergreifen, etwa den Arbeitnehmer nicht fahren lassen. Übermüdete Arbeitnehmer haben ein Mittel an der Hand, um Müdigkeit gegenüber Teamleiter nachweisen zu können. Einschlafen während der Fahrt wird damit vorgebeugt. Konkrete Fälle: LKW-Fahrer in Kanada (siehe Ambiotex-Anwendungsfall), DHL in Deutschland und Bergbauminen in Brasilien und Chile.
Daten	HRV/HR/Bewegungsdaten
Auswertung	individuelle Auswertung
Verwendungszweck	Alarmieren: Prävention von Gefahrensituationen
Datennutzer	Arbeitnehmer, Teamleiter
Messzeitraum für Auswertung	Kontinuierlich (auch beim Schlafen)
Baseline-Messung	Daten müssen auch außerhalb der Arbeit gesammelt werden, etwa während des Schlafens für Baseline

Feedback	Zum einen akutes Feedback bei Ermüdung (Fahrer bekommt selbst Feedback über Ermüdung und hat objektiven Nachweis für Teamleiter, dass Pause nötig ist). Zum anderen bei kurzfristiger Einsatzplanung (Konsequenz: Fahrer darf Fahrt nicht antreten)
Wearable	Gurt oder Smartwatch
Umgebung	Straßen (Fernstraßen); Bergbauminen
Mehrwert für Arbeitnehmer	Sichereres und gesünderes Arbeiten
Mehrwert für Arbeitgeber	Prävention von Personenschäden, Produktionsstillstand. Im Bergbaubereich: Erhalt der Minenlizenz (diese kann bei hohen Unfallzahlen entzogen werden)

4 Stakeholder

Diese Stakeholder wurden in Gesprächen mit Ambiotex und WearHealth erhoben.

Entscheider über Einführung im Unternehmen:

- Betriebsrat
- IT-Security
- Finanzmanagement

Initiatoren

- HSE-Abteilung
- Betriebsarzt

Direkte Nutzer:innen des Systems und der Daten:

- Teamleiter / Manager
- »ausführende« Mitarbeitende / Teammitglieder außer Leiter
- In seltenen Fällen auch der Betriebsarzt

Sonstige:

- Ansprechpartner im Unternehmen für WearHealth

5 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen werden im Ergebnisbericht D 2.1 ausführlich beschrieben. Dieses Deliverable stellt unter anderem die Betroffenenrechte vor sowie die Rechtsgrundlagen für die Datenverarbeitung im Kontext der Arbeitssicherheit und von IoT-Geräten. Daneben nennt es erste konkrete Anforderungen, die beim Design der Anwendungsschnittstelle beachtet werden müssen. Zu diesen Anforderungen zählen etwa:

- Die Arbeitnehmer müssen angemessen aufgeklärt werden. Durch die Sammlung sensibler Gesundheitsdaten sind die Anforderungen diesbezüglich erhöht.
- Einwilligungen müssen schriftlich/elektronisch eingeholt werden aufgrund von § 26 Abs. 3 S. 2 BDSG.
- Aus den abgegebenen Einwilligungen der Arbeitnehmer muss hervorgehen, dass sie sich der Sensitivität der Daten bewusst sind.

Für nähere Details wird auf den Ergebnisbericht D 2.1 verwiesen.

6 Mögliche Probleme und Lösungsansätze

Wearables können den Beschäftigten und ihrem Arbeitgeber Mehrwerte bieten. Dafür müssen die Wearables von den Beschäftigten akzeptiert werden. Gründe für die Ablehnung der Wearables sind unter anderem Datenschutzbedenken. Ziel von WearPrivate ist es daher, Datenschutzbedenken auszuräumen und somit die Akzeptanz von Wearables zu fördern.

Datenschutzbedenken können sowohl aufgrund tatsächlicher Datenschutzmängel entstehen, aber auch aufgrund von lückenhaften oder falschen Informationen über die vorhandenen Datenschutzmaßnahmen. Anders formuliert: Auch der wahrgenommene Datenschutz muss betrachtet und gefördert werden, so dass letztendlich die Beschäftigten und ihre Interessensvertreter überzeugt sind, dass personenbezogene Daten gut geschützt sind.

6.1 Mangel an Transparenz und Selbstbestimmung und damit an Akzeptanz

Mangel an Informationen und Selbstbestimmungsmöglichkeiten können dazu führen, dass Wearables nicht in einem Unternehmen eingeführt werden. Wenn sie denn eingeführt wurden, kann es dennoch zur Ablehnung der Wearables kommen. Im Folgenden gehen wir auf mögliche Probleme ein und stellen entsprechend Lösungsideen vor. Die Probleme sind bisher nicht validiert.

6.1.1 Ablehnung der Wearable-Einführung

Informationsmangel kann dazu führen, dass Wearables überhaupt nicht in ein Unternehmen eingeführt werden. Können Datenschutzbedenken nicht widerlegt werden, so kann dies als Vorwand für die Ablehnung der Wearables herangezogen werden. Zudem können sich Entscheider unzureichend informiert fühlen und sich deshalb gegen die Einführung der Wearables aussprechen. Diese beiden Probleme werden ausführlicher vorgestellt:

Ablehnung der Entscheider: In einem Unternehmen entscheiden verschiedene Akteure darüber, ob Wearables eingesetzt werden. In der Regel sind unter anderem der Betriebsrat, die IT-Sicherheitsabteilung sowie die Geschäftsführung beteiligt. Der Betriebsrat prüft, ob der Datenschutz für die Belegschaft gegeben ist. Die IT-Sicherheitsabteilung prüft die technischen Sicherheitsmaßnahmen. Beide Entscheider möchten nicht einer Technologie zustimmen, die sie nicht überblicken können. Informationsmangel kann dazu führen, dass sie die Wearables »sicherheitshalber« ablehnen. Für Laien ist es zum Beispiel besonders schwer einzuschätzen, wie gut die verwendeten Anonymisierungsverfahren sind.

Datenschutz als Vorwand: Datenschutz kann als Vorwand dienen, um etwas nicht zu tun. Unternehmen weisen auf das (vermeintliche) Risiko der Verletzung des Datenschutzes und den Aufwand hin, der mit der Umsetzung der Datenschutzmaßnahmen und deren Überprüfung einhergeht. In Wirklichkeit spielen jedoch andere Interessen eine Rolle.

Ziel des Projekts WearPrivate ist es, dass die Hürden zur Sicherstellung des Datenschutzes gering sind und das Risiko einer Datenschutzverletzung realistisch eingeschätzt werden kann, so dass einer Einführung des Wearable-Systems aus Datenschutzsicht nichts im Wege steht.

6.1.1.1 Lösungsanforderungen

Die Entscheider erhalten leichtgewichtig alle Informationen, die sie brauchen, um eine fundierte Entscheidung über die Einführung des Systems zu treffen. Der Betriebsrat braucht ein grobes Verständnis der Technologie und ein detailliertes Verständnis über die vorgesehenen

Datenschutzmaßnahmen. Die IT-Sicherheitsabteilung braucht ein detailliertes technisches Verständnis des Systems und der Sicherheitsmaßnahmen.

Die wichtigsten Informationen sollten in schriftlicher Form vorliegen, so dass sie nachgelesen werden können und jeder Zugang zu denselben Informationen hat. Typische Fragen von Entscheidern können durch eine frühzeitige Informationsvermittlung vorweggenommen werden. Dennoch wird es stets individuelle Fragen von Entscheidern geben, die nicht vorhersehbar sind. Daher ist es wichtig, ein Format anzubieten, das dem Entscheider Antworten auf seine individuellen Fragen liefert.

6.1.1.2 Konkrete Lösungsideen

Die Informationen könnten in Form von FAQs, Checklisten oder anderen schriftlichen Handreichungen vermittelt werden. Zudem können sie in einer Veranstaltung vorgestellt werden, die eine Möglichkeit für Fragen über die Wearables und die Datenschutzmaßnahmen bietet.

6.1.1.3 Abgrenzung des Projektscopes

Das Problem der „Ausrede“ wird im Projekt nicht direkt angegangen, sondern eher indirekt. Durch das Bereitstellen der genannten Lösungsideen sollte der Spielraum für Ausreden eingegrenzt werden.

6.1.2 Ablehnung der Wearable-Nutzung nach Wearable-Einführung

Nach der Wearable-Einführung in einem Unternehmen kann es auch nachträglich noch zur Ablehnung kommen. In dieser Phase sind es die Beschäftigten selbst, die über den Erfolg der Wearables entscheiden.

Angst vor Unbekanntem: Die Belegschaft fühlt sich unsicher oder überfordert, da sie die Technologie nicht versteht. Die Konsequenz ist eine pauschale Ablehnung.

Befürchteter Datenmissbrauch: Die Beschäftigten befürchten, dass ihre Daten für Zwecke verwendet werden, die nicht ihrem Willen entsprechen. Manche befürchteten Zwecke sind jedoch technisch ausgeschlossen, da entsprechende Daten nicht erhoben werden oder nur anonymisiert ausgewertete werden.

Gefühlte Überwachung: Sozusagen eine Form der befürchteten Zwecke ist die befürchtete oder gefühlte Überwachung. Die Beschäftigten fühlen sich durch das Wearable überwacht, auch wenn keine Überwachung stattfindet. Es kann das Gefühl entstehen, dass der Aufenthaltsort durch Location Tracking oder die Arbeitsleistung durch körperliche Belastungswerte überwacht wird.

6.1.2.1 Lösungsanforderungen

Transparenz: Die genannten Fälle zeigen, wie wichtig es ist, Informationen bereitzustellen. Unter anderem sollten Betroffene über folgende Punkte informiert werden:

- Funktionsweise der Wearables (d.h. Systemkomponenten und ihr Zusammenspiel)
- Verwendete Daten und Maßnahmen zu deren Schutz (z. B. Verschlüsselung, Anonymisierung, Zugriffsschutz)
- Personenbezug der Daten
- Verwendungszweck der Daten und Datennutzer
- Erhebungsausschlüsse: Daten, die *nicht* erhoben oder verwendet werden, deren Verwendung jedoch von der Belegschaft unterstellt werden könnte
- Verwendungsausschlüsse: Zwecke, für die Daten ausdrücklich *nicht* verwendet werden, die jedoch von der Belegschaft unterstellt werden könnten

Empfehlenswert ist auch, die Belegschaft über ihre Rechte und den gesetzlich vorgeschriebenen Schutz ihrer Daten zu informieren:

- Rechte der Betroffenen, u.a. gemäß DSGVO
- Umsetzung der Betroffenenrechte

Die Beschäftigten sollten auch über die Vorteile der Wearables informiert werden, so dass sie eine Abwägung zwischen Datenschutzrisiken und Mehrwerten für sich und andere vornehmen können.

Selbstbestimmung: Den Beschäftigten sollte zudem die Kontrolle über ihre Daten ermöglicht werden. Ihr Recht auf Selbstbestimmung über ihre Daten kann unter anderem durch das Bereitstellen von Datenschutzeinstellungen ausgeübt werden.

6.1.2.2 Konkrete Lösungsideen bezüglich Transparenz

Interpretationshilfe: Zusammen mit den ausgewerteten Daten sollte eine Interpretationshilfe gegeben werden, so dass deutlich ist, was die Daten aussagen können und was sie nicht aussagen können. Diese Interpretationshilfe kann sowohl den Beschäftigten als auch Datennutzern dienen.

Kontextuelle Datenschutzerklärung: Datenschutzerklärungen geben Informationen darüber, welche Daten potenziell verwendet werden. Jedoch besteht häufig eine Informationslücke, da die Betroffenen nur schwer einschätzen können, welche Daten tatsächlich verwendet werden und wann diese verwendet werden. Eine sogenannte kontextuelle Datenschutzerklärung kann Abhilfe schaffen. Dabei wird im Kontext angegeben, welche Daten in der jeweiligen Situation für welche Zwecke verwendet werden. Zum Beispiel könnte beim Anlegen eines Wearables informiert werden, welche Daten erhoben und verarbeitet werden.

Datenauskunft: Die Beschäftigten sollten Einblick in die erhobenen Daten und die Datenauswertungen erhalten, um sich selbst ein Bild von den tatsächlich erhobenen Daten zu schaffen. Laut DSGVO haben sie das Recht auf eine Datenauskunft.

Nutzungshistorie: Die bereits verwendeten Daten können als eine Nutzungshistorie aufbereitet werden, aus der hervorgeht, wann die Daten für welchen Zweck von welcher Person oder Rolle verwendet wurden.

Feedback zur Aktivität des Wearables: Ein (Aktivitäts-)Indikator am Wearable selbst (LED o.ä.) zeigt an, ob gerade Daten erfasst oder verarbeitet werden. Alternativ könnte auch um Zustimmung gefragt werden, wenn die Aufzeichnung der Daten starten soll, oder die Aufzeichnung könnte manuell gestartet werden.

6.1.2.3 Konkrete Lösungsideen bezüglich Selbstbestimmung und Gefühl der Kontrolle

Deaktivierungsschalter: Die Abschaltung der Datenerhebung sollte mittels eines einfachen Schalters möglich sein, sofern sich die Betroffenen in einer gewissen Situation gegen die Datenerhebung entscheiden. Ein einfacher Knopf ist vor allem bei Wearables, die nicht so leicht wie eine Uhr abgelegt werden können, empfehlenswert.

Grundlage für Beschwerde schaffen: Eine vertragliche Zusicherung, dass aus den Wearable-Daten keine Nachteile erwachsen, schafft eine Grundlage für eine Beschwerde. Bestenfalls gibt es vertrauenswürdige Ansprechpartner, an den sich Betroffene wenden und ihre Bedenken vorbringen können.

Datenschutzeinstellungen: Die Beschäftigten sollten eine einfache Möglichkeit haben, ihr Einverständnis zur Verarbeitung bestimmter Daten zu geben. Umgesetzt werden könnte dies in Form

von Datenschutzeinstellungen, in denen Beschäftigte ihre Präferenzen wiedergeben können, auch bezüglich anderer Wahlmöglichkeiten, die die Datenverarbeitung betreffen. Wichtig ist hierbei, dass Einverständniserklärungen nur dann verwendet werden, wenn sie wirklich nötig sind und dass die Einstellungen per Default so nutzerfreundlich wie möglich sind. Die Datenschutzeinstellungen sollten aufgrund der begrenzten Bildschirmfläche nicht auf einer Smartwatch angeboten werden, sondern auf einem Gerät wie einem Smartphone, so dass die Datenschutzeinstellungen übersichtlich dargestellt werden können.

6.1.2.4 Abgrenzung des Projektscopes

Die Themen Transparenz und Selbstbestimmung spielen in dem Projekt eine wichtige Rolle. Die in diesem Kapitel beschriebenen Probleme und Lösungsideen werden daher tiefergehend betrachtet im weiteren Projektverlauf.

6.1.2.5 Herausforderungen bei der Umsetzung

Verständlichkeit vs. Korrektheit: Eine große Herausforderung bei der Umsetzung ist es, eine gute Balance zu finden zwischen der Verständlichkeit der Informationen, also einer laienverständlichen Sprache, und ihrer juristischen Korrektheit.

Aufwand vs. Vollständigkeit: Außerdem muss eine gute Balance zwischen akzeptablem Aufwand für das Konsumieren der Informationen und Vollständigkeit der benötigten Informationen gefunden werden. Unter anderem sollte geklärt werden, wie viele Informationen über die Nicht-Verwendung erforderlich sind und wie viele und welche Kontextinformationen über das Wearable-System benötigt werden, um die Informationen über die Datenverwendung zu verstehen.

Zentrale Darstellung aller Informationen vs. kleine Darstellungsfläche: Eine andere Herausforderung bezieht sich auf die Darstellung. Die konkreten Vorschläge für die Umsetzung, wie etwa die Nutzungshistorie und die Informationen über die Datenverwendung, können in einem Datenschutzcockpit gebündelt dargestellt werden. Somit wären alle Informationen an einem Ort einsehbar. Damit solch ein Cockpit übersichtlich ist und Details eingesehen werden können, braucht es eine relativ große Darstellungsfläche. Wearables wie Smartwatches haben jedoch nur ein kleines Display. Große Darstellungsflächen würde ein Laptop bieten, der jedoch von körperlich arbeitenden Beschäftigten, die typischerweise Wearables einsetzen, eher weniger oder überhaupt nicht verwendet wird. Ein Lösungsansatz kann die Aufteilung von Informationen in kleinere „Informationshappen“ sein, die auf einem Smartphone dargestellt werden. Dies dient dazu, die Darstellung nicht zu überfrachten und den Anwender nicht mit zu vielen Darstellungsdetails zu überfordern.

Informationsmenge und Detaillierungsgrad können im Sinne eines *Responsive Designs* auch an die Eigenschaften des Endgeräts angepasst werden. So kann die Darstellung auf einem Tablet-Computer umfangreicher ausfallen als auf einem Smartphone.

Sorgen nehmen vs. Sorgen wecken: Transparenz über die beteiligten Akteure und Systeme sollte eigentlich das Vertrauen in Datenschutzmaßnahmen und die beteiligten Akteure fördern. Jedoch könnten Beschäftigte durch ausführliche Informationen erst auf Akteure und Systemkomponenten wie eine KI stoßen, die ihr Misstrauen erregen. Transparenz kann unter Umständen Misstrauen fördern.

Restriktive Datenschutzeinstellungen vs. Nutzbarkeit der Auswertung: Um eine aussagekräftige Interpretation der Daten zu erreichen oder eine hinreichende Anonymisierung zu ermöglichen, braucht es eine bestimmte Datenmenge von einer bestimmten Anzahl von Beschäftigten. Wenn die Betroffenen die Möglichkeit haben, detaillierte Einstellungen vorzunehmen, besteht das Risiko, dass die Einstellungen sehr restriktiv gesetzt werden, so dass die Effektivität der Datenauswertung leidet.

6.2 Datenerhebung

Im Projekt WearPrivate treffen zwei Problemkreise im Bereich des Datenschutzrechts zusammen. So steht einerseits die Verarbeitung personenbezogener Daten im Beschäftigtenkontext unter erhöhten Rechtmäßigkeitsanforderungen. Andererseits steht auch die Verarbeitung von Gesundheitsdaten im Raum, wenn beispielsweise die Herzfrequenz der Arbeitnehmer aufgezeichnet wird. Auch die Verarbeitung besonders sensibler Daten, wie Gesundheitsdaten, ist nur unter besonderen Voraussetzungen möglich. Der erste Schritt der Verarbeitung ist die Erhebung der entsprechenden Daten. Bereits an diesem Punkt sollten Grundsätze der Datenverarbeitung wie Art. 5 Abs. 1 DSGVO beachtet und mögliche Ängste und Befürchtungen der Betroffenen ernst genommen werden.

6.2.1 Datenmenge

Ein erstes mögliches Problem besteht in der erhobenen Datenmenge. Gemäß dem Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c) DSGVO, dürfen nur so viele Daten erhoben werden, wie es für den Verarbeitungszweck angemessen und notwendig ist. Datenminimierung zielt auf die quantitative und qualitative Begrenzung der Daten ab: hinsichtlich der Menge, aber auch hinsichtlich der Art der Daten. Dabei muss die Frage gestellt werden, ob die Datenerhebung notwendig ist, um den zugrundeliegenden Zweck zu erreichen. Nur wenn diese zu bejahen ist, ist der Grundsatz der Datenminimierung eingehalten.[2]

Im Rahmen des Projekts WearPrivate muss darauf geachtet werden, dass der Grundsatz der Datenminimierung eingehalten wird. Dazu gehört einerseits, dass nicht zu viele Daten insgesamt erhoben werden, wenn auch eine geringere Menge ausreichend für die Zwecke der Verarbeitung ist. Andererseits muss auch darauf geachtet werden, dass keine Kategorie von Daten erhoben wird, die es für den Verarbeitungszweck nicht braucht. Beispielsweise bedarf es für die Analyse einer Arbeitsstation im Manufacturing-Bereich keiner durchgehenden Aufzeichnung des Standorts der Beschäftigten.

Auch wenn grundsätzlich die richtigen Daten erhoben werden, kann es zu Verstößen gegen den Grundsatz der Datenminimierung kommen. Wenn beispielsweise auch nach Feierabend Daten ohne triftigen Grund erhoben werden, wird eine größere Menge an Daten verarbeitet als erforderlich.

Jedoch kann es auch notwendig sein, viele Daten zu erheben. Wenn nur bei einer entsprechend großen Datenmenge eine angemessene und individuelle Interpretation der Daten möglich ist, kann das Problem kaum umgegangen werden. Jedoch ist es hier wohl einfacher möglich, die große Datenmenge zu rechtfertigen. Sind die Daten nämlich für den zugrundeliegenden Verarbeitungszweck notwendig, ist kein Verstoß gegen den Grundsatz der Datenminimierung anzunehmen.

Datenmenge und Datenqualität sind nicht nur aus rechtlicher Sicht problematisch, sondern auch für den gefühlten Datenschutz der Arbeitnehmer relevant. Für die Arbeitnehmer ist es wichtig zu wissen, dass nur die wirklich erforderliche Menge an Daten gesammelt wird und auch keine zusätzlichen Daten erhoben werden.

---

[2] FRENZEL in: Paal/Pauly, Art. 5 DSGVO Rn. 34.

6.2.1.1 Lösungsideen

Die Menge der gesammelten Daten sollte grundsätzlich reduziert werden. Dafür müssen die Verarbeitungszwecke zunächst genau benannt werden und es muss geprüft werden, welche Daten wirklich notwendig sind, um diese umzusetzen.

Ferner sollten Daten nur dann erhoben werden, wenn es wirklich notwendig ist. Hierfür kann es beispielsweise sinnvoll sein, zunächst solche Maßnahmen zu ergreifen, die keine Datenerhebung beim einzelnen Arbeitnehmer erfordern (Bsp.: Bewegungsmelder oder Zutrittskontrollen an gefährlichen Orten, um Arbeitsschutz zu gewährleisten).

Zudem ist eine erweiterte Beteiligung der Arbeitnehmer sinnvoll: Das Wearable kann so programmiert werden, dass immer dann, wenn eine Datenerhebung beginnt, eine Meldung angezeigt wird, die den Arbeitnehmer über diesen Umstand informiert. Dies gibt ihm die Möglichkeit, sich in der jeweiligen Situation selbstbestimmt für oder gegen die Datenerhebung zu entscheiden. Auf diese Weise kann verhindert werden, dass in Situationen Daten erhoben werden, in denen es nicht sinnvoll oder nicht notwendig ist. Dies führt zu einer angemessenen Reduzierung der Datenmenge.

6.2.1.2 Abgrenzung des Projektscopes

Zu beachten ist, dass das Problem der zu umfangreichen Datenerhebung in der Praxis weniger relevant ist als in der Theorie. Es gibt Daten und Analysen, die die eingesetzten Wearables gar nicht umsetzen oder durchführen können. Daher kann dieses Problem bereits dadurch umgangen werden, dass entsprechend sichere Wearables genutzt werden, bei denen die Datenmenge bereits konfigurationsbedingt technisch beschränkt werden kann.

6.2.2 Erhebung im privaten Raum

Eine letzte Herausforderung bei der Datenerhebung kann die Erhebung im privaten Raum der Arbeitnehmer sein. Es ist möglich, dass Baseline-Messungen in Ruhe oder direkt nach dem Aufstehen gemacht werden müssen. Auch ist es möglich, dass ein Wearable beim Schlafen getragen werden muss. Dies überschreitet die Grenze zur Privatsphäre der Betroffenen und es werden unter Umständen auch Daten von Dritten aus dem sozialen Umfeld der Beschäftigten erhoben.

6.2.2.1 Lösungsideen

Auch wenn die Datenerhebung im privaten Raum nicht gänzlich ausgeschlossen werden kann, sollte diese doch auf ein Mindestmaß beschränkt werden. Messungen sollten nur an bestimmten, ausgewählten Tagen stattfinden. Unter Umständen kann auch die Einrichtung eines Urlaubstages, an dem die Arbeitnehmer am Arbeitsplatz eine Baseline-Messung vornehmen können, sinnvoll sein. Weiterhin sollte die Messung im Schlaf möglichst vermieden werden. Messungen am Abend könnten noch tiefer in die Privatsphäre eindringen als Messungen zu anderen Tageszeiten.

Zudem kann versucht werden, die erhobenen Daten zu bereinigen und Daten Dritter herauszufiltern. So könnte verhindert werden, dass die Daten Dritter noch weiterverarbeitet werden. Diese Maßnahme ist zwar durchaus sinnvoll, löst jedoch das aufgeworfene Problem nicht. Werden die Daten herausgefiltert, ändert dies nichts an der Tatsache, dass die Daten bereits erhoben und damit im Sinne der DSGVO verarbeitet wurden. Es kann sich damit höchstens um eine Folgemaßnahme handeln. Es sollte jedoch an einem früheren Punkt angesetzt werden, um die Erhebung von Daten von Dritten zu adressieren.

Zudem wäre es auch sinnvoll, von Beginn an Aufklärung zu betreiben und einen Ansprechpartner für Fragen zur Verfügung zu stellen. Hierdurch bekommen die Arbeitnehmer und ihr soziales Umfeld ein

Gefühl dafür, welche Daten erhoben und verarbeitet werden und können einschätzen, wie sie das Tragen der Wearables im privaten Bereich anpassen wollen.

6.2.2.2 Abgrenzung des Projektscopes

Es handelt sich um eine rechtlich relevante Problematik, die im Projekt betrachtet wird, um Lösungen zu finden, die allen Interessen gerecht werden.

6.2.3 Nicht-Nutzung aufgrund mangelnden Tragekomforts

Ein weiteres Problem, das im Rahmen des Projekts relevant werden könnte, ist der fehlende Tragekomfort der Wearables, der dazu führen könnte, dass die Wearables nur ungern oder nicht durchgehend getragen werden, mit der Folge, dass keine Daten erhoben werden können. Mangelt es bereits am Tragekomfort der Wearables, wird es sehr schwer sein, diese zu etablieren. Die Wearables sollen bei der Verrichtung von Arbeit getragen werden, daher sollten sie den Arbeitnehmer nicht stören.

6.2.3.1 Lösungsideen

Dem Problem des mangelnden Tragekomforts kann nur dadurch entgehen, dass im Rahmen der Produktentwicklung besonders darauf geachtet wird und die Wearables auch einem »Stresstest« unterzogen werden, bei dem getestet wird, ob sie beim Arbeiten stören.

6.2.3.2 Abgrenzung des Projektscopes

Die beschriebene Problematik wird im Rahmen des Projekts nicht betrachtet mangels Einwirkungsmöglichkeiten auf die Produktentwicklung. Wir nehmen zudem an, dass dieser Fall selten eintritt, da hochwertige Wearables in der Regel gut anliegen und die Vorteile der Nutzung meist die Beeinträchtigungen durch mangelndes Tragegefühl aufwiegen. Es werden also keine eigenen Verbesserungsmaßnahmen im Rahmen dieses Projekts vorgenommen. Im Rahmen der Evaluation innerhalb des Projekts kann jedoch die Meinung der Teilnehmer zum Tragekomfort und der Auswirkungen eines mangelhaften Tragekomforts erhoben werden.

6.2.4 Verfälschung der Daten bei Erhebung

Ein weiteres Problem liegt in der möglichen Verfälschung der Daten. Zur Verfälschung zählen in diesem Fall sowohl die unabsichtliche als auch die absichtliche Verfälschung. Eine unabsichtliche Verfälschung der Daten könnte beispielsweise durch das Tragen des Wearables eines Kollegen eintreten oder auch durch die unabsichtlich falsche Nutzung des Wearables. Vorsätzliche Fälschungen können dann vorliegen, wenn absichtlich dafür gesorgt wird, dass Wearable-Daten der falschen Person zugeordnet werden. Denkbar ist auch der Eingriff in das Wearable selbst und damit die technische Manipulation der Daten.

6.2.4.1 Lösungsideen

Die praktische Bedeutung des beschriebenen Problems ist voraussichtlich gering. Die Verwechslung des Wearables mit dem eines Kollegen mag zwar grundsätzlich möglich sein, kommt jedoch in der Praxis nur äußerst selten vor. In der Regel ist das Wearable mit einer App auf dem Smartphone des jeweiligen Arbeitnehmers verbunden, weshalb sich sehr schnell herausstellen dürfte, dass eine Verwechslung vorliegt. Wenn aus diesem Grund nicht erklärbare, seltsame Daten entstehen sollten, würden diese herausgefiltert.

Des Weiteren ist zu beachten, dass der Eingriff in das Device selbst nur einer Person möglich ist, die besonders technikaffin ist. Daher ist auch mit einer absichtlichen Manipulation der Daten selbst wohl eher nicht zu rechnen.

Betrachtet werden sollte jedoch die Möglichkeit nicht-technischer Manipulationen der Prozesse. Hierfür kann es unterschiedliche Motivationen geben: Beispielsweise wäre an einen Arbeitnehmer zu denken, der sich aufgrund des sozialen Drucks gezwungen fühlt, entgegen seinem Willen an einer Datenerhebung am Arbeitsplatz teilzunehmen. Denkbar wäre auch, dass Arbeitnehmer die Messung absichtlich manipulieren, um Arbeitsschutzbeschränkungen (z. B. vorgeschriebene Ruhezeiten) zu umgehen. Ferner könnte die absichtliche Manipulation des Messprogramms durch einen engagierten Datenschützer in Betracht kommen.

Dem sozialen Druck sollte möglichst bereits im Vorhinein entgegengewirkt werden, sodass Arbeitnehmer selbstbestimmt der Teilnahme an der Datenerhebung zustimmen.

Dem Widerstand eines Datenschützers könnte man wohl nur dadurch effektiv entgegenwirken, dass die Datenverarbeitung selbst im Einklang mit datenschutzrechtlichen Regelungen steht. Stützt man die Datenverarbeitung nämlich auf eine Einwilligung, wären auch nur diejenigen Personen an der Datenverarbeitung beteiligt, die wirklich damit einverstanden sind.

6.2.4.2 Abgrenzung des Projektscopes

Die beschriebene Problematik ist praktisch gering und befindet sich daher außerhalb des Projektscopes.

6.3 Datenverarbeitung, Übertragung und Speicherung

Der Begriff »Datenverarbeitung« umfasst neben der eigentlichen Verarbeitung und Analyse der Daten u.a. auch deren Übertragung und Speicherung (vgl. Artikel 4 Nr. 2 DSGVO).

6.3.1 Unberechtigter Datenzugang

Personenbezogene Daten, insbesondere Gesundheitsdaten, dürfen für Unberechtigte nicht zugänglich sein. Unberechtigte Datenzugriffe oder Datenabflüsse verletzen die Vertraulichkeit der Daten und können für die Betroffenen nachteilig sein. Sollte ein Unternehmen die Daten nicht ausreichend schützen, ist mit einem Image- und Vertrauensverlust sowohl unternehmensintern als auch -extern zu rechnen, der sich negativ auf die künftigen Geschäftszahlen auswirken kann. Weiterhin können die Aufsichtsbehörden Strafen verhängen und Betroffene können zivilrechtliche Ansprüche geltend machen.

Unberechtigter Zugang zu den Daten kann bei den Komponenten des Wearable-Systems erfolgen oder bei der Übertragung der Daten (vgl. Abbildung 1 auf Seite 3).

Lösungsanforderungen, um unberechtigte Datenzugriffe zu unterbinden:

- **Berechtigte Datenzugriffe technisch und organisatorisch mit geeigneten Hürden versehen**: Zur Wahrung der Vertraulichkeit dürfen nur berechtigte Datenzugriffe zugelassen werden; es sind entsprechende Maßnahmen zu ergreifen, um unberechtigte Datenzugriffe zu verhindern.
- **Datenzugriffe sollten nur im notwendigen Umfang möglich sein**
- **Datenzugriffe sollten nachvollziehbar sein**, um die rechtskonforme Datenverarbeitung nachweisen und Fehlverhalten aufdecken zu können

- **Missbräuchliche Datenzugriffe sollten aufgedeckt und deren Verursacher identifiziert werden können**
- **Die Angriffsfläche sollte minimiert werden**

Konkrete Lösungsideen um unberechtigte Datenzugriffe zu unterbinden:

- IT-Sicherheit, technische und organisatorische Maßnahmen
    - **Datenzugriffskontrolle und Berechtigungsmanagement:** Um nur Berechtigten den Zugang zu den Daten zu erlauben, wird ein Mechanismus zur Datenzugriffskontrolle benötigt und ein entsprechendes Berechtigungsmanagement, um die Zugriffsberechtigungen zu verwalten.
    - **Datennutzungskontrolle implementieren**: Mit Datennutzungskontrolle können Datennutzungsrichtlinien zur Laufzeit durchgesetzt werden.
    - **Anwendung des Least-Privilege-Prinzips**, also die grundsätzliche Beschränkung von Berechtigungen auf das notwendige Minimum, um die Angriffsfläche zu minimieren.
    - **Anwendung des Need-to-know-Prinzips**, also die Einschränkung des Zugriffs auf genau die Informationen, die notwendig sind.
    - **Protokollierung und Überwachung der Datenzugriffe**, um missbräuchliche Datenzugriffe aufdecken, deren Verursacher identifizieren und geeignete Gegenmaßnahmen einleiten zu können.
    - **Anwendung des Mehr-Augen-Prinzips**, also das Erfordernis, dass mehrere Personen bei einer Aktivität beteiligt sind, um die Legitimität der Aktivität sicherzustellen. Beispielsweise könnte der Zugriff auf Daten des Produktivsystems die Mitwirkung von mehreren Personen erfordern. Dadurch soll verhindert werden, dass kritische Aktionen aus Versehen oder durch abtrünnige Einzelpersonen durchgeführt werden können.
    - **Verschlüsselte Datenspeicherung**: Durch das verschlüsselte Abspeichern von Daten kann die Angriffsfläche reduziert werden. Beispielsweise können gestohlene Festplatten nicht ohne Weiteres entschlüsselt werden.
    - **Vertrauenswürdige Infrastruktur:** Eine sichere und vertrauenswürdige Infrastruktur und Ausführungsumgebung sind in der Regel notwendig, um die Sicherheit der Daten zu gewährleisten.
    - **Systemtrennung und Abschottung:** Durch eine Trennung von Systemen und Maßnahmen zur Abschottung (bspw. getrennte Netzwerke) kann die Angriffsfläche reduziert werden. Zudem sind bei einer Kompromittierung von Teilsystemen nicht automatisch alle Systeme des Unternehmens betroffen.
    - **Physischer Schutz von Anlagen vor unberechtigtem Zugang:** Die Rechenzentren der Anbieter sind durch geeignete Maßnahmen zu schützen, um einen unberechtigten Datenzugang zu verhindern (bspw. Diebstahl der Festplatten)
    - **Mitarbeitersensibilisierung und -schulung bzgl. Informationssicherheit:** Neben der technischen Sicherheit von Anlagen und Systemen ist auch das korrekte Verhalten von Mitarbeitern für die Informationssicherheit wichtig. Beispielsweise sollte der Arbeitsplatz gesperrt werden, wenn man diesen verlässt, damit keine anderen Personen diesen Zugang nutzen können.
    - **Sicherheitsüberprüfungen:** Durch Sicherheitsüberprüfungen soll die Effektivität der vorhandenen Schutzmaßnahmen regelmäßig überprüft und attestiert werden.
    - **Multifaktor-Authentifizierung:** Passwörter reichen heute alleine nicht mehr aus, um den Zugang zu Systemen abzusichern. Sie sollten um weitere Elemente ergänzt werden, wie zum Beispiel Biometrie oder Security-Tokens.

6.3.2 Unrechtmäßige Weitergabe an Dritte

Personenbezogene Daten, und damit in der Regel insbesondere auch Gesundheitsdaten, dürfen nicht unberechtigt an Dritte weitergegeben werden. Beispielsweise könnte der Wearable-System-Anbieter oder -Analysedienstleister, der Arbeitgeber oder eine andere Partei (z. B. Infrastrukturanbieter und andere Dienstleister) Daten weitergeben, ohne dass es für diese Weitergabe eine ausreichende Rechtsgrundlage gibt.

Neben einer wissentlich unberechtigten Weitergabe von Daten an Dritte (datenzugriffsberechtigte Person ist sich ihres rechtswidrigen Handelns bewusst) sind auch unwissentlich unberechtigte Weitergaben (datenzugriffsberechtigte Person ist sich ihres rechtswidrigen Handelns nicht bewusst) denkbar. Unabhängig davon, ob sich die Person der Unrechtmäßigkeit ihres Handelns bewusst ist, liegt ein unrechtmäßiger Datenabfluss vor; die zu schützenden Daten wurden Unberechtigten gegenüber preisgegeben.

6.3.2.1 Lösungsanforderungen zur Verhinderung der unrechtmäßigen Weitergabe an Dritte

Die rechtssichere Weitergabe von Daten stellt folgende Anforderungen:

- Die Datenverarbeitung muss in einem rechtssicheren Rahmen erfolgen, um Rechtskonflikte zu vermeiden
- Datenweitergaben sind vor der Ausführung auf Zulässigkeit zu prüfen
- Nur berechtigte Auskunftsersuche dürfen bedient werden
- Datenweitergaben sollen nachverfolgbar sein, so dass der Verursacher einer unberechtigten Datenweitergabe identifiziert werden kann und damit dem Betroffenen entsprechend seiner Betroffenenrechte Auskunft erteilt werden kann, an wen seine Daten weitergegeben wurden

6.3.2.2 Konkrete Lösungsideen zur Verhinderung der unrechtmäßigen Weitergabe an Dritte

Folgende Maßnahmen bieten sich an:

- **Abschottung der Systeme**, um unberechtigte Datenübertragungen technisch zu verhindern
- **Verbot von Medien am Arbeitsplatz, mit denen Daten übertragen oder kopiert werden können**, zum Beispiel Verbot von USB-Sticks, CDs, Kameras
- **Erarbeitung von Prozessen für Datenweitergaben** und deren Prüfung und Freigabe
- **Mitarbeitersensibilisierung und -schulung bzgl. der rechtlichen Hintergründe einer Datenweitergabe**, um unwissentlich unrechtmäßige Datenweitergaben zu vermeiden.
- Erkennen unrechtmäßiger Weitergaben
    - **Protokollierung von Datenweitergaben**, um deren Nachverfolgbarkeit sicherzustellen und dem Betroffenen Auskunft darüber erteilen zu können, an wen seine Daten weitergegeben wurden.
    - **Datenauszüge mit einem Wasserzeichen versehen**: Die Daten werden von der jeweils weiterleitenden Stelle mit einem nicht fälschbaren und schwer entfernbaren Wasserzeichen versehen. Bei Geheimnisbruch kann man dann besser nachvollziehen, wo die Daten abhandengekommen sind. Dies kann zudem für Insider abschreckend wirken, da der Weitergebende Gefahr läuft, aufzufliegen.
- **Ende-zu-Ende-Verschlüsselung in Verbindung mit einer sicheren Ausführungskomponente**: Daten des Betroffenen sind stets verschlüsselt, lediglich innerhalb einer sicheren und abgeschotteten Ausführungskomponente beim Analysedienstleister können die Daten entschlüsselt und verarbeitet werden. Die Ergebnisse der Verarbeitung werden für den

Betroffenen verschlüsselt und verlassen die Ausführungskomponente in dieser verschlüsselten Form. Ein Zugriff auf die unverschlüsselten Daten ist selbst für Mitarbeiter des Analysedienstleisters zu keinem Zeitpunkt möglich.

Darüber hinaus kann eine Datenweitergabe auch berechtigt, aber gegen den Willen des Betroffenen erfolgen, zum Beispiel zur Erfüllung rechtlicher Verpflichtungen. Hierbei ist zu differenzieren, ob die jeweiligen Datenweitergaben oder Auskunftsersuche mit der DSGVO vereinbar sind. Beispielsweise ist die Herausgabe auf richterliche Anordnung im Rahmen der Strafverfolgung zulässig. Auskunftsersuchen von US-Behörden nach dem Cloud-Act sind hingegen problematisch, denn der Cloud-Act steht nach gängiger Meinung im Konflikt zur DSGVO. Hier können Unternehmen, für die der Cloud-Act anwendbar ist, in die Zwickmühle geraten, dass sie entweder gegen den Cloud-Act (wenn sie die Daten nicht herausgeben) oder die DSVGO (wenn sie die Daten herausgeben) verstoßen.

Wahl sicherer **Anbieter und Rechenzentren im EU-Rechtsraum**, um Konflikte mit anderen Gesetzen (bspw. dem Cloud-Act) zu vermeiden.

6.3.3 Unsichere Datenübertragung

Bei der Übertragung von Daten könnte die Kommunikation zwischen zwei Systemen abgehört werden oder ein Dritter übernimmt unbemerkt die Rolle eines Gesprächspartners. In beiden Fällen können Daten an einen unberechtigten Dritten offengelegt werden. Dieser kann die Daten missbrauchen oder manipulieren.

6.3.3.1 Lösungsanforderungen für eine sichere Datenübertragung

Zu fordern ist:

- Vor einer Datenübertragung sollten sich Sender und Empfänger vergewissern, dass der jeweilige Kommunikationspartner wirklich der ist, wer er vorgibt zu sein.
- Die Datenübertragung soll von Dritten nicht abgehört werden können.

6.3.3.2 Konkrete Lösungsideen für eine sichere Datenübertragung

Mögliche Maßnahmen könnten sein:

- **Transportverschlüsselung:** Durch eine Transportverschlüsselung können unverschlüsselte Daten über einen verschlüsselten Kanal zwischen zwei Systemen übertragen werden. Dies verhindert ein Mitlesen der Daten durch potenzielle Dritte, die die Datenübertragung beobachten bzw. abhören könnten. (Abhören des Kanals vermeiden)
- **Ende-zu-Ende-Verschlüsselung:** Bei der Ende-zu-Ende-Verschlüsselung werden die Daten vor der Übertragung selbst verschlüsselt, so dass wirklich nur der intendierte Empfänger sie entschlüsseln kann. Dies hat zur Folge, dass Systeme, die als Vermittler bei der Datenübertragung agieren, die Daten nicht einsehen können. (Nur der Empfänger kann die Daten lesen)
- **Gegenseitige Authentifizierung der Gesprächspartner**, beispielsweise durch Zertifikate: Dadurch kann sichergestellt werden, dass die Gesprächspartner wirklich die sind, als die sie sich ausgeben.
- **Übertragungen minimieren:** Die Übertragung von schützenswerten Daten sollte nach Möglichkeit auf ein notwendiges Minimum beschränkt oder sogar ganz vermieden werden, um die Angriffsfläche zu reduzieren. Denkbar ist zum Beispiel, dass die Daten des Wearables

direkt auf dem Smartphone verarbeitet werden, statt diese zur Verarbeitung an einen Dienstleister zu übermitteln.

6.3.4 Unrechtmäßige Veränderung von Daten

Unberechtigte Veränderung, also eine Verfälschung von Daten, kann zu Fehlinterpretationen führen, die negative Konsequenzen für den Arbeitgeber oder die Beschäftigten mit sich bringen. Angriffspunkte können zum einen die Messdaten selbst sein, aber auch die Analyseergebnisse. Es ist denkbar, dass die Messdaten auf ihrem Weg vom Wearable in die Cloud oder in der Cloud manipuliert werden. Andererseits könnten aber auch die Ergebnisdaten (nach der Analyse) auf dem Weg zum Betroffenen oder vom Betroffenen selbst manipuliert werden. Weiterhin können die Daten an den Speicherorten manipuliert werden, also allen Komponenten der Verarbeitungskette (vgl. Abbildung 1 auf Seite 3).

Arbeitnehmer könnten ein Interesse daran habe, ihre Messdaten oder Ergebnisse zu verfälschen, um beispielsweise ihren Arbeitgeber oder Aufsichtsbehörden zum eigenen Vorteil zu täuschen (z. B. Indizien für Überlastung oder Übermüdung verbergen oder vortäuschen).

Arbeitgeber könnten ein Interesse daran haben, die Messdaten oder Ergebnisse der Arbeitnehmer zu verfälschen, um diese oder Aufsichtsbehörden zum eigenen Vorteil zu täuschen (z. B. Indizien für Überlastung oder Übermüdung verbergen).

Ebenso könnte der Ruf des Analysedienstleisters Schaden nehmen, wenn durch Manipulation falsche Analyseergebnisse erzeugt oder verteilt werden. Folglich kann also ein gemeinsames Interesse daran bestehen, unberechtigte Veränderungen der Daten zu verhindern, um das Risiko von Sabotage oder Täuschung zu reduzieren.

Im Allgemeinen können dieselben Lösungsanforderungen und Lösungsideen, wie sie bereits beim Thema Datenzugang vorgestellt wurden, auch im Hinblick auf die Verfälschung von Daten Anwendung finden. Darüber hinaus sind folgende Lösungsanforderungen und -ideen zu nennen:

6.3.4.1 Lösungsanforderungen

- **Datenintegrität und -authentizität**, also die Gültigkeit und Echtheit der Daten sollte sichergestellt werden, um das Risiko von Manipulationen und die damit verbundenen Folgen zu reduzieren.
- **Nachverfolgbarkeit von Datenänderungen**, um Modifikationen und deren Ursprung nachvollziehen und prüfen zu können.
- **Berechtigte Datenänderungen technisch und organisatorisch vorsehen und mit geeigneten Hürden versehen**, um nur berechtigte Eingriffe zuzulassen.

6.3.4.2 Konkrete Lösungsideen

- **Verwendung von Prüfsummen und digitalen Signaturen**, um die Datenintegrität und -authentizität zu gewährleisten. Manipulationen sollen erkennbar werden.
- **Versionierung und Änderungsprotokolle vorsehen,** also die genaue Protokollierung von Veränderungen über die Zeit und wer diese Änderung durchgeführt hat, um Datenänderungen nachverfolgbar und überprüfbar zu machen.
- **Einführung von Richtlinien und technischen Schnittstellen zur Änderung von Daten**, die legitime Eingriffe ermöglichen und illegitime Eingriffe möglichst verhindern und aufdecken.

Beispielsweise könnte vorgesehen werden, dass Änderungen von einer weiteren Stelle überprüft und freigegeben werden müssen, bevor sie wirksam werden.

Es gibt bereits Lösungsansätze, um die Integrität und Authentizität von Daten zu schützen. Inwiefern eine Implementierung solcher Ansätze in der Praxis tatsächlich notwendig ist, kann vom konkreten Anwendungsfall abhängen, genauer gesagt, von der Eintrittswahrscheinlichkeit einer Datenfälschung und dem daraus resultierendem Schaden. In einem Szenario, bei dem ein Arbeitnehmer die Daten des Wearables für sich selbst nutzt und der Arbeitgeber die Daten sowieso nicht erhält, ist der Nutzen einer Datenfälschung für den Arbeitnehmer gering und damit auch seine Motivation, eine Manipulation vorzunehmen.

6.3.5 Unrechtmäßige oder unnötige Datenspeicherung

Wenn personenbezogene Daten unrechtmäßig oder unnötig gespeichert werden, zum Beispiel auch nach einer Löschfrist oder nachdem der vereinbarte Verarbeitungszweck erfüllt wurde, dann erhöht dies das Risiko von Datenmissbrauch. Zum einen gibt es damit einen zusätzlichen Angriffspunkt auf die Daten durch ein erweitertes »Window of Opportunity«. Zum anderen wird es dadurch überhaupt erst ermöglicht, Daten mit weiteren vorhandenen Daten zu kombinieren, wodurch Auswertungen für illegitime Zwecke (z. B. Leistungsüberwachung) ermöglicht werden.

6.3.5.1 Lösungsanforderungen zur Verhinderung von unrechtmäßiger und unnötiger Datenspeicherung

Wichtige Lösungsanforderungen sind:

- **Rechtmäßigkeit der Datenspeicherung sicherstellen (nur Speichern, was erlaubt ist):** Nach der DSGVO bedarf es einer Rechtsgrundlage für die Speicherung von personenbezogenen Daten. Bevor Daten gespeichert werden, sollte die Rechtmäßigkeit und die Rahmenbedingungen der Speicherung geklärt und dokumentiert werden.
- **Beachtung der Verarbeitungsgrundsätze Datenminimierung und Speicherbegrenzung (Löschen sobald möglich oder notwendig)**: Personenbezogene Daten dürfen nur in dem Umfang und für die Dauer gespeichert werden, wie es für die Zwecke, für die sie erhoben wurden, notwendig ist. Sie sind zu löschen, sobald der Zweck erreicht wurde oder die Rechtsgrundlage der Verarbeitung (z. B. die Einwilligung der betroffenen Person) entfällt.

6.3.5.2 Konkrete Lösungsideen zur Vermeidung von unrechtmäßiger und unnötiger Datenspeicherung

Konkrete Lösungsansätze könnten sein:

- **Ausarbeitung von Datenspeicher- und Löschkonzepten mit einem Fokus auf Datensparsamkeit**: Personenbezogene Daten dürfen nur so lange und auch nur in dem Umfang gespeichert werden, wie sie wirklich notwendig sind. Das heißt auch, dass keine Vorratsdatenspeicherung vorgenommen werden darf. Also die Speicherung auf den Verdacht hin, dass man die Daten in Zukunft brauchen könnte. Das Löschen von Daten, sobald der Verarbeitungszweck erfüllt ist oder die Rechtsgrundlage der Verarbeitung (z. B. die Einwilligung der betroffenen Person) entfällt, sollte explizit in den Konzepten und Prozessen der Datenverarbeitung vorgesehen und möglichst automatisiert durchgeführt werden.
- **Speicher- und Löschfristen festlegen und automatisiert durchsetzen**: Die Festlegung von Speicher- und Löschfristen und deren automatische Durchsetzung können Datenverarbeiter

unterstützen, eine rechtzeitige und gesetzeskonforme Löschung der Daten sicherzustellen. Zudem bieten offen kommunizierte oder sogar selbstkonfigurierbare Speicher- und Löschfristen für die Betroffenen zusätzliche Transparenz und Selbstbestimmung, die das Vertrauen in und Einverständnis mit der Datenverarbeitung fördern können. Neben zeitlich gemessenen Fristen, wie z. B. 24-Stunden, sind auch qualitative Fristen zu berücksichtigen, wie z. B. der Wegfall der Rechtsgrundlage durch Widerspruch der betroffenen Person. Auch hier können automatisierte Prozesse unterstützen.

- **Keine Daten speichern**: Möglicherweise können Daten sofort verarbeitet und das Ergebnis der Verarbeitung sodann dem jeweiligen Empfänger bereitgestellt werden. Eine Speicherung der Daten ist hier ggf. nicht notwendig und sollte dann auch nicht erfolgen.
- **Speicherung von anonymisierten Daten**: Sobald die Daten anonymisiert sind, also deren Bezug zu einer Person nicht mehr hergestellt werden kann, unterliegen diese Daten nicht mehr der DSGVO. Eine Verarbeitung solcher Daten ist weniger kritisch und mit keinen besonderen Auflagen verbunden.

6.3.6 Schlechter Umgang mit Datenlecks

Anbieter sollten präventive Schutzmaßnahmen ergreifen, die einem möglichen Datenleck vorbeugen. Zudem sollten Anbieter ihre Systeme überwachen, um Angriffsversuche und Datenlecks zeitnah feststellen und entsprechend reagieren zu können. Weiterhin sollten Anbieter auf den Ernstfall vorbereitet sein und über entsprechende Notfallpläne verfügen. Hierbei ist auch die Kommunikation mit Behörden, den Betroffenen und den Medien wichtig. Insbesondere sollten die betroffenen Kunden mit ihren Fragen und Ängsten nicht alleine gelassen werden.

Die Kommunikation mit den Betroffenen könnte unnötig verzögert stattfinden, da die Beziehungen zwischen Arbeiternehmer, Arbeitgeber, Analysedienstleister und anderen Akteuren im Kontext des Einsatzes von Wearables im Arbeitskontext können unübersichtlich sein. Möglicherweise ist nicht klar, wer wofür zuständig und verantwortlich ist. Dadurch werden wichtige Verantwortlichkeiten nicht wahrgenommen, Ansprechpartner nicht gefunden und/oder Schritte, zum Beispiel bei einem Datenleck, eventuell nicht schnell genug eingeleitet.

6.3.6.1 Lösungsanforderungen

Wichtige Anforderungen sind:

- **Klarheit bezüglich der Zuständigkeiten und Verantwortlichkeiten**, damit jeder Beteiligte weiß, wofür er selbst verantwortlich ist und an wen er sich bei welchen Angelegenheiten werden kann.
- **Effektive Kommunikation und Zusammenarbeit zwischen den Beteiligten ermöglichen.**

6.3.6.2 Lösungsideen

Mögliche Lösungsansätze sind:

- **Rechtlich saubere Klärung bezüglich der Rollen, Rechte und Pflichten aller Beteiligten**, um Klarheit bezüglich der Zuständigkeiten und Verantwortlichkeiten zu schaffen.
- **Ansprechpartner benennen**, um eine zielgerichtete und effektive Kommunikation und Zusammenarbeit zwischen den Beteiligten zu ermöglichen.

6.4 Datennutzung

Die Auswertung der Wearable-Daten soll entweder aggregiert erfolgen, oder der Personenbezug soll durch geeignete Anonymisierung oder Pseudonymisierung für Dritte unkenntlich gemacht werden. Die Ergebnisse der KI-Analyse werden dann auf verschiedene Weisen aufbereitet. Zum einen können die Daten für den Wearable-Träger aufbereitet werden, um ihm selbst Feedback zu geben. Zum anderen können die Daten verschiedener Wearable-Träger kombiniert werden, um zum Beispiel Erkenntnisse über eine Arbeitsstation zu erhalten und dem Arbeitgeber Möglichkeiten zu geben, potenziellen Problemen an dieser Arbeitsstation entgegenzuwirken.

6.4.1 Unpassende logische Berechnung mit Wearable Daten

Durch mangelndes Wissen und falsche Interpretationen können falsche Schlüsse aus den erhobenen Daten gezogen werden. Dies kann daran liegen, dass etwa eine Moderatorvariable nicht berücksichtigt wird oder natürliche Abweichungen von der Norm nicht als solche erkannt werden.

Kritisiert ein Vorgesetzter etwa einen Mitarbeiter, dass er laut Wearable-Daten schon zu Schichtbeginn ein geringeres Energielevel als gleichaltrige Kollegen hat, lässt bei dem Vergleich jedoch die »Art der Schicht« außer Acht, könnte es sein, dass der beschuldigte Mitarbeiter vielleicht Nachtschicht hatte. Wenn die Vergleichsdaten von Kollegen aus der Tagschicht stammen, könnte das den Unterschied der Leistungsfähigkeit erklären. Es könnte auch passieren, dass Mitarbeiter mit ihrer Kohorte verglichen werden sollen, die Personen eines vergleichbaren körperlichen Fitnesslevels umfasst, die angewendete Kohorte jedoch falsch gewählt wurde. So könnte es wiederum zu Fehlinterpretationen kommen.

6.4.1.1 Lösungsanforderungen

Es muss sichergestellt werden, dass die Berechnungen, die mit den Daten durchgeführt werden, fehlerlos sind und alle relevanten Informationen für die Auswertungen mit einbezogen werden. Zudem muss sichergestellt werden, dass das persönliche Fitnesslevel adäquat erfasst wird und eine zutreffende Einordnung in die passende Kohorte gewährleistet ist.

Wünschenswert wäre, dass die verwendeten Analysemethoden für Experten nachvollziehbar spezifiziert sind. Bei klassischen Regressionsverfahren oder regelbasierten Entscheidungsverfahren ist eine statistische oder medizinische Beurteilung prinzipiell möglich. Allerdings stößt die Nachvollziehbarkeit von Verfahren des maschinellen Lernens oft an ihre Grenzen.

6.4.1.2 Konkrete Lösungsideen

Lösungsansätze könnten sein:

- **Einbinden von Expertenwissen:** Die Verfahren und Berechnungen sollen auf logischer Ebene durch fachliche Experten (aus Auswertungsperspektive) überprüft werden. Dadurch sollen falsche Schlussfolgerungen und fehlerhafte Auswertungen vermieden werden. Zu diesem Zweck sollte auch der Quelltext und die darin beschriebene Verarbeitungslogik inspiziert werden, um zumindest die nachvollziehbaren Aspekte der Verarbeitungslogik zu verifizieren (KI-Komponenten wie etwa neuronale Netze sind solchen Überprüfungen jedoch kaum zugänglich). Des Weiteren sollte die Baseline der zugrundeliegenden Berechnungen auf fundiertem Wissen basieren.
- **Korrekturmöglichkeit:** Der Arbeitnehmer sollte die Möglichkeit erhalten, die Ergebnisse der Auswertung einzusehen und zu korrigieren, sollten die Ergebnisse seiner Meinung nach nicht korrekt sein. Alternativ könnte er ein Gespräch mit dem Arbeitgeber anstoßen, in dem er seine

Sicht auf die Korrektheit mit dem Arbeitgeber besprechen kann. Zudem sollte bei Bedarf die Auswertung durch einen Experten (z. B. durch den Betriebsarzt) angeregt werden können. Es könnte auch sinnvoll sein, dass der Arbeitnehmer bei Bedarf eine Notiz an seine Daten anhängen kann, so dass die Notiz nicht verloren geht und dem Datennutzer nachweislich vorliegt.

- **Selektives Ausschließen:** Der Arbeitnehmer sollte die Möglichkeit haben, im Zweifelsfall einzelne Analyseergebnisse von der Weitergabe auszunehmen oder bereits der Verwendung bestimmter Rohdaten zu Analysezwecken zu widersprechen. Auch der Analysedienst könnte die Stimmigkeit und Plausibilität der erhobenen Rohdaten überwachen und im Verdachtsfall einzelne Messreihen vorsichtshalber von einer Analyse ausnehmen oder die Analyseergebnisse zumindest als „fragwürdig“ markieren.

6.4.1.3 Herausforderungen

In Bezug auf die Ziele des Projekts ergeben sich folgende Herausforderungen:

- **Begrenztes Wissen:** Das Missachten beispielsweise einer Moderatorvariable muss nicht immer Absicht sein. Es kann auch schlichtweg daran liegen, dass die Variable nicht bekannt ist oder nicht gemessen wird. Das Wissen von Menschen ist begrenzt und auch Experten wissen nicht alles oder machen Fehler.
- **Anonymisierung vs. Nutzbarkeit:** Durch die Anonymisierung der Wearable-Daten werden die Daten einen gewissen Grad an Nutzbarkeit und Verständlichkeit verlieren. Nicht jedes Anonymisierungsverfahren ist für jeden Anwendungsfall sinnvoll, und Anonymisierung könnte im Einzelfall zu Fehlinterpretationen verleiten.
- **Reale vs. gewünschte Aussage der Daten:** Korrekturmöglichkeiten der Daten könnten dazu führen, dass Mitarbeiter große Teile ihrer Daten »korrigieren«, was einerseits dazu führen könnte, dass die Daten komplett verfälscht und zum Nutzen der Mitarbeiter verändert werden, und andererseits vielleicht die Datensammlung durch die Wearables obsolet machen, wenn die Mitarbeiter die Daten zu großen Teilen mit Hand einpflegen.
- **Aufhebung der Anonymität durch Korrekturen:** In Anwendungsfällen, in denen die Anonymität der Beschäftigten gewahrt bleiben soll, kann es für betroffene schwierig sein, Korrekturen der Messdaten geltend zu machen, ohne sich dadurch zu erkennen zu geben.
- **Begrenzte Nachvollziehbarkeit von Machine-Learning-Modellen:** Das Problem der Nachvollziehbarkeit von KI-Methoden ist ein wichtiges aktuelles Forschungsthema, denn mangelnde Nachvollziehbarkeit maschineller Lernverfahren gefährdet deren Einsatz in Systemen, deren Korrektheit, Sicherheit oder Verlässlichkeit zertifiziert werden muss (z. B. in der Avionik oder im Automobilbau). Da WearPrivate ebenfalls auf maschinelle Lernverfahren zur Datenanalyse setzt, lässt sich die Güte der Analysen in diesem Fall nicht formal nachweisen, sondern nur im praktischen Test validieren.

6.4.2 Zweckentfremdete Datennutzung des Arbeitgebers

Die bei der Auswertung von Wearable Daten gewonnen Informationen könnten für Zwecke verwendet werden, die rechtlich nicht zulässig sind oder gegen die Absprache mit den Arbeitnehmern und Arbeitnehmervertretungen verstoßen. Zum Beispiel könnte unzulässigerweise die Leistung überwacht werden (z. B. durch Messung der Aufenthaltsdauer an der Arbeitsstelle und des Arbeitsergebnisses) oder ständig eingesehen werden, wo der Arbeitnehmer sich gerade aufhält. Besonders kritisch ist dies, wenn der Gesundheitszustand abgeleitet wird (z. B. anhand der Anzahl der Toilettengänge).

Dazu kommt die Problematik, dass die erhobenen Daten mit weiteren niedergeschriebenen sowie auch mit impliziten Informationen kombiniert werden können, etwa der Anzahl der Urlaubstage oder persönlichem Wissen von verarbeitenden Personen. Ein Teamleiter könnte die Daten zum Beispiel mit seinen persönlichen Beobachtungen kombinieren, und dies könnte dann zu negativen Konsequenzen für den Arbeitnehmer führen.

6.4.2.1 Lösungsanforderungen

Die Daten und Verarbeitungen sollen derart geschützt werden, dass eine Verarbeitung zu anderen als den vereinbarten Zwecken unterbunden wird. Die Erhebung und Verarbeitung der Daten sollten von einer neutralen Partei vorgenommen werden, niemals von einer am Verfahren beteiligten Interessengruppe.

6.4.2.2 Konkrete Umsetzungsideen

Maßnahmen zur Verhinderung unerwünschter Datenauswertungen:

- **Anonymisierung und Aggregation:** Durch die anonymisierte oder pseudonymisierte Verarbeitung und den fehlenden Personenbezug der Daten könnte es ermöglicht werden, dass nur der Arbeitnehmer die Ergebnisse seiner Auswertungen sieht, der Arbeitgeber jedoch nicht. Alternativ könnte der Arbeitgeber zwar die Informationen der einzelnen Beschäftigten sehen, dürfte jedoch nicht zuordnen können, zu wem welcher Datensatz gehört. Anonymisierung durch Aggregation könnte andererseits dafür genutzt werden, dass der Arbeitgeber nur Informationen über eine Gruppe von Arbeitnehmern erhält und somit ebenfalls nicht eindeutig auf eine Person zurückschließen kann.
- **Strikte Datenzugriffs- und Datennutzungskontrolle:** Es sollte eine Überwachung und Kontrolle des Verarbeitungsprozesses derart durchgesetzt werden, dass sichergestellt werden kann, dass keine weitere (technische) Verarbeitung der Daten möglich ist und Daten nicht unbemerkt in weitere Verarbeitungsprozesse abfließen können. Die Möglichkeit des Datenzugriffs soll dabei direkt an die Einwilligung gebunden sein. Dazu sollte ebenfalls die Verarbeitungslogik geprüft werden
- **Daten beim Nutzer halten:** Soweit möglich sollten die Berechnungen lokal auf den Geräten des Nutzers durchgeführt und nicht auf den Server oder in die Cloud des Arbeitgebers oder eines Auftragsdatenverarbeiters verlagert werden. Bei der Nutzung von maschinellem Lernen könnte gegebenenfalls das fertig trainierte Model auf die Geräte des Nutzers übertragen werden, um dort lokale Analysen zu ermöglichen, ohne die aufwändigen Trainingsberechnungen lokal vornehmen zu müssen.
- **Datensparsamkeit:** Den Datennutzern sollten nur die ausgewerteten Daten zur Verfügung gestellt werden, jedoch nicht die Rohdaten, damit diese nicht für andere, nicht legitime Auswertungen genutzt werden können. Die ausgewerteten Daten können ebenfalls in einer abstrahierten Form vorliegen: So könnte etwa nur mitgeteilt werden, dass ein Grenzwert überschritten wurde, jedoch keine zugrundeliegenden Werte angeben werden.

6.4.2.3 Herausforderungen

Das Bestreben, sensible Daten möglichst lokal beim Betroffenen zu halten, stößt an technische Beschränkungen:

- **Rechenleistung:** Die begrenzte Batteriekapazität und die Rechenleistung von Smartphones und vor allem von Wearables ermöglicht es nur eingeschränkt, komplexe Berechnungen wie Verfahren des maschinellen Lernens beim Nutzer direkt auszuführen.

6.4.3 Negative Folgen der Analysen

Durch die Analysen der Wearable Daten werden unter Umständen zulässige Schlüsse aus den Daten gezogen, die jedoch zu Konsequenzen führen, die nicht den Interessen der Arbeitnehmer entsprechen. Daten könnten beispielsweise darauf hindeuten, dass ein Arbeitnehmer eine Arbeitsstation als belastend empfindet. Die Konsequenz wäre, den Arbeitnehmer weniger an der Station arbeiten zu lassen. Es könnte jedoch sein, dass der Arbeitnehmer die Station belastend im Sinne von herausfordernd findet, jedoch nicht überlastend. Der Arbeitnehmer freut sich vielleicht über die Herausforderung. Im Extremfall könnten die Daten sogar zu einer unerwünschten Versetzung oder gar zur Kündigung führen.

Zudem könnten die Analysen Informationen für den Arbeitnehmer preisgeben, die er nicht wissen möchte (Recht auf Nichtwissen). Beispielsweise könnte der Arbeitnehmer vermeintlich zu seinem Wohle über persönliche gesundheitliche Probleme informiert werden, über die er eigentlich nicht informiert werden möchte.

6.4.3.1 Lösungsanforderungen

Die Nutzung der Wearables soll nicht dazu führen, dass der Nutzer nur auf Basis dieser Verarbeitungen nachteilige Konsequenzen erfährt. Der Nutzer sollte zudem in der Lage sein zu bestimmen, gewisse Informationen über seinen Gesundheitszustand nicht zu erhalten.

6.4.3.2 Konkrete Umsetzungsideen

Ansätze, um negative Auswirkungen der Datenanalysen zu vermeiden, könnten sein:

- **Erhaltene Informationen begrenzen:** Durch das Angeben von persönlichen Präferenzen sollen Arbeitnehmern selbst bestimmen, welche Informationen sie nicht erhalten möchten. Zudem sollten alle Beteiligten über das Recht auf Nichtwissen informiert werden und ihr Verhalten dementsprechend anpassen, denn ein Verstoß gegen das Recht auf Nichtwissen ist strafbar.
- **Einschränken der Ergebnisverwertung:** Die Betroffenen sehen die Auswertung ihrer Daten zuerst ein und entscheiden dann, ob und welche Ergebnisse sie anderen Personen zur Verfügung stellen möchten.
- **Prozesse vertrauensvoller gestalten:** Der Arbeitgeber sollte seinen Arbeitnehmern durch Zusicherungen ein erhöhtes Maß an Sicherheit geben. Dafür könnte etwa vertraglich festgelegt werden, dass die Ergebnisse der Analysen keinen Einfluss auf Personalentscheidungen haben werden. Zudem könnte eine vertrauensvolle Mittelperson mit der Auswertung beauftragt werden (z. B. ein externes Unternehmen, für Mitarbeiterbefragungen bereits üblich) und der gesamte Prozess einem unabhängigen Review unterzogen werden.

6.4.3.3 Herausforderungen

Bei der Umsetzung ergeben sich folgende Herausforderungen:

- **Recht auf Nicht-Wissen vs. Fürsorgepflicht:** Der Wunsch des Einzelnen, verschiedene gesundheitliche Informationen nicht zu erfahren, widerspricht dem Wunsch des Arbeitgebers, seine Mitarbeiter zu schützen und vor (gesundheitlichen) Gefahren zu bewahren.
- **Objektive vs. subjektive Einschätzung:** Der Arbeitgeber könnte eine große Belastung eines Arbeitnehmers feststellen und ihn davor bewahren wollen. Andererseits könnte der besagte Arbeitnehmer dennoch Spaß an dieser Herausforderung haben. Aber auch, wenn eine Person Spaß an einer Station hat, kann es erforderlich sein, ihre dort verbrachte Zeit zu reduzieren, jedenfalls dann, wenn sich ernste Gefährdungen ergeben könnten.

6.4.4 Abgrenzung des Projektscopes

In Bezug auf den Projektscope lässt sich feststellen, dass die Aspekte der korrekten Datenanalyse eher organisatorischer Natur sind. Falsche Interpretationen der Daten sind stets möglich und sehr stark von den gewählten Berechnungen sowie der Erfahrung der verarbeitenden Stelle abhängig. Da diese Informationen einzelfallabhängig und nicht vorhersehbar sind, kann hier nur empfohlen werden, für nötige Eingruppierungen, beispielsweise in eine passende Kohorte vergleichbarer Beschäftigter, wenn möglich Normen wie ISO-Standards zu nutzen und die Wearable-Daten nicht als alleinige Basis für schwerwiegende Entscheidungen heranzuziehen. Diese Daten können Indizien darstellen und Dinge andeuten, doch die Aussagekraft dieser Informationen ist stark anwendungsfallabhängig.

Werden die unerwünschten Konsequenzen durch die Nutzung der Wearables und ihrer Daten betrachtet, so ist es das Ziel des Projekts, Möglichkeiten zur Verhinderung oder Abmilderung negativer Folgen zu erforschen. Auch in Bezug auf das Recht auf Nichtwissen sollen Maßnahmen gefunden werden, um es mit der Fürsorgepflicht des Arbeitgebers zu vereinbaren.

Ein wichtiger Aspekt des Projekts wird es zudem sein, die Verarbeitung der Daten zu illegitimen Zwecken auf technische Weise zu unterbinden. Die dazu genutzten Anonymisierungs- und Pseudonymisierungsverfahren sind den Betroffenen womöglich aber schwer zu vermitteln. Hier gilt es, durch bessere Informationsangebote dafür zu sorgen, dass die Arbeitnehmer dem durch Anonymisierung gegebenen Schutz vertrauen und ihn wahrnehmen, um möglichst zielführende Analysen zu ermöglichen.

Im Projekt ist auch die Frage zu klären, wie stark der Informationsverlust durch Anonymisierung ist und welche Verfahren für eine sinnvolle Nutzung der Wearable-Daten eingesetzt werden können. Bestimmte Anonymisierungsverfahren, wie etwa Differential Privacy, sollen sogar in der Lage sein, Daten auch vor Zusatzinformationen zu schützen, die nur implizit als Wissen von Personen vorliegen, was im Projekt näher betrachtet werden soll.

6.5 Sozialer Druck

Neben der Wirkung auf den Anwender selbst soll auch das soziale Umfeld des Anwenders betrachtet werden. Wenn Wearables am Arbeitsplatz zum Standard werden, so entsteht zum einen sozialer Druck auf den Einzelnen, sich diesem Trend anzuschließen. Der soziale Druck kann dazu führen, dass eine Einwilligung nicht mehr als freiwillig angesehen werden kann. Sozialer Druck kann auch auftreten, wenn es um eine konkrete Einwilligung oder Datenschutzeinstellungen geht. Probleme sind unter anderem Nudging mit Dark Patterns und Social Engineering.

6.5.1 Lösungsanforderung

Die Betroffenen sollen sich ermächtigt fühlen, selbstbestimmt und ohne negative Konsequenzen zu entscheiden, ob sie Wearables nutzen möchten oder nicht.

6.5.2 Konkrete Umsetzungsidee

Mögliche Ansätze könnten sein:

- **Unabhängige Stelle:** Eine zwischengeschaltete unabhängige Person kann helfen, Anonymität darüber zu wahren, wer ein Wearable nutzt. Nur dieser Person erfährt, welche Beschäftigten das Wearable nutzen. Da Daten nur anonymisiert übertragen werden, erfährt der Vorgesetzte nicht, wer diese Personen sind. Wearables könnten zum Schein getragen werden, ohne dass tatsächlich Daten erhoben werden.

- **Aufklärung:** Mitarbeiter sollten über typische Dark Patterns und Social Engineering-Methoden aufgeklärt werden, so dass sie die Versuche der negativen Beeinflussung erkennen und abwenden können.
- **Vertrauensperson:** Es sollte ein Ansprechpartner zur Verfügung stehen, an den sich Betroffene wenden können, wenn sie sich unter Druck gesetzt fühlen.
- **Regelungen**: Es sollten Organisationsregeln festgelegt werden, die sozialem Druck entgegenwirken, zum Beispiel eine Regel, dass nur der Betriebsrat einsehen kann, wer das Wearable tatsächlich nutzt.

6.5.3 Herausforderung

Die weitgehende Akzeptanz eines Wearable-Einsatzes kann zwiespältige Folgen haben:

- **Anonymität der Gruppe vs. Gruppenzwang:** Je mehr Beschäftigte die Wearables nutzen, desto schwieriger ist es, Individuen in den Datensätzen zu identifizieren, das heißt, desto höher ist die Anonymität. Jedoch erhöht ein hoher Anteil an Wearable-Nutzern den Druck auf die verbliebenen ablehnenden Beschäftigten, ebenfalls ein Wearable zu verwenden.

Trotz guter Datenschutzmaßnahmen werden einzelne Beschäftigte die Wearables ablehnen. Beweggründe könnten sein, dass die Betreffenden regelmäßig gegen Sicherheitsvorschriften verstoßen und ihr Fehlverhalten durch die Wearables aufgedeckt werden könnte. Zum Beispiel könnte aufgedeckt werden, dass sich Berufskraftfahrer trotz Müdigkeit hinter das Steuer setzen.

6.5.4 Abgrenzung des Projektscopes

Weitere Voraussetzungen für die Akzeptanz sind die Überzeugung, dass die Nutzung der Wearables sinnvoll ist, dass man im Stande ist, die Wearables zu bedienen und dass Kollegen und Vorgesetzte die Nutzung ebenfalls sinnvoll finden. Zudem muss eine gute Vertrauensbasis bestehen zwischen Belegschaft und Arbeitgeber. Die Vertrauensbasis kann geschädigt werden, wenn Datenschutzverstöße nicht geahndet werden. Daher ist es wichtig, Fehlverhalten zu ahnden, um den Beschäftigten zu signalisieren, dass der Schutz ihrer Daten dem Arbeitgeber wirklich wichtig ist.

Wie diese Voraussetzungen konkret umgesetzt und die zuvor beschriebenen Fälle verhindert werden können, wird im Rahmen dieses Projekts nicht näher betrachtet.

7 Erhebung der Anforderungen

Die zuvor vorgestellten möglichen Probleme und Lösungsideen dienen als Ausgangsbasis, um Anforderungen zu erheben. Die möglichen Probleme wurden aus den Anwendungsfällen abgeleitet und die Lösungsideen sind wiederum von den möglichen Problemen inspiriert. Jedoch sind die genannten Probleme und Lösungsideen bisher nicht validiert. Sie sollen nun mit Stakeholdern validiert werden und dabei weitere Anforderungen und Lösungsideen erhoben werden, so dass anschließend ein Rahmenwerk für die Entwicklung sicherer Wearables erstellt werden kann.

Die von den Stakeholdern genannten Lösungsideen sollten kritisch hinterfragt werden. In vielen Fällen gibt es bessere Lösungsideen als jene, die den Stakeholdern als erstes einfallen. Die genannten Lösungsideen sollten daher auf enthaltene Anforderungen untersucht werden; basierend auf den Anforderungen können dann weitere Lösungsideen entwickelt werden.

7.1 Anforderungen der Beschäftigten

Folgende Aspekte sollten von den Beschäftigten erfragt werden:

- Validierung der Probleme und der konkreten Lösungsideen aus Abschnitt 6.1.2 »Ablehnung der Wearable-Nutzung nach Wearable-Einführung«
- Bedarfe
    - **Transparenzbedarf:** Welche Informationen möchten die Betroffenen über die Verwendung ihrer Daten haben?
    - **Selbstbestimmungsbedarf:** Über welche Datennutzung möchten Betroffene mitbestimmen?
    - **Schutzbedarf:** Welche Daten sind für die Betroffenen schützenswert?
    - **Benutzungsbedarfe:** Welche Bedarfe bezüglich der Interaktion mit Datenschutzmaßnahmen haben die Betroffenen?
- Motivation für Nutzung und Gründe für Nicht-Nutzung
- Eigene Lösungsideen

7.2 Anforderungen des Betriebsrats

Die folgenden Aspekte sollten vom Betriebsrat erfragt werden:

- Validierung der Probleme und der konkreten Lösungsideen der Abschnitte
    - »Ablehnung der Wearable-Einführung« (Abschnitt 6.1.1)
    - »Unerwünschtes Verhalten des Arbeitgebers in der Verarbeitung« (Abschnitt 6.4.2)
    - »Negative Folgen der Analysen« (Abschnitt 6.4.3)
    - »Sozialer Druck« (Abschnitt 6.5)
- Bedarfe in der Rolle als Arbeitnehmervertretung
    - **Transparenzbedarf:** Welche Informationen möchten die Beschäftigten über die Verwendung ihrer Daten haben?
    - **Selbstbestimmungsbedarf:** Über welche Daten möchten die Beschäftigten mitbestimmen?
    - **Schutzbedarf:** Welche Daten sind für die Beschäftigten schützenswert?
    - **Benutzungsbedarfe:** Welche Bedarfe bezüglich der Interaktion mit Datenschutzmaßnahmen haben die Beschäftigten?
- Bedarfe in der Rolle als Betriebsratsmitglieder
    - **Transparenzbedarf:** Welche Informationen möchten Betriebsratsmitglieder über die Verwendung personenbezogener Daten haben?
    - **Schutzbedarf:** Welche Daten sehen Betriebsratsmitglieder als schützenswert an?
    - **Benutzungsbedarfe:** Welche Bedarfe bezüglich der Interaktion mit Datenschutzmaßnahmen haben Betriebsratsmitglieder?
- Eigene Lösungsideen

7.3 Anforderungen der IT-Security-Abteilung

Von der betrieblichen IT-Security sollen folgende Aspekte erfragt werden:

- Validierung der Probleme und der konkreten Lösungsideen unter

    - »Ablehnung der Wearable-Einführung« (Abschnitt 6.1.1)
    - »Datenmenge« (Abschnitt 6.2.1)
    - »Erhebung im privaten Raum« (Abschnitt 6.2.2)
    - »Datenverarbeitung« (Abschnitt 6.3)
    - »Unpassende logische Berechnung mit Wearable Daten« (Abschnitt 6.4.1)
- Bedarfe
    - **Transparenzbedarf:** Welche Informationen möchten IT-Security-Mitarbeitende über die Verwendung personenbezogener Daten haben?
    - **Schutzbedarf**: Welche Daten sehen IT-Security-Mitarbeitende als schützenswert an?
    - **Benutzungsbedarfe:** Welche Bedarfe bezüglich der Interaktion mit Datenschutzmaßnahmen haben IT-Security-Mitarbeitende?
- Eigene Lösungsideen

7.4 Anforderungen der Datennutzer

Die folgenden Aspekte sollten von Datennutzern (z. B. Management, Betriebsarzt, Gesundheits- oder Arbeitsschutzbeauftragter) erfragt werden:

- Bedarfe
    - **Datennutzungsbedarf:** Welche Daten sollen genutzt werden?
    - **Umsetzungsbedarfe:** Bei der Umsetzung welcher Pflichten, die sich aus der DSGVO und anderen rechtlichen Regelungen bzgl. Datenschutz ergeben, ist Unterstützung gewünscht?
    - **Informationsbedarf:** Welche Informationen über die rechtsichere Nutzung der Daten brauchen die Datennutzer?

Hier bei ist zu berücksichtigen, dass auch der Anwender selbst ein Datennutzer ist, der womöglich nicht allen denkbaren Verwertungen seiner gemessenen Vitaldaten zustimmt. Vielleicht möchten manche Anwender zum Beispiel keine weit zurückliegende Belastungshistorie erfassen, um das Risiko von Datenschutzverletzungen zu beschränken. Unter Umständen möchten sie auch nicht über alle denkbaren Befunde informiert werden, die aus den Messdaten theoretisch ableitbar wären: Hinweise auf eine unheilbare Krankheit könnten zum Beispiel eher belastend als hilfreich wirken.

8 Anforderungen für »Belastungsmessung«

Nach Abwägung der Forschungsfragen des Projekts und der Möglichkeiten, verschiedene Anwendungsfälle in einem Demonstrator zu realisieren, haben sich die Forschungspartner darauf verständigt, sich vornehmlich die Anwendungsfälle »Belastung im Manufacturing-Bereich« (siehe Abschnitt 3.1) und »Belastung in Risikosituationen« (siehe Abschnitt 3.3) zu konzentrieren. In diesem Kapitel entwickeln wir für diese Szenarien grundlegende Anforderungen, um einerseits die Privatsphäre der Nutzer zu schützen, andererseits aber auch die legitimen Interessen des Arbeitgebers, der das System einführt und bezahlt, sowie des Dienstleisters, der die Dienstleistung gegen Bezahlung erbringt, zu wahren.

8.1 Grundansatz zur Wahrung des Datenschutzes und der Privatsphäre

Das Ziel des Datenschutzes muss es sein, personenbeziehbare Daten nur in dem unbedingt erforderlichen Maß zu erheben oder weiterzuverarbeiten und den Zugriff auf diese Daten auf den unvermeidlich erforderlichen Kreis von Berechtigten einzuschränken. Ein wichtiger Baustein hierzu ist eine generelle *Datensparsamkeit*: Je weniger Daten überhaupt erhoben werden und je weniger davon personenbeziehbar sind, umso eher lässt sich der Datenschutz realisieren.

Der zweite wichtige Baustein zur Wahrung des Datenschutzes und der Privatsphäre ist *Anonymität*: Entlang der Verarbeitungskette der Daten sollte so selten wie möglich Bezug auf die wahre Identität der Nutzer genommen werden. Wann immer möglich, sollten Daten ganz ohne Bezug auf einen spezifischen Nutzer verarbeitet werden, etwa als aggregierte Daten einer ganzen Nutzergruppe. Wo eine Zuschreibung der Daten zu einem bestimmten Individuum nicht vermeidbar ist (etwa bei der Speicherung individueller Nutzerpräferenzen), sollte das Individuum zumindest nur unter einem Pseudonym bekannt sein, nicht aber unter seiner wahren Identität.

Die Wahrung der Anonymität muss zwei wesentliche Gesichtspunkte berücksichtigen:

- **Prozessmodell:** Der Verarbeitungsprozess zur Nutzerregistrierung, Erfassung und Analyse der Rohdaten sowie Offenlegung der Befunde muss so gestaltet sein, dass eine Zuschreibung individueller Nutzeraktivitäten zu einer bestimmten Person nicht schon aufgrund der Interaktionen zwischen den Komponenten der Prozesskette sofort möglich ist. So soll etwa eine Identifizierung einer Person nicht dadurch möglich sein, dass sich die Person mit ihrer Rechnungsanschrift oder ihrem E-Mail-Account zuvor registrieren musste.
- **Datenmodell:** Eine einfache Personenzuordnung individueller schützenswerter Informationen aufgrund verräterischer, charakteristischer Datenmerkmale muss ebenfalls vermieden oder zumindest hinreichend erschwert werden. Wenn etwa gewisse Vitaldaten ähnlich individuell wie ein Fingerabdruck sind, dann soll deren Verbreitung bestmöglich eingeschränkt werden, indem sie zum frühestmöglichen Zeitpunkt durch unpersönliche, abgeleitete Belastungsindikatoren ersetzt werden, die nicht mehr charakteristisch für ein bestimmtes Individuum sind. Alternativ dazu könnten die Vitaldaten auch zu einem gewissen Grad

»verrauscht« oder vergröbert werden, bis ihr individueller Charakter verschwindet, sofern dadurch die Güte der Analyse nicht zu sehr gemindert wird.[3]

In welchem Grad eine solche Anonymisierung des Datenmodells möglich ist, muss jeweils für den konkreten Anwendungsfall untersucht werden. Hier stehen Anforderungen an die Datengüte unter Umständen im Widerspruch zu einer vollständigen Anonymisierung oder Pseudonymisierung, denn manche Analysen erfordern sehr präzise, unverfälschte Daten. Vorläufige Befunde des Projekts deuten darauf hin, dass im von uns betrachteten Anwendungsfall gerade die Herzratenvariabilität – eine zentrale Größe in unserem Ansatz zur Beurteilung der persönlichen Belastung – einerseits recht charakteristisch für eine bestimmte Person ist, andererseits aber mit hoher Genauigkeit gemessen werden muss, um aussagekräftig zu sein.

Im Folgenden konzentrieren wir uns daher auf das Prozessmodell und versuchen zumindest aus Sicht des Prozesses Personenbezüge zu vermeiden. Sofern statt vollständiger Anonymisierung nur eine Pseudonymisierung möglich ist, streben wir an, das Wissen um die Pseudonyme (und überhaupt um individuelle, nicht aggregierte Daten) auf einen möglichst kleinen Kreis zu beschränken.

8.2 Grundansatz zur Wahrung der wirtschaftlichen Interessen der Beteiligten

Neben den Datenschutzansprüchen der Wearable-Nutzer (Datengeber) müssen wir auch die wirtschaftlichen Interessen der übrigen Beteiligten berücksichtigen:

- **Arbeitgeber (Datennutzer):** Bei Belastungsmessungen im Arbeitsplatzkontext zahlt der Arbeitgeber für die Ausstattung der Arbeitnehmer, für deren Zeitaufwand zur Teilnahme am Messprogramm und für die Kosten des Dienstleisters, der die Messdaten auswertet und seine Befunde vorlegt. Für alle diese Aufwände darf der Arbeitgeber auch einen Nutzen erwarten. Daher sollte eine ungestörte Durchführung des Messprogramms mit unverfälschten Messergebnissen gewährleistet sein; insbesondere sollten einzelne Teilnehmer das Programm nicht böswillig hintertreiben können.
- **Dienstleister (Datennutzer):** Der Analysedienst stellt dem Arbeitgeber seine Dienstleistung, seine technische Infrastruktur sowie sein geistiges Eigentum im Bereich der Auswertung und Interpretation von Vital-Rohdaten zur Verfügung. Für diesen Aufwand darf er erwarten, dass seine Dienste ordnungsgemäß entlohnt werden und dass nicht Trittbrettfahrer die Belastungsmessung unentgeltlich nutzen.

Das Prozessmodell muss also sicherstellen, dass nur autorisierte Teilnehmer am Prozess teilnehmen können und nur in der vorgesehenen Weise, dass die Vergütung für die Teilnahme gewährleistet ist und dass nicht einzelne Rollen (Arbeitgeber, Nutzer, Dienstleister) den Erfolg des Messprogramms gefährden können. Diese Ziele sind eng mit einer sicheren Authentisierung und Autorisierung der Beteiligten verbunden, die eine Grundlage für die ordnungsgemäße Abrechnung der Dienstleistungen und für die Kontrolle des Teilnehmerkreises schaffen. Allerdings muss das Prozessmodell den Konflikt zwischen sicherer Authentisierung auf der einen und Wahrung der Anonymität auf der anderen Seite auflösen.

[3] Im Arbeitspaket 6 untersuchen die Projektpartner, welche Möglichkeiten es zur Verfremdung von Profil- und Vitaldaten gibt, und wie sehr eine solche Verfremdung das Analyseergebnis verfälscht. Dazu werden die Berechnungen einmal mit unverfremdeten und einmal mit verrauschten Daten durchgeführt und die Analyseergebnisse miteinander verglichen.

8.3 Lösungsstrategie für ein datenschutzfreundliches Prozessmodell

In Bezug auf das Prozessmodell sehen wir zusammenfassend folgende grundlegende Bedrohungen für die Beteiligten:

- Arbeitnehmer:
    - Der Arbeitnehmer könnte sich als Teilnehmer am Messprogramm durch seine Registrierungs-, Profil- und Vitaldaten, durch seine Aktivitäten oder durch die von ihm genutzten Komponenten (Wearable, Smartphone-App) verraten, so dass seine Vitaldaten seiner Person zugeschrieben werden können.
    - Die vom Wearable erfassten Daten oder die daraus abgeleiteten Befunde könnten in die falschen Hände geraten oder den grundsätzlich autorisierten Empfängern in einem nicht hinreichend anonymisierten Format offengelegt werden.
    - Ein unbefugter Dritter könnte die Identität des Arbeitnehmers annehmen, um sich den Zugriff auf die persönlichen Daten und Einstellungen des Arbeitnehmers zu erschleichen oder den Analysedienst in anderer Form zu missbrauchen.
    - Der Arbeitnehmer könnte sein legitimes Zugriffsrecht verlieren (etwa dadurch, dass er seine Zugangsdaten vergisst), was neben einer Komforteinbuße (Anfordern neuer Zugangsdaten und Neukonfiguration der Nutzerpräferenzen) auch eine Minderung der Analysegüte zur Folge haben könnte, etwa durch den Verlust von Kalibrierdaten.
- Arbeitgeber:
    - Unbefugte Dritte, zum Beispiel Angehörige der autorisierten Arbeitnehmer, könnten den Dienst auf Kosten des Arbeitgebers in Anspruch nehmen oder der Dienstleister könnte fälschlich Nutzer in Rechnung stellen, die gar nicht am Messprogramm teilgenommen haben.
    - Das Analyseergebnis könnte durch Fehlverhalten einzelner Nutzer oder durch unbefugte Dritte so stark verfälscht sein, dass die Befunde für den Arbeitgeber wertlos sind.
    - Ein Datenleck im Messprogramm könnte die Reputation des Arbeitgebers innerbetrieblich und öffentlich nachhaltig schädigen.
    - Rufschädigend könnte auch sein, wenn ein für den Arbeitgeber unvorteilhafter Befund unerlaubt an die Öffentlichkeit durchgestochen wird.
- Analysedienstleister:
    - Unbefugte Dritte könnten den Dienst unentgeltlich nutzen und damit den Dienstleister wirtschaftlich schädigen.
    - Angreifer könnten versuchen, sich unberechtigt das geistige Eigentum des Analysedienstleisters die Analyse von Vitaldaten betreffend anzueignen, um damit in Konkurrenz zum Dienstleister zu treten.
    - Ein Datenleck bei der Verarbeitung der Messdaten könnte die Reputation des Dienstleisters und damit seine Marktposition nachhaltig schädigen

Um diesen Bedrohungen zu begegnen, wählen wir folgenden Ansatz:

- **Rollentrennung:** Wir führen eine zusätzliche Rollentrennung ein und zerlegen den Analysedienst in zwei unabhängige Akteure:
    a. **Marketing & Vertrieb:** Diese Rolle ist für die Geschäftsbeziehung mit dem Kunden und die Abrechnung der Dienstleistungen zuständig. Sie muss daher die Identität des Geschäftspartners kennen. Die Rolle benötigt aber keinen Zugriff auf individuelle Vitaldaten.
    b. **Analyse-Service:** Diese Rolle verarbeitet ausschließlich die Vitaldaten anonymer Individuen, die sich zuvor als autorisierte Nutzer ausgewiesen haben, ohne dabei ihre Identität preiszugeben. Der Analysedienst erlangt als einzige Rolle (neben dem Betroffenen selbst) Kenntnis über individuelle Vitaldaten, kennt aber dafür den Geschäftspartner und die Teilnehmer nicht.

  Optional kann auch noch eine weitere Rolle, die des Gruppenaggregators, abgespalten werden. In diesem Falle sieht der Analysedienst nur Individuen, kennt aber deren Gruppenzugehörigkeit nicht. Folglich kann er auch nur Individualreports erstellen, die erst der Gruppenaggregator zu Gruppenreports verdichten kann. Der Gruppenaggregator kennt aber dann aufgrund der Rollentrennung keine individuellen Rohdaten mehr, sondern nur noch abgeleitete individuelle Belastungsdaten.

- **Keine direkte Geschäftsbeziehung zwischen Marketing & Vertrieb und Arbeitnehmern:** Alle vertraglichen Absprachen werden ausschließlich zwischen dem Arbeitgeber und Marketing & Vertrieb getroffen und die Vergütung erfolgt über den Arbeitgeber, nicht über die individuellen Teilnehmer am Messprogramm. Marketing & Vertrieb benötigt daher keine Kenntnis der Dienstnutzer.
- **Autorisierung der Teilnehmer mittels anonymer Tickets:** Teilnehmer weisen ihre Teilnahmeberechtigung durch sogenannte Registration Tokens nach, vergleichbar mit einer Eintrittskarte. Die Tokens sind fälschungssicher und werden von an den Arbeitgeber verkauft. Sie berechtigen zur einmaligen Teilnehmerregistrierung und verfallen nach Gebrauch. Für deren Ausgabe an autorisierte Nutzer ist allein der Arbeitgeber zuständig. Dabei muss er gewährleisten, dass die Tickets ohne Personenbezug zufällig den Teilnehmern zugeteilt werden. Dies stellt sicher, dass nur berechtigte, zahlende Teilnehmer den Dienst in Anspruch nehmen und dass sie anhand ihrer Registrierungstickets nicht identifiziert werden können.
- **Informationsaustausch zwischen Arbeitnehmer und Analyse-Service nur mittels nicht-personalisierter Smartphone-App:** Teilnehmer am Messprogramm nutzen eine anonyme Smartphone-App, um ihre Vitaldaten an den Analyse-Service zu übermitteln; umgekehrt erhalten sie alle Mitteilungen und Befunde des Analyse-Services ausschließlich über diese App. Der Analyse-Service kann so anonymen Kontakt zum Teilnehmer halten, ohne dessen Identität oder Anschrift zu kennen. Die nicht personalisierte Smartphone-App dient den Betroffenen auch dazu, ihre Betroffenenrechte geltend zu machen und informationelle Selbstbestimmung auszuüben. Dazu nutzen sie ihre Teilnehmer-ID und ihr Passwort, ohne dabei ihre wahre Identität preisgeben zu müssen.

Ziel dieser Strategie ist es, eine Offenlegung nicht-anonymisierter Daten zuverlässig zu unterbinden, solange sich nicht wenigstens zwei verschiedene Rollen verbünden, um sich gegen die Teilnehmer zu verschwören. Zum Beispiel kennt der Analyse-Service zwar die Daten der Teilnehmer und weiß, mit welchem Ticket sie sich autorisiert haben. Um aber die Identität des Ticketinhabers auszuspähen,

müsste er den zugeordneten Arbeitgeber kennen und Informationen über die Ticketvergabe beim Arbeitgeber einholen, wäre also auf dessen Kooperation angewiesen. Umgekehrt könnte der Arbeitgeber zwar versuchen, bei der Zuordnung von Tickets an die teilnehmenden Arbeitnehmer zu tricksen; den Zugriff auf die Vitaldaten würde er dennoch nur unter Mithilfe des Analyse-Service erhalten. Der Analysedienst seinerseits hat aber keine direkte Berührung mit dem Arbeitgeber, denn diesen Kontakt stellt Marketing & Vertrieb her, ohne die Information mit dem Analysedienst zu teilen.

Der Ansatz, dass eine Rolle allein nur sehr begrenzten Schaden anrichten kann, soll insbesondere vor Innentätern schützen. Würde etwa ein unzufriedener Mitarbeiter des Analyse-Services Vitaldaten ins Internet stellen, so wäre die Datenschutzverletzung überschaubar, solange niemand außer dem Teilnehmer selbst das Pseudonym des Teilnehmers auflösen kann: Die Daten wären höchstens aufgrund ihrer Eigenschaften und mit zusätzlichem Kontextwissen einer Person zuzuordnen, sofern es personenbeziehbare Vergleichsdaten mit den gleichen charakteristischen Merkmalen gibt. Dies wäre aber in jedem Einzelfall ein recht mühseliger Vorgang. Ein Innentäter würde sich also schwertun, die Identität eines größeren Teilnehmerkreises großflächig zu enttarnen, solange er nicht Unterstützung durch einen Innentäter bei einem anderen Rolleninhaber erhält.

8.4 Systematische Bedrohungsanalyse zur Ermittlung des Schutzbedarfs

Um den genauen Schutzbedarf zu ermitteln, den der Abschnitt 8.3 skizzierte Lösungsansatz befriedigen muss, werden zunächst die potenziellen Bedrohungen systematisch und umfassend identifiziert. Dazu bedienen wir uns der in [1] 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. Um also systematisch alle Bedrohungen zu ermitteln, stellen wir uns folgende Fragen:

- Threat Agent
    - Wer könnte ein Interesse daran haben, das System und seine Nutzer anzugreifen?
      Als Angreifer kommen unbeteiligte Dritte in Frage, die eigentlich keinen regulären Zugriff auf das System haben sollten. Aber auch die beteiligten Stakeholder, etwa die autorisierten Nutzer oder der Hersteller des Systems, könnten versucht sein, das System für unrechtmäßige Zwecke zu missbrauchen oder dessen Betrieb zu stören.
    - Was wären mögliche Angriffsmotive des jeweiligen Angreifers?
      Die Spanne reicht von purem, ungezieltem Vandalismus über gezielte Sabotage bis hin zu unberechtigtem Ausweiten der eigenen Zugriffsprivilegen, um etwa wertvolle Daten auszuspähen.
- Asset
    - Was sind die schützenswerten Güter des Systems und seiner legitimen Stakeholder?
      Für eine umfassende Betrachtung ist es zweckmäßig, Assets zu unterteilen in die Unterkategorien Informations-Assets (Daten und Programmcode), Funktions-Assets (Prozesse und Funktionen) und physische Assets (Hardware). Jede Unterklasse hat charakteristische Schutzbedarfe.
    - Welche Sicherheitsgrundwerte eines schützenswerten Guts ist relevant?
      Bei Informations-Assets steht meist deren Integrität, Verfügbarkeit und gegebenenfalls deren Vertraulichkeit im Vordergrund. Bei Funktions-Assets ist vor

allem Integrität, Verfügbarkeit, korrekte Autorisierung und gegebenenfalls Zurechenbarkeit vor Bedeutung. Bei physische Assets muss vor allem auf deren Unversehrtheit und Verfügbarkeit geachtet werden sowie auf deren Authentizität, um nicht durch minderwertige Produktfälschungen Schaden zu erleiden.

- Adverse Action:
    - Welche grundlegende Wirkung könnte ein Angreifer anstreben?
      Die Analyse kann hier zunächst auf die von Microsoft [2] propagierten Kategorien *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service* und *Elevation of Privilege* (die sogenannten STRIDE-Kategorien) zurückgreifen und diese dann Asset-spezifisch verfeinern.

Für unsere Bedrohungs- und Risikoanalyse sind nur solche Bedrohungen von Interesse, die einen Schaden verursachen, also eine aus Sicht eines Stakeholders relevante Eigenschaft eines Assets (z. B. dessen Integrität, Vertraulichkeit oder Verfügbarkeit) beeinträchtigen. Angriffe, die dem Angreifer einen Nutzen bieten, ohne dabei aber die legitimen Stakeholder-Interessen zu berühren, können in der Analyse ignoriert werden.

8.4.1 Threat Matrix

Um die Bedrohungen auf diese Weise im 3-Tupel-Format zu erheben, empfiehlt sich eine Bedrohungsmatrix (siehe [1], Abschnitt 5.2). Die Spalten der Bedrohungsmatrix repräsentieren je einen Angreifertypus.

Solch ein Typus ist charakterisiert durch seine *Zugriffsprivilegien* (Handelt es sich um einen autorisierten Stakeholder oder einen außenstehenden Dritten? Verfügt der Angreifer über besondere Zugriffsprivilegien?), seine *Fähigkeiten* (Verfügt der Angreifer über Spezialwissen und besondere Fertigkeiten?) und seine verfügbaren *Angriffsressourcen* (Verfügt der Angreifer über besondere Ausrüstung? Steht ihm ein großer Zeitraum für Angriffsversuche zur Verfügung? Kann er auf weitere Experten zurückgreifen?). Außerdem zeichnet sich jeder Typus durch seine individuellen *Angriffsmotive* aus (Welche ideellen oder materiellen Ziele verfolgt der Angreifer? Was kann er durch einen Angriff gewinnen und welchen Schaden kann er damit anderen zufügen?). Um das Spektrum relevanter Angreifertypen abzubilden, wählt der Analyst repräsentative Klassen von Angreifern und charakterisiert deren erwarteten Angriffsmotive und deren Schadenspotential.

Die Zeilen der Bedrohungsmatrix repräsentieren je einen bedrohten Assettypus. Sie sind, wie oben beschrieben, in drei Unterabschnitte gegliedert, je einen für Informations-Assets, Funktions-Assets und physische Assets. Die Analyse startet hier zunächst mit wenigen, grundlegenden Assettypen. Bezüglich Informations-Assets können zum Beispiel Konfigurationsdaten, Anwendungsdaten und Programmcode als Startpunkt dienen.

Assetklassen können bei Bedarf verfeinert werden. So kann man etwa bei den Anwendungsdaten zwischen personenbezogenen und nicht-personenbezogenen Daten unterscheiden, wenn für die beiden Unterklassen unterschiedliche Angriffe oder unterschiedlicher Schutzbedarf besteht. Eine Verfeinerung sollte aber nicht ohne Not erfolgen, sondern nur, wenn für die Unterklassen unterschiedliche Adverse Actions in Frage kommen.

Für jede Bedrohung der Form (Threat Agent, Asset, Adverse Action) wird in der Tabelle im Schnittpunkt von Angreiferspalte (Threat Agent) und Wertezeile (Asset) die jeweilige Angriffsaktion (Adverse Action) eingetragen. Die Zellen der Bedrohungsmatrix füllen sich während der Analyse so nach und nach mit

möglichen Angriffsszenarien, die von dem jeweiligen Angreifer auf das jeweilige schützenswerte Gut ausgehen.

Abbildung 3 zeigt eine beispielhafte Bedrohungsmodellierung des von uns betrachteten Anwendungsfalls (»Kontrolle der physischen und mentalen Belastung am Arbeitsplatz«) mittels Bedrohungsmatrix. Im Beispiel wird grundlegend zwischen nicht-autorisierten und autorisierten Angreifern unterschieden.

	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	**Marketing Service (MS)** selling WearPrivate solution to EMP	**App Developer (AD)** providing the software for the WearPrivate App
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 access 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 (→ invalid 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)	* May want to **sell personal identifiable data** to interested parties (e.g., to employers or insurance companies) * May **charge employers for more analyses than actually performed** (fee fraud)	* May want to **exfiltrate personal identifiable data** to interested parties * May secretly **support re-identification of PRTs** for the benefit of a third party by tagging messages or tamper with PRTs' privacy preference settings
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		Exfiltrating personal identifyable data of PRT PRT_RE-IDENT PRT_DATA_DISCLOSURE
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		Exfiltrating personal identifyable data of PRT PRT_RE-IDENT PRT_DATA_DISCLOSURE
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		Exfiltrating personal identifyable data of PRT PRT_RE-IDENT PRT_DATA_DISCLOSURE
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 unnecessarily 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	Spoofing ticket usage to perform ticket fraud with respect to the employer TICKET_FRAUD Encoding hidden identifying information into the ticket codes to assist in re-identification PRT_RE-IDENT	Exfiltrating PRT credentials to spoof PRT identity IDENTITY_THEFT

Abbildung 3 Ausschnitt einer beispielhaften Bedrohungstabelle

Unter den nicht-autorisierten Angreifertypen werden nur zwei besonders herausgehoben: Plattformbetreiber der verwendeten Cloud-Plattform sowie Personen, die autorisierten Nutzern nahestehen und daher von diesen mit Zugangsinformationen versorgt werden könnten. Alle sonstigen Angreifer werden zusammenfassend als unautorisierte Dritte modelliert.

Zu den autorisierten potenziellen Angreifern zählen die Nutzer, deren Arbeitgeber, der Analyse-Dienst, Marketing & Vertrieb sowie der Entwickler der Smartphone-App. Jeder dieser Stakeholder hat individuelle Motive, das System und seine Nutzer anzugreifen.

Abbildung 3 zeigt nur einen kleinen Ausschnitt der betrachteten Informations-Assets, die potenziell bedroht sind. Die vollständige Tabelle (siehe Anhang A) enthält weitere Informations-Assets sowie entsprechende Abschnitte für Funktions-Assets und physische Assets.

Nachdem das Analyseteam die Bedrohungsmatrix Schritt für Schritt vervollständigt hat, bis den Analysten keine relevanten neuen Threats, Assets oder Adverse Actions mehr in den Sinn kommen, werden die einzelnen Zellen der Matrix noch einmal in einer Gesamtschau inspiziert. Dabei lassen sich wiederkehrende, vergleichbare Bedrohungen zusammenfassen, die in ähnlicher Weise von unterschiedlichen Angreifern auf unterschiedliche Assets ausgehen. Für jede solche Bedrohung wird ein Name vergeben. Dieser Name (in Abbildung 3 in roten Großbuchstaben zu erkennen) bezeichnet ein gemeinsames Bedrohungsszenario, und er wird jetzt allen betroffenen Zellen zugeordnet.

So werden der Reihe nach alle relevanten Bedrohungsszenarien benannt, bis alle befüllten Zellen der Matrix vollständig durch zugeordnete Bedrohungsszenarien überdeckt sind. Weil von einem Angreifer unterschiedliche Angriffsaktionen auf ein Asset ausgehen können, kann es mehrere Tupel der Form (Threat Agent, Asset, *) mit unterschiedlichen Adverse Actions geben. Dementsprechend werden diese Einträge dann auch mehreren verschiedenen Bedrohungsszenarien zugeordnet, so dass die entsprechende Zelle dann mehrere rote Bedrohungsnamen enthält.

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
SABOTAGE	Subvert the monitoring program (e.g., in order to enforce data privacy at the workplace or to harm EMP)
ENTITY_SPOOFING	Falsely claim to be certain entity within the monitoring program (e.g., spoof the role of a communication endpoint or a hardware device)
IP_DISCLOSURE	Disclose intellectual property of AD or of AS
TROJAN_HORSE	Implant malicious code into Smartphone app or service software
CLOUD_INFILTRATION	Infiltrate cloud services or AP-Cloud communication to subvert the stress monitoring
INTRANSPARENCY	Conceil essential security- or privacy information from PRT (e.g., notification about security incidents, forwarding of personal data to other parties, or the analysis of certain health parameters)
JAIL_BREAK	Run Smartphone App on a jail-breaked device, thus undermining the built-in security and privacy mechanisms of the stress monitoring service

Abbildung 4 Beispielhafte abgeleitete Bedrohungsdefinitionen aus der Bedrohungstabelle gemäß Abbildung 3

8.4.2 Risiko-Bewertung

Nach diesem Verfahren erhält man schließlich eine Liste der potenziell relevanten Bedrohungen, wie in Abbildung 4 ausschnittweise dargestellt ist. Das Analyseteam wird nun versuchen, für jede Bedrohung das Bedrohungsrisiko zu bewerten. Das Risiko bestimmt sich aus der Experteneinschätzung der Wahrscheinlichkeit oder Machbarkeit eines erfolgreichen Angriffs sowie dessen Schadenshöhe. Die Risikobewertung dient dazu, vernachlässigbare Risiken aus der weiteren Betrachtung auszuschließen und die als besonders relevant erachteten Risiken zu priorisieren.

Mit der Risikobewertung endet der Prozessschritt *Threat Analysis and Risk Assessment* (TARA). Es gilt nun, für jede Bedrohungen geeignete Gegenmaßnahmen zu entwickeln, um die Bedrohung zu beseitigen oder zumindest auf ein erträgliches Maß zu reduzieren. Als Leitlinie für die Gegenmaßnahmen dienen dabei die in Abschnitt 8.3 skizzierten Lösungsideen, die im Folgenden zu spezifischen Sicherheitsanforderungen konkretisiert werden müssen.

8.4.3 TPAxO-Matrix

Der Schutzbedarf des Systems ergibt sich jedoch nicht nur aus den Bedrohungen, denen das System ausgesetzt ist. Darüber hinaus gelten für das System, das persönliche Daten erfasst und datenschutzrelevante Funktionen bereitstellt, auch allgemeine gesetzliche Vorgaben sowie – im Allgemeinen – auch domänenspezifische Standards, Best Practices oder Qualitätsansprüche des Herstellers für seine Produktpalette. In der von uns angewendeten Analysemethode werden diese Vorgaben zusammenfassend als *Security Policies* bezeichnet (siehe [1], Abschnitt 5.4).

Security Policies sind Richtlinien, die Erfahrungswissen widerspiegeln, ohne dabei ausdrücklich auf eine bestimmte Bedrohung zu verweisen. So sind etwa die Bestimmungen der Datenschutz-grundverordnung (DSGVO) aufgrund zahlreicher vorangegangener Datenschutzverstöße formuliert worden, die anerkannten ethischen Grundsätzen und den Grundrechten von Individuen

zuwiderlaufen. Die DSGVO gilt nach dem Inkrafttreten unabhängig davon, ob für jede einzelne Bestimmung im System eine spezifische Bedrohung ausgemacht wurde.

Ergänzend zur TARA, in der die relevanten *Threats* ermittelt wurden, werden daher die einschlägigen gesetzlichen Bestimmungen, Domänenstandards, Entwicklerrichtlinien und Best Practices ausgewertet, um die relevanten Security Policies zu ermitteln. Für jede Security Policies sind dann im Folgenden geeignete Sicherheitsanforderungen abzuleiten, um die Einhaltung der Policy zu gewährleisten.

Als Hilfsmittel dient dabei eine sogenannte TPAxO-Matrix[4] (siehe [1], Kapitel 6). Die Matrix listet in ihren Zeilen alle zuvor ermittelten Threats (T) und Security-Policies (P). Diesen Einträgen werden nun in den Matrixspalten geeignete Sicherheitsziele (sogenannte Objectives: O) zugeordnet, die dazu dienen, die Bedrohung zu bekämpfen beziehungsweise die Security Policy durchzusetzen. Dabei bedarf es mitunter mehrerer, sich ergänzender Sicherheitsziele, um einer einzelnen Bedrohung ausreichend zu begegnen oder eine Policy überzeugend durchzusetzen.

Die Zeilen der Matrix gliedern sich in drei Abschnitte. Neben den Abschnitten für Threats und Policies gibt es zusätzlich noch einen Abschnitt für getroffene Annahmen (Assumptions: A). Annahmen bezeichnen Sachverhalte, die aus Sicht des Analyseteams als gegeben vorausgesetzt werden (siehe [1], Abschnitt 5.5). Die Ergebnisse der Analyse und die daraus abgeleitete Sicherheitslösung gelten nur vorbehaltlich dieser Annahmen.

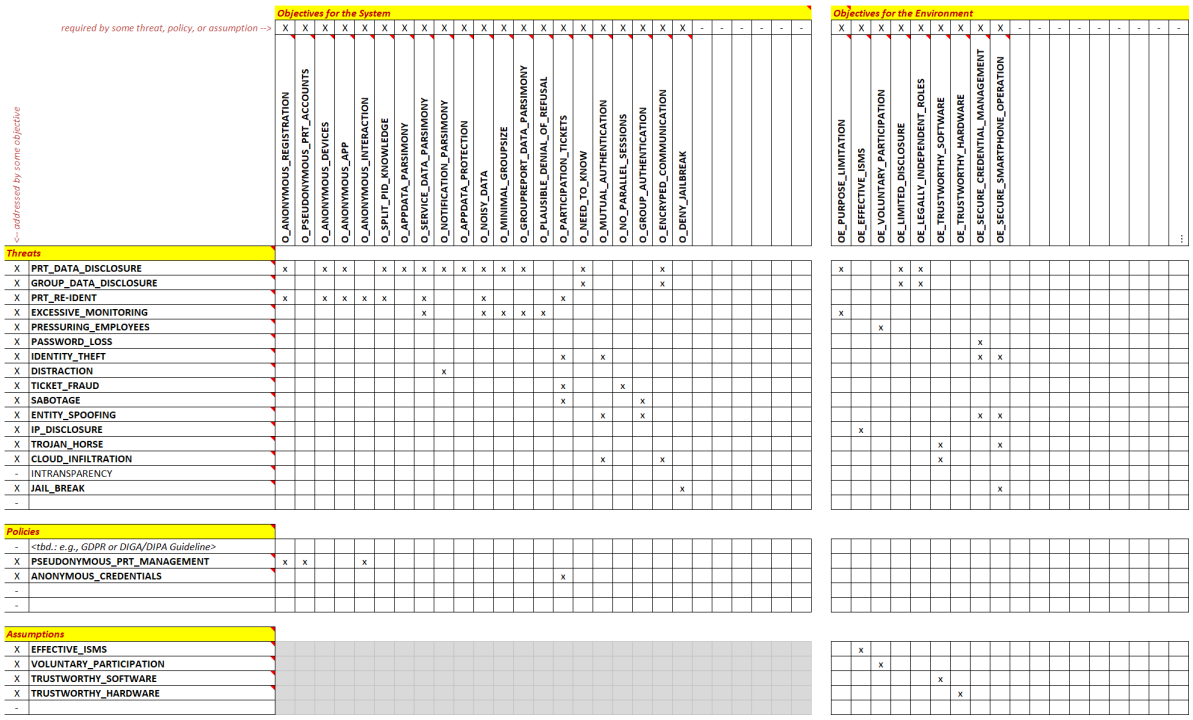

Abbildung 5 Beispielhafte TPAxO-Matrix für unseren Anwendungsfall »Belastungsmessung am Arbeitsplatz«

Abbildung 5 zeigt eine beispielhafte TPAxO-Matrix. Wie man sieht, ist jedem in der TARA-Phase definierten Threat (vgl. Abbildung 4) und jeder geltend gemachten Policy eine Reihe von Sicherheitszielen (Objectives) zugeordnet. Die Sicherheitsziele untergliedern sich in Ziele für das

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

System und Ziele für dessen Umgebung. Die System Objectives bezeichnen Ziele, die innerhalb des Systems technisch umgesetzt werden sollen. Im Unterschied dazu bezeichnen Environment Objectives Ziele, die außerhalb des Systems realisiert werden sollen, entweder durch nichttechnische Prozessvorgaben (z. B. als Organisationsanweisungen, die bestimmte Handlungsweisen vorgeben, wie etwa ein Vier-Augen-Prinzip) oder durch technische Lösungen, die von Partnersystemen außerhalb der betrachten Analysegrenzen realisiert werden (z. B. durch eine vorgeschaltete Firewall oder ein Intrusion Detection System).

Das Ziel einer Sicherheitanforderungsanalyse besteht nun darin allen Zeilen der TPAxO-Matrix –also allen Threats, Policies und Assumptions – entsprechende Objectives zuzuordnen, um allen Threats zu begegnen, alle Policies durchzusetzen und alle Annahmen zu erfüllen. Am Ende muss jede Zeile mindestens ein Kreuzchen enthalten (alle Threats, Policies und Assumptions wurden betrachtet), und jede Spalte ebenso (jede Objective dient einem konkreten Zweck). Da Annahmen als gegeben betrachtet werden, enthält das System selbst keine Mechanismen, um deren Gültigkeit zu gewährleisten. Daher werden Assumptions in der TPAxO-Matrix auch ausschließlich Environment Objectives zugeordnet, aber niemals System Objectives, während Threats oder Policies eine Kombination aus System Objectives und Environment Objectives zugeordnet werden kann.

Alle Objectives erhalten einen eindeutigen Namen und eine zugeordnete Zieldefinition, die in der Matrix als Kommentar an die entsprechende Zelle angeheftet werden kann. Die Vervollständigung der TPAxO-Matrix ist in der Regel ein iterativer Prozess, denn durch die Vorgabe eines Sicherheitsziels werden mitunter neuen schützenswerte Güter eingeführt, für die eine Bedrohungsanalyse neue, Bedrohungen identifizieren kann, die dann als zusätzliche Zeilen in die TPAxO-Matrix aufgenommen werden und entsprechende Sicherheitsziele nach sich ziehen.

Wenn zum Beispiel »mangelnde Nachvollziehbarkeit« als Bedrohung identifiziert worden ist, dann könnte als Gegenmaßnahme das Sicherheitsziel »Protokollierung aller relevanten Ereignisse« abgeleitet werden. Das hat jedoch zur Folge, dass im System ein Ereignisprotokoll angelegt werden muss, dessen Integrität und Verfügbarkeit dann aber potenziell bedroht sein kann, was eine neues Sicherheitsziel »Schutz des Ereignisprotokolls« nach sich zieht.

Das Analyseteam erstellt und vervollständig nach dem beschriebenen Verfahren die TPAxO-Matrix. Als Ergebnis ergibt sich so eine Liste von technischen Zielen und nicht-technischen Umgebungszielen. Die letztgenannten werden dokumentiert und in das Benutzerhandbuch oder die Systemdokumentation des Systems übertragen: Ein sicherer Betrieb des Systems ist nur gewährleistet, wenn alle Umgebungsanforderungen erfüllt sind. Die technischen Ziele bilden die Grundlage für eine detaillierte Anforderungsanalyse, bei die abstrakten Sicherheitsziele für das System zu konkreten Systemanforderungen auf der Systementwurfsebene verfeinert werden. Diese Anforderungsspezifikationen sollten SMART sein:

- Specific: Was genau soll erreicht werden?
- Measurable: Wann gilt die Anforderung als erfüllt?
- Attainable: Ist die Anforderung mit den verfügbaren Ressourcen umsetzbar?
- Result-based: Spezifiziere das Ziel, nicht den Weg dorthin
- Time-bound: Bis wann soll die Anforderung umgesetzt sein?

8.5 Abgeleitete Anforderungen an den WearPrivate-Demonstrator

Aufgrund der in Abschnitt 8.4 identifizierten Bedrohungen, den daraus abgeleiteten Sicherheitszielen und der vorgeschlagenen Lösungsstrategie ergeben sich konkrete Anforderungen an die Realisierung unseres Systems zur Erfassung von Belastungen am Arbeitsplatz. Diese lassen sich in Arbeitnehmeranforderungen (R_AN), Arbeitgeberanforderungen (R_AG), Anforderungen bezüglich Marketing & Vertrieb (R_MV) und Anforderungen bezüglich des Analyse-Services (R_AS) untergliedern.

Tabelle 1 fasst die Bedrohungen, abgeleiteten Ziele und detaillierten Anforderungen an den Analyseprozess zusammen, gegliedert nach den Rollen Arbeitnehmer (AN), Arbeitgeber (AG), Marketing & Vertrieb (MV), Analyse-Service (AS) sowie Entwickler (E).

Tabelle 1 **Bedrohungen, resultierende Ziele und abgeleitete Anforderungen aus Sicht der verschiedenen Rollen: Arbeitgeber, Arbeitnehmer, Analysedienstleister, Marketing & Vertrieb sowie Entwickler.**

Bedrohung (Threat)	Ziel (Objective)	ID	Anforderung (Requirement)
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 Angaben zur Identität des Nutzers (z. B. Name, Adresse, Ausweisnummer) niemals 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*
Re-Identifizierung anhand der Registrierungs-Credentials T_PRT_RE-IDENT	Registrierungs-Credentials werden zufällig ohne spezifische Personenzuordnung vergeben O_ANONYMOUS_REGISTRATION	R_AN6	Die AN entnehmen ihren Freischaltcode RT unbeobachtet einer Grabbelkisten oder erhalten einen versiegelten »PIN-Brief«, den MV dem AG für alle Teilnehmer zur Verfügung stellt.
	Registrierungs-Credentials tragen keine personenbezogene Kennzeichnung (z. B. Bezug zur Identität, zu Vital- oder Kalibrierungsdaten, zum Geschlecht, ...) O_ANONYMOUS_REGISTRATION	R_AN7	Die Ausgabe der Freischaltcodes gemäß Anforderungen AN3 und AN6 ist so zu gestalten, dass AN ihre Codes innerhalb er Gruppe untereinander nach Belieben tauschen können. (Perspektivisch im gesamten Unternehmen, momentan beschränkt auf die Gruppe)
Re-Identifizierung anhand der Vitaldaten oder Stammdaten	AG, MV oder andere AN erhalten keinen Einblick in die Kalibrier-, Vital- oder	R_AN8	Der Datenaustausch (Registrierung, Login, Nutzerpräferenzen, Vitaldaten, individuelle

(z. B. Alter, Geschlecht) T_PRT_RE-IDENT	Analysedaten eines individuellen AN O_SPLIT_PID_KNOWLEDGE O_ANONYMOUS_INTERACTION O_GROUPREPORT_DATA_PARSIMONY O_ENCRYPTED_COMMUNICATION		Analyseergebnisse) der AN erfolgt ausschließlich mit AS, nie mit AG, MV oder anderen AN
		R_AN9a	Die Kommunikation zwischen Wearable und Smartphone erfolgt verschlüsselt
		R_AN9	Die Kommunikation zwischen AN (Smartphone) und AS ist Ende-zu-Ende-verschlüsselt
		R_AN10	Die für den Dienst benötigten Daten eines Individuums werden nur unter einem Pseudonym PSEU ohne Bezug zu irgendwelchen persönlichen Merkmalen geführt, und sie sind ausschließlich für AS sowie für den Pseudonyminhaber zugreifbar.
	Vital- und Kalibrierungsdaten (Alter, Gewicht, Körpergröße, ...) sollen so weit verrauscht werden, wie es möglich ist, ohne die Güte der Belastungsmessung zu sehr zu beeinträchtigen. O_NOISY_DATA	R_AN11	Soweit es die Analysequalität nicht gefährdet, werden die Rohdaten von der Smartphone-App vor einer Weitergabe an AS möglichst schon vorverarbeitet, um den persönlichen »Fingerabdruck« bestmöglich zu verwischen. (z. B.: BMI statt Größe und Gewicht, Jahrgangskohorte statt Geburtsdatum). Diese Anforderung umfasst auch die Vitaldaten (Puls, HRV, Acc, ...). *siehe auch Verrauschung, R_AN52*
Re-Identifizierung aufgrund zu geringer Gruppengröße T_PRT_RE-IDENT	Die Erstellung von Gruppenreports erfordert eine Mindestgröße gmin; bei weniger Teilnehmern wird kein Gruppenreport erstellt O_MINIMAL_GROUPSIZE	R_AN12	Der Gruppenreport gibt Analysedaten nur für solche Intervalle preis, für die von wenigstens gmin Individuen entsprechende Rohdaten vorliegen. Inaktive Gruppenmitglieder werden beim gmin-Kriterium nicht mitgezählt
Re-Identifizierung durch Scheinidentitäten in einer Gruppe (d.h. AG füllt Gruppe mit nur einem Mitglied mit Pseudoteilnehmern auf) T_PRT_RE-IDENT T_ENTITY_SPOOFING	AS prüft die erhaltenen Rohdaten auf Plausibilität, um auszuschließen, dass fingierte Nutzerkennungen fingierte Vitaldaten simulieren. Verdächtige Datenquellen werden beim gmin-Kriterium nicht mitgezählt	R_AN13	AS ignoriert Rohdaten, die offenbar nicht von einem authentischen Teilnehmer per Wearable als echte Aktivitäten gemessen wurden. Verdächtige Datenquellen werden beim gmin-Kriterium (siehe R_AN12) nicht mitgezählt.
	Die App bietet den Teammitgliedern die Möglichkeit, ihre Gruppenmitgliedschaften zu vergleichen. Sie können sich damit vergewissern, dass alle Teamkollegen wirklich im gleichen Team registriert sind O_GROUP_AUTHENTICATION	R_AN14	Die Gruppennummer, unter der ein Nutzer sich mit seiner Smartphone-App registriert hat, wird im Icon der App (oder auf anderem Weg innerhalb der App, ohne jedoch persönliche Daten des Nutzers dabei preiszugeben) angezeigt, so dass Nutzer ihre Gruppenzugehörigkeiten unmittelbar per App vergleichen können.
Re-Identifizierung durch markanten Registrierungs- oder Kündigungszeitpunkt (z. B. »Nachzügler«) oder markanten Gruppenein- oder -austritt (z. B. Kündigung) T_PRT_RE-IDENT	Gruppenreports geben keinen Aufschluss über die genaue Gruppenstärke, sondern nur über die Einhaltung des gmin-Kriteriums O_GROUPREPORT_DATA_PARSIMONY	R_AN15	Gruppenreports zeigen keine individuellen Marker für die einzelnen Mitglieder einer Gruppe, sondern nur geeignet statistisch aufbereitete Darstellungen (z. B. Quantile, Intervallbreiten)
Re-Identifizierung durch Fehler oder Vorsatz bei AG, MV, AS oder anderen AN T_PRT_RE-IDENT T_CLOUD_INFILTRATION	Registrierung, Kündigung oder Nutzung des Dienstes ist so zu gestalten, dass eine einzelne Rolle (andere AN, AS, MV oder AG) allein die Identität eines Nutzers nicht mit vertretbarem Aufwand aufdecken kann. Ein »Datenleck« bei einer einzelnen Stelle soll die Anonymität des AN noch immer wahren. O_SPLIT_PID_KNOWLEDGE O_ANONYMOUS_REGISTRATION O_ANONYMOUS_INTERACTION	R_AN16	AG kennt nicht den genauen Freischaltcode oder das vom AN jeweils genutzte Wearable
		R_AN17	AG und MV sehen nur aggregierte und weiterverarbeitete Gruppendaten, aber keine Individualdaten (auch nicht anonymisiert) der AN
		R_AN18	AS kennt weder AG noch AN, sondern sieht nur das unpersönliche Registrierungstoken (Freischaltcode) und später das willkürliche Pseudonym
		R_AN19	MV sieht keine Individualdaten (auch nicht anonymisiert), sondern nur die Gruppenreports in geeigneter Aggregation
		R_AN20	MV kennt keine AN, sondern nur den AG, und MV hat keine Informationen über die wahre Identität der gebildeten Gruppen (also deren Funktion innerhalb der Organisation des AG)
Re-Identifizierung anhand der Wearable-Hardware oder des	Zu Zuteilung von Wearables an AN erfolgt zufällig ohne Registrierung der genauen	R_AN21	Die AN besorgen sich die Wearables entweder selbst aus einer unabhängigen

Smartphones T_PRT_RE-IDENT	Hardware-ID O_ANONYMOUS_DEVICES		Bezugsquelle oder AG stellt sicher, dass die Zuteilung unbeobachtet und zufällig erfolgt (z. B. per Grabbelkiste)
	Bei der Nutzung des Dienstes wird keine Hardware-ID des Wearables oder des Smartphones und keine Betriebssystem-Kennung übertragen (z. B. Seriennummer) O_ANONYMOUS_DEVICES O_ANONYMOUS_INTERACTION	R_AN22	Die Smartphone-App speichert oder verwertet keine Hardware-ID des Wearables (z. B. Seriennummer oder MAC-Adresse), oder des Betriebssystems und gibt entsprechende Informationen auch nicht an AS oder andere Kommunikationspartner weiter.
Nichtautorisierte Offenlegung der individuellen AN-Daten (unabhängig von ihrer Anonymisierung) T_PRT_DATA_DISCLOSURE	AS verwaltet Roh- und Analysedaten der Nutzer unter strenger Zugriffskontrolle (Need-to-know-Prinzip) und automatisiert seine Prozesse so weit, dass ein Zugriff durch AS-Mitarbeiter kaum je notwendig ist O_NEED_TO_KNOW	R_AN23	AS und seine Mitarbeiter werden auf die Prinzipien des Datenschutzes und der DSGVO verpflichtet und sorgen für den erforderlichen technischen Schutz der verarbeiteten Daten
	Aus Gruppenberichten können keine verwertbaren Hinweise auf individuelle Vitaldaten einzelner AN abgeleitet werden. O_GROUPREPORT_DATA_PARSIMONY		*siehe Anforderungen aus Datensicht*
	AS leitet Gruppenberichte ausschließlich an MV weiter, und MV leitet sie ungelesen an AG weiter. O_NEED_TO_KNOW O_MUTUAL_AUTHENTICATION O_ENCRYPTED_COMMUNICATION	R_AN24	AS erfährt von MV nicht die Identität des AG und erstellt die geeignet anonymisierten Gruppenberichte blind, ohne Kenntnis des Empfängers. Die Gruppenberichte werden an MV weitergegeben, der auf Seiten des Dienstes als einziger die Identität des AG kennt, und von diesem dem AG zugestellt.
		R_AN25	MV und seine Mitarbeiter werden auf die Prinzipien des Datenschutzes und der DSGVO verpflichtet. MV sorgt für den technischen Schutz der AG-Informationen und Gruppenberichte und gibt die Daten des AG nicht an AS weiter.
	Die Sicherheit der Daten wird sichergestellt und kontinuierlich verbessert OE_EFFECTIVE_ISMS	R_AN25a	Es wird ein ISMS (Information Security Management System) etabliert. (Die Forderung ergibt sich aus Art. 32 DSGVO, vgl. https://www.dr-datenschutz.de/isms-dsgvo-was-unternehmen-beachten-sollten/)
Sozialer Druck, gegen den eigenen Willen an einem Messprogramm teilzunehmen T_PRESSURING_EMPLOYEES	Niemand darf vom AG zur Teilnahme an einem Messprogramm gezwungen werden OE_VOLUNATARY_PARTICIPATION	R_AN26a	Die Smartphone-App bietet dem Nutzer die Wahlmöglichkeit, die Teilnahme an einer Gruppenauswertung abzulehnen. *siehe R_AN49*
	Die App (ggf. zusammen mit dem Wearable) bietet dem Nutzer eine Möglichkeit, eine Nutzung plausibel vorzutäuschen O_PLAUSIBLE_DENIAL_OF_REFUSAL	R_AN26	Eine registrierte App und ein gekoppeltes Wearable zeigen nicht an, ob sie tatsächliche Messdaten an AS weitergeben oder dies nur plausibel vorspiegeln.
	Ob die Teilnahme am Messprogramm (d.h. Bereitschaft zur Registrierung) zugleich auch die Teilnahme an Gruppenberichten zwingend impliziert, muss vorher zwischen AN und AG ausdrücklich vereinbart werden. Die Datenschutzerklärung muss die Bedingungen für ein Opt-In/Opt-Out beim Gruppenreporting eindeutig klarstellen. OE_PURPOSE_LIMITATION OE_LIMITED_DISCLOSURE	R_AN27	Im einfachsten Fall umfasst die Einverständniserklärung schon eine entsprechende Klausel, die zur Teilnahme am Messprogramm verpflichtet. Ggf. wird hier aber auch eine Möglichkeit gegeben, die Gruppenteilnahme nur plausibel vorzutäuschen. Im anderen Extremfall stellt es AG den AN ausdrücklich frei, sich überhaupt unter einer spezifischen Gruppenkennung zu registrieren oder wahlweise die Messungen nur als persönliches Bio-Feedback zu nutzen, ohne sie dem AG für Gruppenreports zur Verfügung zu stellen.
Verlust der Nutzerkennung oder des Passworts (z. B. Passwort vergessen) T_PASSWORD_LOSS	Der Verlust der Credentials wird zugunsten der Wahrung von Anonymität in Kauf genommen. O_PARTICIPATION_TICKETS	R_AN28	Bei Verlust seiner Credentials (PSEU und RT) muss sich der Anwender vollständig neu registrieren. Dazu kann ihm AG im Rahmen seines Analysekontingents einen neuen Freischaltcode RT und ggf. ein passendes Gruppenticket zur Verfügung stellen.
Verlust des Smartphones oder Wearables T_PRT_DATA_DISCLOSURE T_IDENTITY_THEFT	Ein registrierter Nutzer ist nicht an ein festes Endgerät oder Smartphone gebunden. Er kann diese Hardware jederzeit wechseln, die App neu installieren und sich dann nahtlos mit seinem Pseudonym PSEU und dem Passwort		*siehe Anforderung R_AN3*

	anmelden, ohne dass AS diese Identität verliert O_ANONYMOUS_DEVICES O_ANONYMOUS_APP O_ANONYMOUS_REGISTRATION		
	Zu jeder Zeit kann nur ein Gerät unter einem Pseudonym eingeloggt sein O_NO_PARALLEL_SESSIONS	R_AN29	AS prüft bei jeder Kontoaktaufnahme eines Smartphones, ob unter den angegebenen Credentials bereits eine Session besteht. Mehrfach-Sessions unter der gleichen Nutzerkennung werden abgewiesen.
Identitätsdiebstahl T_IDENTITY_THEFT	Jeder Erst-Registrierung (d.h., ohne zuvor schon erhaltenes Pseudonym PSEU und Passwort) mit einem Registrierungstoken RT begründet bei AS eine neue Identität O_PARTICIPATION_TICKETS		*siehe Anforderung R_AN3*
	Access-Tokens sollten möglichst wenig von anderen Personen missbraucht werden können. O_PARTICIPATION_TICKETS	R_AN30a	Die Access-Tokens sollen kurzlebig sein.
	Allein der Besitz von Wearable, Smartphone und App nützt Dritten nichts, um die Identität eines registrierten AN anzunehmen. O_MUTUAL_AUTHENTICATION O_SECURE_CREDENTIAL_MANAGEMENT	R_AN30	AN muss sich für jede Kommunikation mit AS zuvor registrieren und dann seine Authentizität mittels Pseudonym PSEU und zugehörigem Passwort nachweisen. Nur so können sie den Dienst nutzen oder die Daten des pseudonymisierten Accounts abrufen
Verlust der Privacy durch Datenleck T_PRT_DATA_DISCLOSURE	Der AN ist für den sicheren Umgang mit PSEU und Passwort selbst verantwortlich. OE_SECURE_CREDENTIAL_MANAGEMENT		*siehe Anforderung R_AN28*
	Der AN ist für die Sicherung des Zugriffs auf das Smartphone selbst verantwortlich. OE_SECURE_SMARTPHONE_OPERATION	R_AN31	Der Zugriff auf die App ist durch ein Passwort geschützt *siehe Anforderung R_AN3*
	Die App minimiert die Speicherdauer von Vital-Daten auf dem Smartphone und optional auch die Speicherdauer von weiterverarbeiteten Analysedaten auf diesem Endgerät O_APPDATA_PARSIMONY	R_AN32	Die Smartphone-App realisiert das Prinzip der Datensparsamkeit und speichert nur die unbedingt erforderlichen Daten. Sie minimiert die Speicherdauer der Daten im Smartphone.
	Sensitive Daten, die in der App gespeichert sein müssen, sollen für Unbefugte nicht auslesbar sein (etwa bei Diebstahl des Smartphones) O_APPDATA_PROTECTION OE_SECURE_SMARTPHONE_OPERATION	R_AN32b	Die Smartphone-App speichert schützenswerte Daten in verschlüsselter Form.
	Lokal in der App gehaltene, sensitive Daten sollen nicht unverschlüsselt in Backups verschoben werden O_APPDATA_PROTECTION	R_AN32c	Sensitive Daten der Smartphone-App sind so zu markieren, dass sie vom Backup-Mechanismus des Smartphone-Betriebssystems ausgenommen werden oder nur in verschlüsselter Form im Backup aufgezeichnet sind.
	Daten werden nur so lange und nur in dem Umfang gespeichert, wie es notwendig ist, um Risiken zu reduzieren. O_SERVICE_DATA_PARSIMONY	R_AN33	Die Sensordaten der ArbeitnehmerInnen, die an den Dienstleister übermittelt werden, werden nach der Auswertung schnellstmöglich gelöscht, da sie nicht mehr benötigt werden (Datenminimierung, Speicherbegrenzung). Es werden lediglich die Sensordaten der letzten 5 Minuten benötigt. Sensordaten, die älter sind, werden nicht mehr benötigt und daher gelöscht (These: 15 Minuten nach dem Upload / der ersten Verarbeitung eines Sensor-Datenpakets, wird dieses nicht mehr benötigt und kann gelöscht werden). Ggf. müssen abgeleitete Kennwerte länger gespeichert werden (z. B. Historie der ermittelten Belastungswerte). Für die Ermittlung des Ruhepulses sind die vollständigen Sensordaten nicht notwendig, hier sollte es ausreichen, z. B. nur den niedrigsten Puls, der an einem Tag gemessen wurde, zu behalten. Möchte der Dienstleister die Sensordaten länger behalten / für andere (eigene?) Zwecke nutzen, benötigt er eine entsprechende Rechtsgrundlage / Einwilligung. ArbeitnehmerInnen sollten frei entscheiden

			können, ob sie diese zusätzliche Einwilligung geben oder nicht.
Arbeitgeber verwenden die Daten zur Überwachung der ArbeitnehmerInnen T_EXCESSIVE_MONITORING	Arbeitgeber können die Daten NICHT zur Überwachung der Belegschaft verwenden O_SPLIT_PID_KNOWLEDGE O_ANONYMOUS_INTERACTION O_ENCRYPTED_COMMUNICATION	R_AN34	Der Arbeitgeber darf die Daten nicht zur Überwachung, Leistungs- und Verhaltenskontrolle verwenden (können) Anonymität der Daten: *siehe R_AN1, R_AN2, R_AN3, R_AN4, R_AN6, R_AN7* Anonymität durch Gruppenaggregation: *siehe R_AN12, R_AN13, R_AN14, R_AN15, R_AN17, R_AN19* Vertraulichkeit der Daten: *siehe R_AN5, R_AN8, R_AN9, R_AN9a, R_AN16, R_AN21, R_AN22, R_AN23* Freiwilligkeit der Teilnahme: *siehe R_AN26, R_AN26a*
Betroffene werden über Datenschutzzwischenfälle nicht hinreichend informiert oder müssen mit den Folgen von Datenschutzverstößen alleine zurechtkommen T_INTRANSPARENCY	Verantwortungsübernahme und Unterstützung bei der Folgenbehandlung O_SUPPORT_IN_ASSERTION_OF_DATA_SUBJECT_RIGHTS	R_AN35	ArbeitnehmerInnen werden über Datenschutzverstöße benachrichtigt und erhalten Unterstützung, etwaige daraus resultierende negative Folgen zu bewältigen Als Teilaspekt eines ISMS (Monitoring, Notfallkonzept, Krisenkommunikation, ...): *siehe R_AN25a*
	Nutzer werden unter Wahrung ihrer Anonymität zeitnah über relevante Datenschutzvorfälle informiert, um bei Bedarf geeignete Maßnahmen ergreifen zu können O_TRANSPARENCY_AND_SELF-DETERMINATION O_SUPPORT_IN_ASSERTION_OF_DATA_SUBJECT_RIGHTS	R_AN35b	Bei Datenschutz-relevanten Ereignissen muss die Smartphone-App eine Mitteilung erhalten. In der App muss diese Ausnahmesituation deutlich und unverzüglich zur Anzeige gebracht werden und der Nutzer ist auf das Vorliegen einer solchen Mitteilung aktiv hinzuweisen. *siehe R_AN42*
Die Nutzer verstehen nicht, wie wann und wo welche ihrer Daten verarbeitet werden; ihre Daten werden unter Umständen unabsichtlich erfasst und zur Analyse bereitgestellt (Transparenz) T-EXCESSIVE_MONITORING T_INTRANSPARENCY	Transparente Datenerhebung: * Die Wearable-Träger sind sich stets bewusst, ob ihre Vitaldaten gerade erfasst und verarbeitet werden * Die Wearable-Träger wissen stets, welche Vital- und Verhaltensdaten erfasst oder an den Analysedienst weitergeleitet werden O_DATA_PROCESSING_INFORMATION O_TRANSPARENCY_AND_SELF-DETERMINATION	R_AN36	Die Smartphone-App signalisiert jederzeit eindeutig und klar erkennbar, ob gerade Vitaldaten erfasst und verarbeitet werden oder nicht.
	Die Nutzer können jederzeit die Vitaldatenerfassung pausieren oder deaktivieren OE_VOLUNTARY_PARTICIPATION	R_AN36c	Nur Daten aus den vom Nutzer freigegebenen Verarbeitungsintervallen dürfen verarbeitet werden. Die App bietet angemessene Möglichkeiten, diese Intervalle planmäßig oder spontan festzulegen oder die Festlegung jederzeit zu revidieren
	Die Wearable-Träger sind sich stets bewusst, was mit den erfassten Profil- und Vitaldaten geschieht und zu welchen Zwecken sie erhoben werden O_DATA_PROCESSING_INFORMATION	R_AN36a	Die Smartphone-App stellt bei Bedarf nähere, auch für IT- und Medizinlaien leicht verständliche Informationen darüber bereit, welche Daten erhoben werden, nach welchen Regeln sie erhoben werden, zu welchem Zweck und wer die weiterverarbeiteten Daten einsehen kann. (Die Information kann bei Bedarf auch Verweise auf entsprechende Quellen im Internet enthalten, soweit sie zu umfangreich für die Darstellung in der App ist oder sich das Bereitstellungsformat nicht für den kleinen Smartphone-Bildschirm eignet.)
		R_AN36b	Die Aktivierung und Deaktivierung einzelner Sensoren wird in einem Verlaufprotokoll von der App erfasst und ist in der App einsehbar für einen Zeitraum T. Die Protokollierung umfasst einen Zeitstempel sowie (bei eingeschaltetem Ortungsdienst auf dem Smartphone) den aktuellen Ort des Smartphones zum Umschaltzeitpunkt.

	Transparente Datenverarbeitung O_TRANSPARENCY_AND_SELF-DETERMINATION	R_AN37	ArbeitnehmerInnen sollen Informationen darüber erhalten, welche Kennwerte aus ihren Sensordaten abgeleitet werden. *siehe R_AN36a*
	Transparenz bezüglich des Datenzugangs O_ADJUSTMENT_OF_CONSENT_TO_DATA_SENSITIVITY O_LIMITATION_OF_DATA_SENT	R_AN38	ArbeitnehmerInnen sollen Informationen darüber erhalten, wer Zugriff auf die Informationen erhält (Sensordaten + abgeleitete Kennwerte) *siehe R_AN36a, R_AN43*
	Transparenz / Awareness O_TRANSPARENCY_AND_SELF-DETERMINATION	R_AN39	ArbeitnehmerInnen sollen sich aller relevanten Datenflüsse, Datenübermittlungen, Datenverarbeitungen und Datennutzungen stets bewusst sein. *siehe R_AN36a, R_AN43*
	Betroffene werden befähigt und unterstützt, selbstbestimmte Entscheidungen in ihrem eigenen Interesse zu fällen O_TRANSPARENCY_AND_SELF-DETERMINATION	R_AN40	Das System ist auch für IT- Laien transparent und leicht bedienbar im Sinne von »Usable Security & Privacy«. Anwender werden vom System unterstützt und befähigt, selbstständig, wohlinformiert und frei ihre Entscheidungen zu treffen.
		R_AN41	Arbeitnehmer werden bei der selbstbestimmten Entscheidungsfindung und Konfiguration ihrer Präferenzen unterstützt. Unterstützung und Information erfolgen transparent und objektiv und im Zweifel eher datenschutzfreundlich. Nudging im Sinne des Dienstleisters ist zu verhindern. Teilnahme am Messprogramm generell: *siehe R_AN26* Teilnahme am Gruppenreporting: *siehe R_AN26a* Mehr oder weniger Verrauschung: *siehe R_AN11* Auswahl der zulässigen Analysen: *siehe R_AN50* Bereitstellung der Daten zu Forschungszwecken: *siehe R_AN41d* Bereitstellen der Messdaten zur Verbesserung von AS: *siehe R_AN51*
		R_AN41a	AN kann wochentagsweise Zeitfenster bestimmen, in denen eine Datenerfassung automatisch deaktiviert werden soll
		R_AN41b	AN kann die Erfassung seiner Vitaldaten auf bestimmte Geolokationen (Standort mit Umkreis) einschränken
		R_AN41c	AN kann die Datenerfassung der App jederzeit deaktivieren und reaktivieren
		R_AN41d	AN kann die Nutzung seiner Daten auf bestimmte Nutzerkreise einschränken (z. B. nur zu Forschungszwecken, zur Weiterentwicklung der Analysemodelle, ...)
	Betroffenenrechte können ohne eine Offenlegung der Identität der Betroffenen wahrgenommen werden O_ANONYMOUS_INTERACTION	R_AN42	AS bietet eine Self-Service Möglichkeit zur Wahrnehmung der Betroffenenrechte an, um die Identität der Betroffenen nicht zu offenzulegen. Betroffene legitimieren sich als Inhaber ihres Pseudonyms mithilfe ihres Passworts zum Pseudonym.
	Transparenz bzgl. der tatsächlich erfolgten Datennutzungen O_TRANSPARENCY_AND_SELF-DETERMINATION	R_AN43	Tatsächlich erfolgte Datennutzungen/-verarbeitungen sind auf Wunsch des Betroffenen zu protokollieren, um dem jeweiligen Betroffenen Transparenz bzgl. der tatsächlich erfolgten Datennutzungen/-verarbeitungen zu ermöglichen (Protokoll). Die Protokollierung erfasst den Zeitpunkt der Nutzung, den Nutzenden, die Daten, die genutzt wurden, sowie den Verwendungszweck.
Der Nutzer kann nicht selbst über seine Daten und deren	ArbeitnehmerInnen werden an der Ausübung ihrer Selbstbestimmung nicht gehindert	R_AN44	ArbeitnehmerInnen sollen auch dann noch einen (wenn auch geringeren) Nutzen haben,

Verarbeitung entscheiden (Selbstbestimmung) T_PRESSURING_EMPLOYEES T_EXCESSIVE_MONITORING T_INTRANSPARENCY	O_ANONYMOUS_INTERACTION OE_VOLUNTARY_PARTICIPATION		wenn sie ihre Selbstbestimmungsmöglichkeiten vollständig ausnutzen.
		R_AN45	ArbeitnehmerInnen dürfen keine Nachteile aus der Wahrnehmung ihrer Selbstbestimmung entstehen Plausibles Vortäuschen der Teilnahme: *siehe R_AN26*
	Kontrolle über die eigenen Daten O_TRANSPARENCY_AND_SELF-DETERMINATION	R_AN46	ArbeitnehmerInnen können für jeden relevanten Datenfluss, jede Datenübermittlung und Datenverarbeitung individuell nach ihren eigenen Vorstellungen einstellen, ob und wem und in welcher Form sie ihre Daten preisgeben (z. B. nur aggregiert oder anonymisiert oder nur an gewissen Orten oder zu gewissen Zeiten) Beschränkung auf gewisse Zeiten: *siehe R_AN41a* Beschränkung auf gewisse Orte: *siehe R_AN41b* Beschränkung auf gewisse Auswertungen: *siehe R-AN50, R_AN51* Beschränkung auf bestimmte Nutzerkreise: *siehe R-AN41d*
	Datennutzung in gewünschtem, begrenztem Rahmen zulassen OE_PURPOSE_LIMITATION OE_LIMITED_DISCLOSURE	R_AN47	Arbeitnehmer sollen AS ausgewählte Analysen ihrer Wearable-Daten gestatten können und dabei die größtmögliche Kontrolle über ihre Daten behalten. *siehe R_AN50, R_AN51*
	Daten können nur in Übereinstimmung mit den Wünschen des Betroffenen verarbeitet werden OE_PURPOSE_LIMITATION OE_LIMITED_DISCLOSURE	R_AN48	Eine Verarbeitung personenbezogener Daten – sowohl durch den Dritten als auch durch den Wearable-Hersteller –, die über das vom Anwender/Betroffenen Zugelassene hinausgeht, soll durch den Einsatz datenschutzfreundlicher Technik verhindert werden.
		R_AN49	AN sollen selbst darüber entscheiden können, ob ihre Daten zur Erzeugung eines Gruppenberichts verwendet werden dürfen. *Deckungsgleich mit R_AN26a*
		R_AN50	AN können selbst auswählen, welche Analysen sie wünschen. *siehe R_AN47*
		R_AN51	AN können selbst darüber entscheiden, ob ihre Daten für die Verbesserung des Dienstes verwendet werden dürfen. *siehe R_AN47*
	Möglichkeiten zur Selbstbestimmung / Abwägung O_NOISY_DATA	R_AN52	ArbeitnehmerInnen können zwischen der Qualität der Analyseergebnisse und Privatheit / Anonymität abwägen (3 Verrauschungsstufen). *siehe auch Verwischen von Details: R_AN11*
Unerwünschte Push-Benachrichtigungen T_DISTRACTION T_PRT_DATA_DISCLOSURE	Die Anwender sollen vor störenden Push-Nachrichten geschützt werden (z. B. in der jeweiligen Nutzungssituation kompromittierenden oder ablenkenden Mitteilung). O_NOTIFICATION_PARSIMONY	R_AN54	Vor der Zustellung einer Push-Nachricht ist eine ausdrückliche Erlaubnis einzuholen, dass solche Nachrichten erwünscht sind. Die Erlaubnis soll in einem angemessenen Nutzungskontext eingeholt werden, in denen der Anwender mit dem Aspekt von Benachrichtigungen konkret befasst ist.
		R_AN55	Push-Nachrichten dürfen keine sensitiven Vitaldaten enthalten

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*
Nichtverwertbarkeit der Analysedaten wegen mangelnder Gruppengröße T_SABOTAGE	**OPTION 1:** Die Nichtverwertbarkeit der Individualdaten für Gruppenreports wird aus Gründen der informationellen Selbstbestimmung, des Datenschutzes und der Abwehr von äußeren Zwängen in Kauf genommen O_MINIMUM_GROUPSIZE		*siehe Anforderung R_AN26*
	OPTION 2: Mit seiner Bereitschaft, überhaupt an dem Messprogramm teilzunehmen, erklärt sich der AN auch bereit, seine Individualdaten für einen Gruppenreport (hinreichende Gruppenstärke vorausgesetzt) zur Verfügung zu stellen O_MINIMUM_GROUPSIZE		*in diesem Fall keine technische Opt-Out-Möglichkeit*
Anonyme Nutzer blockieren ungenutzte Analysekontingente T_SABOTAGE	Registrierte Nutzer müssen ihre Registrierung in regelmäßigen Abständen erneuern. Erfolgt innerhalb einer festgelegten Frist keine Erneuerung, so erlischt die Nutzerkennung, ohne dass der AN sie ausdrücklich kündigen muss. O_PARTICIPATION_TICKETS	R_AG3	Eine Nutzerregistrierung ist nur für ein zuvor festgelegtes Zeitintervall T gültig. Danach erlischt der Nutzeraccount, sofern er nicht rechtzeitig durch Erneuerung der Registrierung aufgefrischt wird.
	Eine Erneuerung der Registrierung ist nur mit Zustimmung des AG möglich O_PARTICIPATION_TICKETS	R_AG4	Für die Erneuerung einer Registrierung ist ein fälschungssicherer, von MV erstellter Freischaltcode erforderlich, den die AN ausschließlich über den AG beziehen können nach einen anonymen, zufälligen Zuteilungsverfahren. *(vgl. R_AN3)*
Reputationsverlust durch ungünstige Gruppenreports T_GROUP_DATA_DISCLOSURE	Der AG entscheidet, wie breit er den Bericht (innerhalb des Unternehmens) streut. OE_LIMITED_DISCLOSURE	R_AG5	Gruppenberichte werden von MV ausschließlich an den AG zugestellt: AG entscheidet, an wen er diese Gruppenberichte weitergibt.
	Das Streuen der Gruppenberichte außerhalb des Unternehmens bedarf der Unterrichtung und Einverständniserklärung der betroffenen AN OE_LIMITED_DISCLOSURE	R_AG6	Die Regelung zur Weitergabe ist in der Datenschutzerklärung des Dienstes genau beschrieben. Nutzer des Dienstes müssen zuvor ihr Einverständnis mit den Regelungen erklären.
Reputationsverlust durch Datenleck T_PRT_DATA_DISCLOSURE T_GROUP_DATA_DISCLOSURE	Der AG kennt weder die Pseudonyme noch die individuellen Daten oder vom AN genutzten Registrierungstokens und Gruppen-IDs der AN-Nutzerkennungen, sondern nur die Einteilung seiner AN in Analysegruppen. Er kennt auch nicht die Verbindungsdaten der Kommunikation zwischen AN und AS, was den potenziellen Schaden begrenzt, sollten die Gruppenberichte unautorisierten Dritte bekannt werden. O_ANONYMOUS_REGISTRATION O_ANONYMOUS_INTERACTION O_SPLIT_PID_KNOWLEDGE O_GROUP_AUTHENTICATION O_ENCRYPTED_COMMUNICATION	R_AG7	Keine direkte Geschäftsbeziehung zwischen AS und AG *Gefahrenreduktion durch Datensparsamkeit, Rollentrennung und Anonymisierung: siehe R_AN18, R_AN24, R_AN25*
Der Dienstleister rechnet Dienstnutzung über das vereinbarte Kontingent hinaus ab T_TICKET_FRAUD	AG und MV vereinbaren ein festes Kontingent. Ist das Kontingent ausgeschöpft, werden weitere Anmeldungen entweder abgewiesen oder des wird in Absprache mit dem AG das Analysekontingent entsprechend erweitert. O_PARTICIPATION_TICKETS	R_AG8	Je nach Bezahlmodell besteht keine Notwendigkeit einer zahlenmäßigen Beschränkung.
		R_AG9	Mittels Registrierungs- und Gruppentoken (RT, GID) kann der AG die Kontrolle über die Maximalzahl der Kennungen und Gruppen

			behalten: *siehe Anforderungen R_AG1, R_AG2, R_AG10*
		R_AG10	AG und MV können bei Bedarf eine Least-recently-used-Strategie vereinbaren: Die am längsten nicht mehr genutzte Kennung fliegt aus dem Analysekontingent, um Platz für neue Teilnehmer zu machen. Dann kann es keine Kontingentüberschreitungen geben.
	Es können nur solche Nutzer ihre Registrierung erneuern, die vom AG eine entsprechende Autorisierung erhalten haben. O_PARTICIPATION_TICKETS	R_AG11	*siehe Anforderung R_AG3*
Rechtliche Anforderungen werden nicht erfüllt T-PRT_DATA_DISCLOSURE T_EXCESSIVE_MONITORING T_PRESSURING_EMPLOYEES T_INTRANSPARENCY	Rechtliche Pflichten der Verantwortlichen werden erfüllt O_WRITTEN_ELECTRONIC_CONSENT O_DATA_PROCESSING_INFORMATION O_ADJUSTMENT_OF_CONSENT_TO_DATA_SENSITIVITY O_LIMITATION_OF_DATA_SENT O_TRANSPARENCY_AND_SELF-DETERMINATION O_SUPPORT_IN_ASSERTION_OF_DATA_SUBJECT_RIGHTS	R_AG13	Eine Datenschutz-Folgenabschätzung nach Art 35 DSGVO wird durchgeführt und liegt schriftlich dokumentiert vor. Die darin geplanten Abhilfemaßnahmen (sind effektiv umgesetzt und) reduzieren die Risiken hinreichend.
		R_AG14	ArbeitnehmerInnen können jederzeit die Löschung der sie betreffenden Daten verlangen (das umfasst NICHT die bereits erzeugten Gruppenberichte)
		R_AG15	Betroffene werden bei der Ausübung der Betroffenenrechte unterstützt.
		R_AG16a	Das System ermöglich eine anonyme Nutzerregistrierung ohne Angabe des Namens oder der E-Mail-Adresse *siehe R_AN1, R_AN2, R_AN3, R_AN6, R_AN7*
		R_AG16b	Der Verbindungsaufbau zwischen App und AS ist so gestaltet, dass er keinen Personenidentifizierung ermöglicht
		R_AG16c	Alle Einwilligungen des AN sind mit dem ihm zugewiesenen Pseudonym PSEU verknüpft, so dass ein AN seine Einwilligungen jederzeit widerrufen kann, ohne seine Identität preiszugeben.
		R_AG16d	AS oder AG dürfen keine Datenverarbeitungen vornehmen, mit denen ein AN vernünftigerweise nicht rechnen würde (siehe DiGA/DiPA-Prüfkriterien [3], Abschnitt 3.3, TuG1.1)
		R_AG16e	Etwaige, zum sicheren Betrieb des Dienstes geschriebene Protokolle mit Personenbezug müssen spätestens nach drei Monaten wirksam gelöscht werden. ([3] DMM2.3)
		R_AG16f	Nutzt ein AN den Dienst nicht mehr, so können seine Daten und sein Account noch eine definierte Zeit bei AS gespeichert bleiben, um eine Wiederaufnahme der Analysen zu ermöglichen. Erfolgt innerhalb dieser Grace-Periode keine erneute Freischaltung der Anwendung, so muss die AN-Kennung und alle daran gebundene Daten gemäß Löschkonzept gelöscht werden ([3] DMN4.2b)
		R_AG17	Die gemeinsam Verantwortlichen müssen einen Joint-Controller-Vertrag abschließen.
	Die Grundsätze der Verarbeitung personenbezogener Daten werden eingehalten	R_AG18	Einhalten der Rechenschafts- und Nachweispflicht für die Einhaltung der Pflichten der DSGVO (Rechenschaftspflicht)
		R_AG19	Daten werden nur für jene Zwecke verarbeitet, für die sie erhoben wurden (Zweckbindung)
		R_AG20	Die erhobenen Daten müssen dem Zweck angemessen sein und auf das für die Zwecke der Verarbeitung angemessene Maß beschränkt sein (Datenminimierung)
		R_AG21a	ArbeitnehmerInnen entscheiden selbst, wie lange der Dienstleister ihre Daten/Kennwerte vorhält (z. B. wie lange historische Belastungsverläufe,

			Benachrichtigungen, ... im System gespeichert bleiben sollen, bevor sie automatisch gelöscht werden)
		R_AG21	Die Daten müssen nach dem Entfallen des Zwecks der Erhebung gelöscht oder ihr Personenbezug entfernt werden (Speicherbegrenzung)
	Rahmenbedingungen zur Erhebung einer Einwilligung werden eingehalten O_WRITTEN_ELECTRONIC_CONSENT O_DATA_PROCESSING_INFORMATION O_ADJUSTMENT_OF_CONSENT_TO_DATA_SENSITIVITY	R_AG22	Die Einwilligung muss in schriftlicher oder elektronischer Form eingeholt werden.
		R_AG23	Es muss eine angemessene Aufklärung der Arbeitnehmer durchgeführt werden.
		R_AG24	Die Einwilligung muss auf die besondere Sensibilität der Daten eingehen.
		R_AG25	Negative Konsequenzen bei Verweigerung der Einwilligung müssen verhindert werden. *siehe Anforderungen, um die Freiwilligkeit zu unterstützen: R_AN26, R_AN26a, R_AN49*
	Anforderungen bei Datenübermittlungen in Drittländer OE_AUTHORISATION_Art._45_ff._GDPR O_INFORMATION_ON_THIRD_COUNTRY_TRANSFER	R_AG26	Die Datenschutzerklärungen muss Informationen darüber enthalten, dass ein Datentransfer in Drittländer stattfindet.
		R_AG27	Es muss ein Erlaubnistatbestand nach Art. 45 ff. DSGVO für die Verarbeitung vorliegen.

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
Reputationsverlust durch Datenleck T_GROUP_DATA_DISCLOSURE	MV kennt weder individuelle Daten noch die wahren Identitäten der AN, noch deren Pseudonyme. Er kennt auch nicht die Bedeutung der Gruppenkennungen in der AG-Organisation. Er erhält von AS nur aggregierte, anonymisierte Gruppenreports zur Weiterleitung an den AG, die er möglichst ungelesen weitergibt O_SPLIT_PID_KNOWLEDGE O_NEED_TO_KNOW	R_MV3	Organisatorische Trennung der Rollen MV und AS *Die Prinzipien der Datensparsamkeit, Rollenteilung und Anonymisierung, Need-to-Know-Prinzip begrenzen die Risiken durch Datenlecks:* *siehe R_AN5, R_AN8, R_AN18, R_AN20, R_AN23, R_AN24, R_AN25*
	MV kennt keine Verbindungsdaten bezüglich der Kommunikation zwischen AS und einzelnen AN O_SPLIT_PID_KNOWLEDGE O_ENCRYPTED_COMMUNICATION	R_MV4	Keine direkte Kommunikation oder Geschäftsbeziehung zwischen AN und MV Die Prinzipien der Rollenteilung und Anonymisierung begrenzen die Risiken durch Datenlecks *siehe R_AN5*
Dienstleister wird dafür verantwortlich gemacht, dass die Betroffenen nur einen eingeschränkten Nutzen haben oder die Ergebnisse für den AG nicht hilfreich sind, wenn die Betroffenen sich für eine Priorisierung des	Dem Dienstleister entstehen keine wirtschaftlichen Nachteile aus der datenschutzfreundlichen Gestaltung seines Angebots	R_MV5	Die finanzielle Kompensation des Dienstleisters wird nicht verringert, wenn sich Betroffene nur für einen Bruchteil der angebotenen Leistungen / Analysen entscheiden oder schlechtere Ergebnisse aufgrund einer Verrauschung erhalten.

Datenschutzes entscheiden T_SABOTAGE			
Rechtliche Anforderungen werden nicht erfüllt T_PRT_DATA_DISCLOSURE T_EXCESSIVE_MONITORING T_PRESSURING_EMPLOYEES T_INTRANSPARENCY	Rechtliche Pflichten der Verantwortlichen werden erfüllt	R_MV7	*siehe Anforderung R_AG13*
		R_MV8	*siehe Anforderung R_AG14*
		R_MV9	*siehe Anforderung R_AG15*
		R_MV10	*siehe Anforderung R_AG16<x>*
		R_MV11	*siehe Anforderung R_AG17*
	Die Grundsätze der Verarbeitung personenbezogener Daten werden eingehalten	R_MV12	*siehe Anforderung R_AG18*
		R_MV13	*siehe Anforderung R_AG19*
		R_MV14	*siehe Anforderung R_AG20*
		R_MV15	*siehe Anforderung R_AG21*
	Rahmenbedingungen zur Erhebung einer Einwilligung werden eingehalten	R_MV16	*siehe Anforderung R_AG22*
		R_MV17	*siehe Anforderung R_AG23*
		R_MV18	*siehe Anforderung R_AG24*
		R_MV19	*siehe Anforderung R_AG25*
	Anforderungen bei Datenübermittlungen in Drittländer	R_MV20	*siehe Anforderung R_AG26*
		R_MV21	*siehe Anforderung R_AG27*

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 Intellectual Property 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.
Karteileichen: Ungenutzte Kennungen blockieren Ressourcen T_SABOTAGE	Entfernen aller Pseudonymkennungen und ihrer Daten (vorbehaltlich gesetzlicher Aufbewahrungsfristen), für die innerhalb festgesetzter Frist keine Erneuerung der Registrierung erfolgt ist O_PARTICIPATION_TICKETS	R_AS3	AS prüft die Befristung aller Freischaltcodes und legt solche Kennungen still, die ihre Freischaltung nicht rechtzeitig durch einen gültigen neuen Freischaltcode erneuern. Erneuerung der Registrierung erfordert ein gültiges, von MV in Umlauf gebrachtes, fälschungssicheres Registrierungstoken. *siehe Anforderung R_AG3 und R_AG4*
Reputationsverlust durch Datenleck T_PRT_DATA_DISCLOSURE T_GROUP_DATA_DISCLOSURE	AS kennt weder die Identitäten der registrierten Nutzer noch die Bedeutung der Analysegruppen und auch nicht den Arbeitgeber, kann daher die Kennungsinformationen ohne AG keinen Personen zuordnen O_SPLIT_PID_KNOWLEDGE O_NEED_TO_KNOW	R_AS4	MV und AS sind organisatorisch zu trennen und es gibt keine Geschäftsbeziehung zwischen AS und AG die Anonymisierung sowie die Rollentrennung und Begrenzung der Geschäftsbeziehungen zwischen MV, AS, AG und AN begrenzt das potenzielle Risiko eines Datenlecks *siehe auch R_AN18, R_AN20, R_AN24, R_AN25, R_MV3*
	AS verwaltet alle Vital- und Analysedaten (ungeachtet einer Pseudonymisierung, Aggregation oder Ähnlichem) nach einem strikten Need-to-know-Prinzip. AS-Mitarbeiter haben nur eng beschränkte Zugriffsrechte auf diese Daten -- soweit überhaupt erforderlich O_NEED_TO_KNOW	R_AS5	Die Verarbeitungskette soll weitestgehend vollautomatisiert sein, ohne dass AS-Mitarbeiter im Normalfall überhaupt mit solchen Daten hantieren müssen.
AS übergibt AG Gesundheitsdaten der Beschäftigen T_PRT_DATA_DISCLOSURE	AS muss vor etwaigen Herausgabeansprüchen des AG geschützt werden, um die Gesundheitsdaten der Beschäftigten vertraulich behandeln zu können OE_LEGALLY_INDEPENDENT_ROLES	R_AS6	Der Analysedienstleister ist insofern unabhängig vom Arbeitgeber / nicht an dessen Weisungen gebunden, dass der AG nicht die Herausgabe/Offenlegung der Gesundheitsdaten der Beschäftigten verlangen darf. Die Beschäftigen verlassen sich darauf, dass der Analysedienstleister ihre Daten vertraulich behandelt und lediglich anonymisierte, aggregierte

			Informationen (Gruppenberichte) an den AG übermittelt, aus denen die Daten einzelner nicht ersichtlich sind (Schutz vor negativen Folgen). Könnte der AG dem AS Weisung erteilen, ihm die Daten einzelner offenzulegen, wäre das problematisch.
Rechtliche Anforderungen an die Datenerhebung werden nicht erfüllt T_PRT_DATA_DISCLOSURE T_GROUP_DATA_DISCLOSURE T_EXCESSIVE_MONITORING T_INTRANSPARENCY	Rechtliche Anforderungen an die Datenerhebung werden erfüllt: O_WRITTEN_ELECTRONIC_CONSENT O_DATA_PROCESSING_INFORMATION O_ADJUSTMENT_OF_CONSENT_TO_DATA_SENSITIVITY O_LIMITATION_OF_DATA_SENT O_TRANSPARENCY_AND_SELF-DETERMINATION O_SUPPORT_IN_ASSERTION_OF_DATA_SUBJECT_RIGHTS O_ANONYMOUS_RESEARCH_DATA	R_AS7	AS informiert den Anwender schriftlich über die erhobenen Daten, die Art ihrer Weiterverarbeitung und ihrer Weitergabe an Dritte. Eine genaue Beschreibung ist jederzeit mittels App abrufbar.
		R_AS7a	AS weist insbesondere auf die Behandlung der besonders sensiblen persönlichen Gesundheitsdaten hin. Eine entsprechende Beschreibung ist jederzeit abrufbar.
		R_AS7b	Die Übertragung von Rohdaten beschränkt sich strikt auf Informationen, die sich auf den Arbeitsschutz und den Arbeitnehmer-Gesundheitsschutz beziehen. Für jedes übertragene Datenattribut liegt eine Begründung vor, warum dieses Attribut für den beschriebenen Zweck unabdingbar ist.
		R_AS7c	AS ermöglicht Analysen auf unterschiedlichen Privacy-Levels. Die Analysetiefe und -genauigkeit wächst mit steigender Privacy-Kritikalität; der Anwender kann selbst bestimmen, auf welchem Level er einer Analyse zustimmt.
		R_AS7d	AS richtet eine Kontaktstelle für Anwender ein, wo den Anwender in der Ausübung seiner Rechte als Datensubjekt unterstützt und ihm alle seine laut DSGVO zustehenden Einflussmöglichkeiten bietet.
		R_AS8	Eine Totalüberwachung wird vermieden.
		R_AS9	Es werden nur Daten mit Bezug zu Arbeitssicherheit und Arbeitnehmer-Gesundheitsschutz erhoben.

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.
Bezug der Counterfeit-Smartphone-App aus nicht vertrauenswürdigen Quellen T_ENTITY_SPOOFING T_TROJAN_HORSE	Die zur Vitaldatenerfassung genutzte App soll authentisch sein und frei von Manipulationen, die den Datenschutz oder die korrekte Funktionalität der Anwendung gefährden könnten. OE_TRUSTWORTHY_SOFTWARE	R_E5	Die Smartphone-App wird ausschließlich über den wohlbekannten App Store vertrieben.

Wie ein Prozessablauf gemäß den hier beschriebenen Anforderungen aussehen könnte, zeigt Abbildung 6. In diesem Realisierungsvorschlag gehen wir davon aus, dass der Arbeitgeber mit

Marketing & Vertrieb ein Analysekontingent (AK) aushandelt über eine bestimmte Laufzeit und eine bestimmte Teilnehmer- und Gruppenzahl.

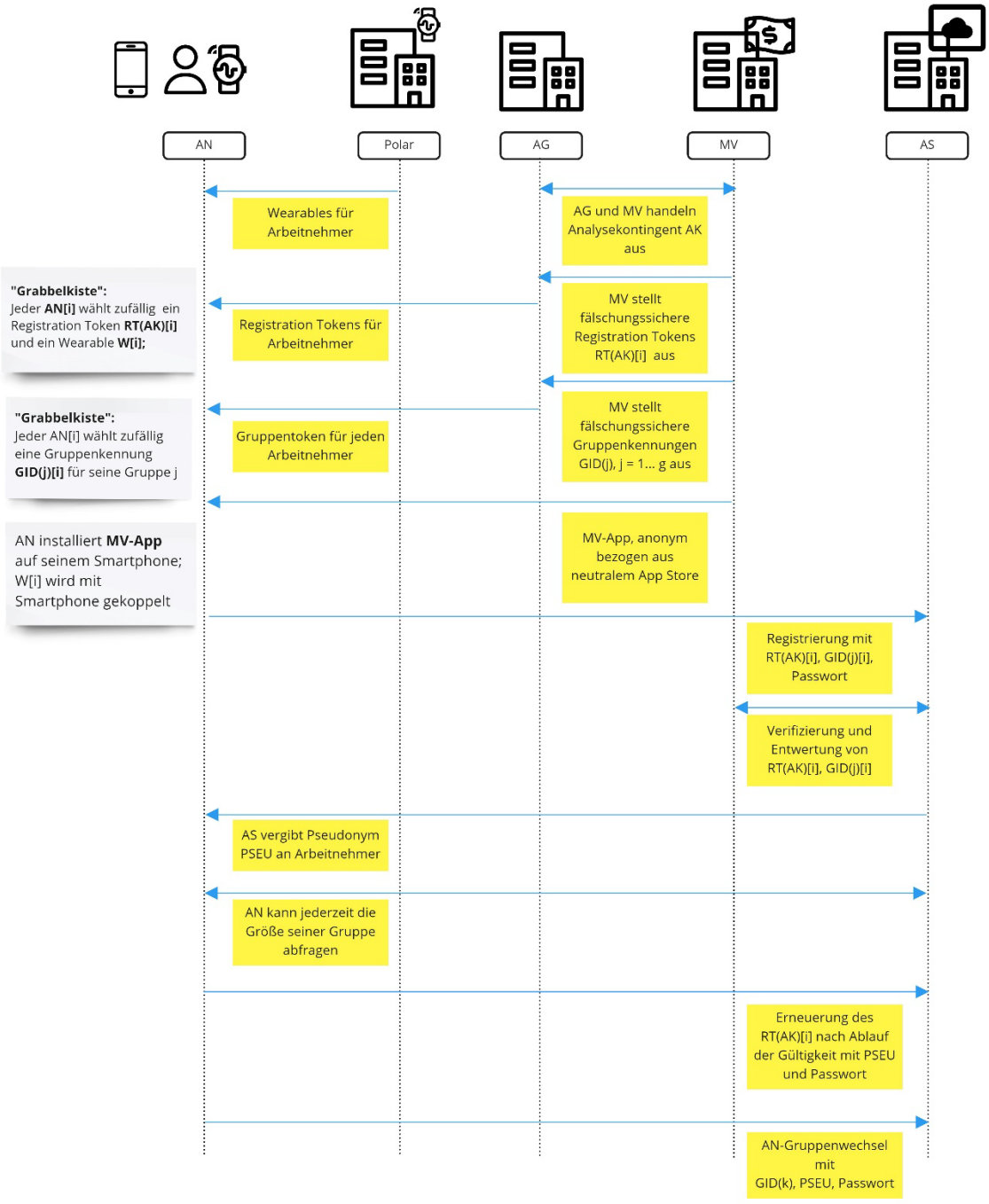

Abbildung 6 Übersicht über den Anmeldevorgang gemäß dem in Abschnitt 8.3 vorgeschlagenen Lösungskonzept. Der Ablauf ist mit den in Abschnitt 8.4 genannten Anforderungen verträglich.

MV erstellt dann eine ausreichende Menge von Registrierungs- und Gruppentokens für den Arbeitgeber, die sich auf dieses Analysekontingent beziehen. Der Arbeitgeber verteilt diese Tokens nach einem zufälligen Verfahren an die Teilnehmer, so dass die Zuordnung von Token zu Teilnehmer unbeobachtet bleibt.

Die Teilnehmer nutzen dann ihre Registrierungs- und Gruppentoken, um sich beim Dienst und in einer bestimmten Analysegruppe als gültige Nutzer anzumelden. Bei erfolgreicher Registrierung erhält der Teilnehmer ein eindeutiges, zufälliges Pseudonym PSEU vom Analyse-Service. Mit PSEU und dem bei

der Registrierung festgelegten Passwort kann sich der Teilnehmer dann später immer wieder als ein spezifisches registriertes Individuum zu erkennen geben, ohne dafür seine Identität preiszugeben.

Um anonyme »Karteileichen« erkennen und eliminieren zu können, muss die Registrierung in angemessenen Zeitintervallen erneuert werden. Arbeitnehmer erhalten dazu von ihrem Arbeitgeber rechtzeitig ein frisches Registrierungstoken. Trotz Neuregistrierung können die Teilnehmer anhand ihres Pseudonyms PSEU immer wieder der gleichen Nutzerkennung zugeordnet werden.

8.6 Ausblick

In den vorangegangen Abschnitten des Kapitels 8 haben wir vornehmlich die Anforderungen an ein datenschutzfreundliches, wirtschaftlich faires Prozessmodell betrachtet. Wie wir in Abschnitt 8.1 erläutert haben, ist dies aber nur eine Seite der Medaille: Auch der beste Prozessdatenschutz läuft ins Leere, sofern die verarbeiteten Daten selbst ihrer Natur nach leicht personenbeziehbar sind. Wenn es einem Angreifer also gelingt, die Messergebnisse aufgrund von Kontextwissen außerhalb der technischen Prozesskette doch wieder konkreten Personen zuzuordnen, dann verfehlen die Schutzmechanismen des Prozessmodells die beabsichtigte Wirkung.

Solche Kontextinformation könnten zum Beispiel gewonnen werden, wenn Teilnehmer des Messprogramms privat auch noch weitere Gesundheits-Apps nutzen und ihre Vitaldaten-Messwerte in Internetforen teilen, zum Beispiel in Trainingsgruppen ihres Sportvereins. Ein Angreifer, der Zugriff auf solche Trainingsdaten erhält und den Bezug zu dem entsprechenden Teilnehmer im Internetforum herstellen kann, könnte mit diesem Wissen auf die Identität der WearPrivate-Nutzer zurückschließen, indem er die Daten der WearPrivate-Belastungsmessung mit den Daten des Internetforums korreliert.

Die Frage, wie man das Datenmodell möglichst datenschutzfreundlich gestalten kann, ohne dabei die erhobenen Vitaldaten zu sehr zu verfremden und medizinisch zu entwerten, muss für das ins Auge gefasste Szenario »Belastungsmessung« noch eingehender untersucht werden. Insbesondere ist zu klären, in welchem Maß die Analysegenauigkeit abnimmt, wenn man die Rohdaten zunehmend vergröbert, etwa durch großzügiges Runden oder durch Aggregation. Genaueren Aufschluss darüber können Sensitivitätsanalysen der bestehenden Analysesoftware des Projektpartners WearHealth geben. Anhand von Beispieldaten lässt sich beobachten, wie sich der errechnete Befund ändert, wenn man die Rohdaten schrittweise verfremdet. Hierzu sind im Projekt weitere Untersuchungen geplant.

Quellennachweise

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

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

[3] BfArM: Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz (Version 1.0). Bundesinstitut für Arzneimittel und Medizinprodukte, April 2024 https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.html (zuletzt besucht am 19.07.2024)

Anhang A Bedrohungsmatrix für den Anwendungsfall »Belastungsmessung«

Abschnitt 8.4 beschreibt ein Verfahren für eine systematische Bedrohungs- und Risikoanalyse (TARA). Ausgangspunkt des Verfahrens ist eine Bedrohungsmatrix, in der alle identifizierten Bedrohungspotenziale der Form (Threat Agent, Asset, Adverse Action) eingetragen werden.

Dazu werden die Threat Agents als Spalten und die Assets als Zeile der Bedrohungsmatrix dargestellt, und im Schnittpunkt von Zeile und Spalte stehen die Bedrohungen, die der Agent in der betreffenden Spalte auf das Asset der betreffenden Zeile ausübt. Abbildung 7 zeigt das grundlegende Gliederungsschema der Bedrohungsmatrix.

		Threat Agents			
		Agent1	Agent2	Agent3	...
Information Assets	I_Asset1	adverse action(s)	adverse action(s)	adverse action(s)	...
	I_Asset2	...	...	...	...
	I_Asset3	...	...	...	...
	...	...	...	...	...
Function Assets	F_Asset1	adverse action(s)	adverse action(s)	adverse action(s)	...
	F_Asset2	...	...	...	...
	F_Asset3	...	...	...	...
	...	...	...	...	...
Physical Assets	P_Asset1	adverse action(s)	adverse action(s)	adverse action(s)	...
	P_Asset2	...	...	...	...
	P_Asset3	...	...	...	...
	...	...	...	...	...

Abbildung 7 Aufbau einer Bedrohungsmatrix für eine Übersicht über die Bedrohungstupel der Form (Agent, Asset, Adverse Action)

Im Rahmen des Vorhabens WearPrivate haben die Projektpartner für den Hauptdemonstrator des Projekts den Anwendungsfall »Kontrolle der physischen und mentalen Belastung am Arbeitsplatz« ausgewählt. Für diesen Anwendungsfall wurde eine Bedrohungsmatrix gemäß dem Schema aus Abbildung 4 erstellt. Die Matrix ist als Excel-Datei in Ergänzung zum vorliegenden Ergebnisbericht verfügbar.

Aus den erhobenen Bedrohungen wurden die in Tabelle 1 gelisteten grundlegenden Bedrohungsszenarien abgeleitet.

Tabelle 1 Abgeleitete Bedrohungsszenarien für den Anwendungsfall zu »Kontrolle der physischen und mentalen Belastung am Arbeitsplatz«

Bedrohungsszenario	Beschreibung
PRT_RE-IDENT	Re-identify participants and re-attribute their PRT data to them by exploiting characteristic properties of the hardware devices (i.e., wearables, smartphones), the registration credentials (i.e., tickets) being used, the profile data provided by the PRT, the vital data being recorded, the communication parameters of the communication session with AS, or the monitoring context (e.g., the time a PRT registers, logs in, or shows strong symptoms of physical stress).
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 involuntarily 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
SABOTAGE	Subvert the monitoring program (e.g., to enforce data privacy at the workplace or to harm EMP)
ENTITY_SPOOFING	Falsely claim to be certain entity within the monitoring program (e.g., spoof the role of a communication endpoint or a hardware device)
IP_DISCLOSURE	Disclose intellectual property of AD or of AS
TROJAN_HORSE	Implant malicious code into Smartphone app or service software
CLOUD_INFILTRATION	Infiltrate cloud services or AP-Cloud communication to subvert the stress monitoring
INTRANSPARENCY	Conceal essential security- or privacy information from PRT (e.g., notification about security incidents, forwarding of personal data to other parties, or the analysis of certain health parameters)
JAIL_BREAK	Run Smartphone App on a jail-broken device, thus undermining the built-in security and privacy mechanisms of the stress monitoring service

Anhang B TPAxO-Matrix für den Anwendungsfall »Belastungsmessung«

Die Bedrohungs- und Risikoanalyse (TARA) gemäß Abschnitt 8.4.1 dient als Ausgangspunkt, um für das untersuchte System die erforderlichen Sicherheits- und Datenschutzziele festzulegen, die notwendig sind, um allen identifizierten Bedrohungen zu begegnen. Wie im Abschnitt 8.4.3 beschrieben, werden dazu allen Threats, Policies und Assumptions, die für das System ermittelt wurden, die entsprechenden Objectives in einer TPAxO-Matrix gegenübergestellt: {Threat | Policy | Assumption} × Objective.

Abbildung 8 zeigt eine entsprechende Matrix für den im Projekt gewählten Anwendungsfall des Hauptdemonstrators.

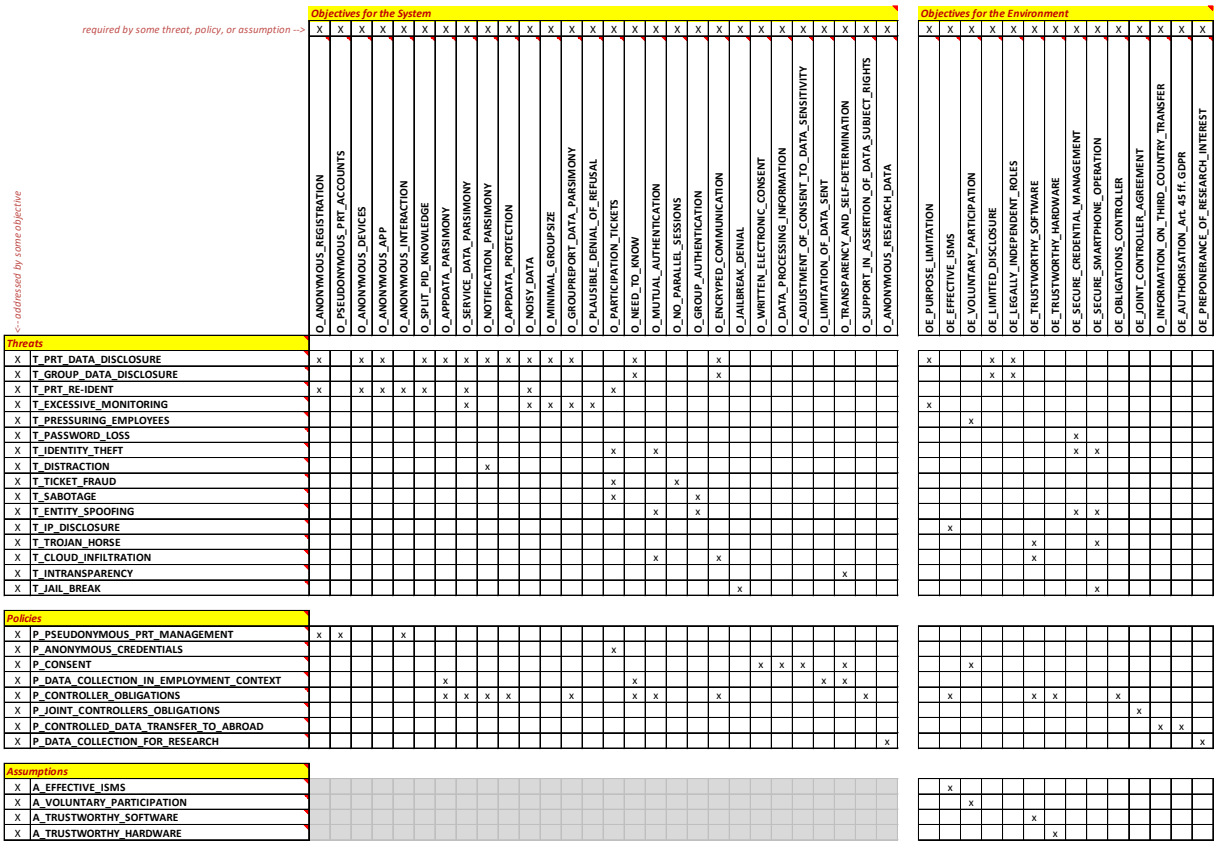

Abbildung 8 Beispielhafte TPAxO-Matrix für den Anwendungsfall »Kontrolle der physischen und mentalen Belastung am Arbeitsplatz«

Neben den in Anhang A beschriebenen Bedrohungen wurden die in Tabelle 2 genannten Security Policies identifiziert.

Tabelle 2 Relevante Security Policies für den Anwendungsfall »Kontrolle der physischen und mentalen Belastung am Arbeitsplatz«

Security Policy	Beschreibung
P_PSEUDONYMOUS_PRT_MANAGEMENT	The Analysis Service must bind all data regarding an individual participant (e.g., participant profile, vital data, analysis results, or privacy preferences) to a corresponding pseudonymous user account in accordance with DiGA/DiPA

Security Policy	Beschreibung
	Critreria [3], Clause DMN_4.1. These accounts must not contain any references to the identity of the participant, such as name, address, telephone number, or employee number, and a data transfer from one such user account to another must not occur.
P_ANONYMOUS_CREDENTIALS	To ensure the legitimacy of a participant registration and to prove that the expenses of the Analysis Service and the Marketing Service are covered while concealing the identity of the participant, anonymous participation tickets shall be used that contain no reference to person-identifiable data of the participant in accordance with DiGA/DiPA Criteria [3], Clause DMN_1.1b (see specific explanations in Section 6.5 of the Guideline). Once registered using such a ticket, participant receive an ID as their pseudonym and a password; after that, all authentication and authorization are bound to the knowledge of ID and password, and all participant-related data is kept under the account assigned to this ID.
P_CONSENT	The processing of personal data requires a legal basis under the GDPR. Exemplary consent (§ 26 Abs. 3 S. 2 BDSG) can be used.
P_DATA_COLLECTION_IN_EMPLOYMENT_CONTEXT	Certain requirements must be met when collecting data for the purpose of the employment relationship. These include that data may only be collected in relation to occupational health and safety, total surveillance must be avoided, and measures must be taken to strengthen and safeguard transparency and self-determination.
P_CONTROLLER_OBLIGATIONS	The controller has a duty of accountability and proof of compliance with the obligations of the GDPR, must support data subjects in asserting their rights, and must ensure the security of data processing.
P_JOINT_CONTROLLERS_OBLIGATIONS	Joint controllers must conclude a joint controller agreement.
P_CONTROLLED_DATA_TRANSFER_TO_ABROAD	For data transfers to third countries, information on third country transfers is required in the data protection declaration and a permission must be granted in accordance with Art. 45 et seq. GDPR.
P_DATA_COLLECTION_FOR_RESEARCH	If data is collected for research purposes, it must be anonymized, and the interests of the project partners must significantly outweigh the interests of the participants.

Im Zuge der TPAxO-Modellierung wurden unter anderem die in Tabelle 3 gelisteten Ziele für das System definiert.

Tabelle 3 Beispielhafte abgeleitete Systemziele gemäß TPAxO-Modellierung

System Objective	Beschreibung
O_ANONYMOUS_REGISTRATION	To use the stress monitoring Smartphone App, participants can register anonymously without disclosing their identity (e.g., name, social security number, or passport number) or

System Objective	Beschreibung
	any address information (e.g., postal address or email address)
O_PSEUDONYMOUS_PRT_ACCOUNTS	For each registered participant, the Analysis Service shall create an individual account, and all data related to the participant (e.g., PRT profile, collected wearable data, analysis results for this participant, privacy preferences) shall be kept exclusively under this account.
O_ANONYMOUS_DEVICES	The hardware ID of the participants' personal devices (i.e., wearables and smartphone) are not disclosed to their employer, and no device I is ever assigned to or transmitted with the data sent from the Smartphone to the Analysis Service
O_ANONYMOUS_APP	All participants use the same Smartphone App without any participant-specific labelling or functionality, so that the app provides no indication of the participant using it.
O_ANONYMOUS_INTERACTION	Participants can use the stress-monitoring service anonymously. In particular, they do not have to disclose their identity to unregister or to exercise their legitimate rights as a data subject according to the GDPR.
O_SPLIT_PID_KNOWLEDGE	Knowledge about the stress monitoring participants and their data is split among the different roles of the involved parties so that no single role has sufficient local data to re-identify a participant or to assign the measured raw datal data to a specific natural person (thus turning it into person-identifiable data, PID).
O_APPDATA_PARSIMONY	As few as possible vital data, profile data, and analysis data should be collected stored by the analysis service, and the retention time of that data should be minimized.
O_SERVICE_DATA_PARSIMONY	As few as possible vital data, profile data, and analysis data should be collected stored by the analysis service, and the retention time of that data should be minimized.
O_NOTIFICATION_PARSIMONY	Notifications sent from the Analysis Service to the Smartphone App shall not contain sensitive personal information (unless absolutely necessary for reasons of employee safety and well-being). Moreover, only essential and urgent notifications shall be sent to the participant to avoid distraction at work. The participant shall be enabled to disable or to temporarily pause each type of notification on request, according to personal preferences and current needs
O_APPDATA_PROTECTION	Sensitive data stored by the Smartphone APP shall be stored in encrypted format, and it shall not be included in backups in unencrypted form. Moreover, the app shall apply adequate access protection to the data to shield it from other apps and to prevent access without proper authentication.
O_NOISY_DATA	Profile data requested from the participant should be requested with the minimum accuracy that is required to obtain the desired quality of the analysis results. Noise should be deliberately added to the measured raw data to the

System Objective	Beschreibung
	degree possible so as to retain the desired quality of the analysis results.
O_MINIMAL_GROUPSIZE	The Employer does never gain access to the data or analysis results of individual participants, but only to aggregated analysis results for groups of participants. To hide the analysis results of individual group members, group reports are only generated if the respective group comprises sufficient group members. (The threshold value is application dependent.)
O_GROUPREPORT_DATA_PARSIMONY	Group reports disclose as little as possible about group membership or the positioning of individual group members compared to one other. For example, the exact number of members is hidden from the reader, and the aggregated data avoids to isolate the individuals with the "best" or "worst" analysis results by rather focusing on mean and distribution characteristics (e.g., standard deviation or quartiles) of the member results.
O_PLAUSIBLE_DENIAL_OF_REFUSAL	The user interface and the user interaction concept enable participants to plausibly pretend that they participate in the monitoring program when in fact they do not. In the presence of an independent observer, they can convincingly simulate participation to plausibly deny their refusal to join stress monitoring.
O_PARTICIPATION_TICKETS	To participate in the stress-monitoring program, participants must have a participation ticket. These tickets are provided by the Marketing Service, and their authenticity is guaranteed by a digital signature scheme. The tickets prove that the Employer has paid for the services provided by the Analysis Service and the Marketing Service. The Employer is responsible for handing out tickets to the authorized Participants. Once it has been used successfully for registration, the ticket becomes invalid immediately and cannot be re-used again. The registration lasts only for a limited period; after expiry, a new ticket is required to renew the registration. Tickets do not carry any open or hidden marks indicating the ticket holder, and they are assigned randomly among all participants.
O_NEED_TO_KNOW	Analysis Service and Marketing Service collect and process their required data according to strict need-to-know principle. That is, only data that is indispensable for service provisioning is collected and processed, and processing involves minimal human intervention by as few persons as possible.
O_MUTUAL_AUTHENTICATION	The interacting parties mutually authenticate each other (e.g., wearable/smartphone, participant/analysis service, analysis service/marketing service, marketing service/employer) at a security level commensurate with the risks inherent in entity spoofing
O_NO_PARALLEL_SESSIONS	At any moment, a participant's credential can only be used to start one unique session. Multiple parallel log-ins under the same participant ID are denied by the Analysis service.

System Objective	Beschreibung
O_GROUP_AUTHENTICATION	On registration, participants authenticate themselves as members of a certain analysis group with a level of security commensurate with the quality demands of their Employer. The Smartphone App provides means for the participants to verify and prove their group membership in the presence of the Employer without disclosing their participant credentials or ID within the stress-monitoring program. For example, if the Employer fully trusts the participants, they may be free to just pick their expected group membership; if the Employer wants to keep full control over group assignment, participation tickets may be equipped with a group-specific tagging so that participants can be automatically assigned to their respective group on registration with their ticket.
O_ENCRYPED_COMMUNICATION	Communication between Smartphone an Analysis, Service, between Analysis Service and Marketing Service, and between Marketing Service and Employer is encrypted so that a third party cannot disclose the data being transmitted. If the Wearable offers this option, the data exchange between wearable and Smartphone App shall also use encryption.
O_JAILBREAK_DENIAL	The Smartphone App inspects the Smartphone for signs of a jail-broken operating system. If a jailbreak is detected, the Smartphone App denies further access to or participation in the stress-monitoring program.
O_WRITTEN_ELECTRONIC_CONSENT	The system shall record the written consent of each participant and a clear indication to what kinds of data processing, exactly, the PRT agreed to. The electronic consent record must be retrievable on request.
O_DATA_PROCESSING_INFORMATION	The employee must be adequately informed. This is best done by making the privacy policy available in simple language and easily accessible.
O_ADJUSTMENT_OF_CONSENT_TO_DATA_SENSITIVITY	Provide a separate section in the privacy policy with reference to the fact that health data is processed and that this information is particularly sensitive data
O_LIMITATION_OF_DATA_SENT	Data sent from app to cloud is constrained by limits imposed on data collection in an employer-employee relationship. That is, only data related to occupational health and worker safety and meta data indispensable for its processing must be transmitted.
O_TRANSPARENCY_AND_SELF-DETERMINATION	The system shall clearly indicate to the participant: * Whether any data is collected / transmitted or not * What kind of processing and analysis is applied to the data * Who has access to which data * When events that are significant for privacy occur. In addition, each participant may select one of several available privacy levels. The levels provide different trade-offs between privacy and accuracy of the data analyses.

System Objective	Beschreibung
O_SUPPORT_IN_ASSERTION_OF_DATA_SUBJECT_RIGHTS	The system must inform the participants about means to contact the data controller in order to exert their rights as a data subject (e.g., information about data processing, objection to data processing, correction or deletion of data).
O_ANONYMOUS_RESEARCH_DATA	Participant profile data, raw data, or analysis results derived from such data must be provided for research only in anonymized format.

Neben den Sicherheits- und Datenschutzzielen für das System liefert die TPAxO-Modellierung auch entsprechende Ziele für die Systemumgebung, die entweder organisatorisch (also nicht-technisch) oder von anderen technischen Komponenten in der Umgebung des Systems zu erfüllen sind – nicht aber vom untersuchten System selbst. Tabelle 3 zeigt beispielhaft einige der Umgebungsziele für die Demonstratoranwendung des WearPrivate-Projekts.

Tabelle 4 Beispielhafte abgeleitete Ziele für die Systemumgebung gemäß TPAxO-Modellierung

Environment Objektive	Beschreibung
OE_PURPOSE_LIMITATION	Participants and their Employer agree by contract on the extent to which wearable data may be recorded and used for stress-level monitoring; this agreement puts limits on the types of analyses that may be carried out with the data being measured.
OE_EFFECTIVE_ISMS	The service providers (Analysis Service, Marketing Service) and the Employer have established an effective Information Security Management System (ISMS) to protect the data collected, processed, and reported within the stress-level monitoring program adequately against loss of confidentiality, integrity, or loss and to ensure personal and operational cybersecurity according to established standards.
OE_VOLUNTARY_PARTICIPATION	Participation in the stress-level monitoring program is voluntary. Employees have no obligation to participate, and they face no disadvantages if they refuse to join the program. Moreover, participants can pause or disable stress-level monitoring at any time, and they can permanently unregister at any time without requiring a justification.
OE_LIMITED_DISCLOSURE	Before joining the stress-monitoring program, the Participant formally agrees with the Employer on the recipients of raw data (and -- potentially -- the corresponding profile date), derived analysis results, aggregated group reports. The agreement is legally binding for both parties.
OE_LEGALLY_INDEPENDENT_ROLES	Employer, Analysis Service, and Marketing Service are mutually independent legal entities. No party can request information disclosure from another party beyond what is necessary for the agreed-upon service provisioning. For example, the Analysis service cannot force the Marketing Service to disclose the name of the Employer to which a given participation ticket has been sold, nor can the

Environment Objektive	Beschreibung
	Employer require the Analysis Service to disclose profile or measurement data for a given participant ID.
OE_TRUSTWORTHY_SOFTWARE	The software of the Smartphone App, the Analysis Service, and the Marketing Service have been designed and developed according to established quality and security standards, and its trustworthiness has been confirmed by a diligent approval process whose scrutiny is commensurate with the risks inherent to employing the software.
OE_TRUSTWORTHY_HARDWARE	The hardware infrastructure used for service provisioning, especially the wearables and the smartphone, is trustworthy and free of manipulations targeting at subverting or tapping the information processing and transmission.
OE_SECURE_CREDENTIAL_MANAGEMENT	Once registered under an anonymous participant ID and a personal password, participants securely manage their credentials so that they are not lost or stolen. The safeguards applied to credential management are commensurate with the risks inherent to losing control over these credentials. If they lose access to their credentials, they need to register under a new, independent ID with a fresh participation ticket.
OE_SECURE_SMARTPHONE_OPERATION	Participants make sure that their smartphone software is kept secure and receives the recommended security updates in a timely manner, that smartphone access is protected by a suitable authentication scheme (e.g., fingerprint, face ID, or password login), and that apps of dubious provenance or functionality are not installed on the device. The security measure being applied are commensurate with the risks inherent to unauthorized access to or privilege elevation.
OE_OBLIGATIONS_CONTROLLER	The controller must comply with the accountability and verification obligation for compliance with the obligations of the GDPR. This includes the documentation of all processing activities, documentation of consents granted and prior information provided to data subjects.
OE_JOINT_CONTROLLER_AGREEMENT	A joint controller agreement must be concluded. This includes defining the functions and responsibilities of joint controllers and specifying contact persons for asserting data subject rights.
O_INFORMATION_ON_THIRD_COUNTRY_TRANSFER	Information on third country transfers must be included in the privacy policy
OE_AUTHORIZATION_Art. 45 ff. GDPR	At best, adequacy decision pursuant to Art. 45 GDPR; shall be documented; otherwise: standard data protection clauses, adoption of suitable safeguards.
OE_PREPONERANCE_OF_RESEARCH_INTEREST	A significant preponderance of research interest must be substantiated by the service provider if participant data is transferred to third parties for research purposes. The justification must be documented, and participants must be

Environment Objektive	Beschreibung
	informed about these research transfers and their justification.