WearPrivate

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

Ergebnisbericht D4.2

Interaktionskonzept für informationelle Selbstbestimmung und transparente Datennutzung

Version	1.0
Datum	20.11.2024
Verfasser	Stefanie Ludborzs (IESE) Reinhard Schwarz (IESE)

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

BMI	Body-Mass-Index
GNSS	Global Navigation Satellite System
IT	Informationstechnik
WLAN	Wireless Local Area Network

1 Einführung

Der vorliegende Bericht beschreibt die entwickelten Interaktions- und Bedienkonzepte zur Förderung der informationellen Selbstbestimmung und einer transparenten Datennutzung in Wearable-basierten Anwendungsszenarien. Wearables, die als tragbare Geräte kontinuierlich personenbezogene Daten erfassen, bieten vielfältige Möglichkeiten zur Gesundheitsüberwachung, Fitnesssteigerung und Effizienzsteigerung in unterschiedlichen Lebens- und Arbeitsbereichen. Die damit verbundene umfangreiche Datensammlung stellt jedoch erhebliche Herausforderungen an den Schutz der Privatsphäre der Nutzer.

Datenschutz und Transparenz sind entscheidende Faktoren für die Akzeptanz von Wearable-Technologien, insbesondere im betrieblichen Kontext, wo der Einsatz solcher Geräte auf größere Vorbehalte stößt. Benutzerfreundliche Konzepte, die den Nutzern eine klare Kontrolle über ihre Datenflüsse ermöglichen, sind unerlässlich, um diese Bedenken auszuräumen und das Vertrauen in den bestimmungsgemäßen, datenschutzkonformen Einsatz der Technologie zu stärken.

Der vorliegende Ergebnisbericht D4.2 baut auf den Erkenntnissen des Ergebnisbericht D.4.1 [1] auf. Er zielt darauf ab, innovative Interaktionskonzepte vorzustellen, die den Nutzern größtmögliche Transparenz und Kontrolle über ihre persönlichen Daten bieten. Ziel ist es, den Nutzer in die Lage zu versetzen, individuell zu entscheiden, welche Daten er in welcher Form an wen weitergeben möchte. Dazu gehört auch die Möglichkeit, Daten nur aggregiert, anonymisiert oder unter bestimmten Bedingungen weiterzugeben.

Ein weiterer Schwerpunkt der Interaktionskonzepte liegt auf der Nachvollziehbarkeit der Datenflüsse und deren Auswertung. Da die Auswertung auf einer Vielzahl von Datenquellen und -typen beruht, die für den Nutzer oft nur schwer zu überblicken sind, haben wir Konzepte entwickelt, um die Transparenz und Nachvollziehbarkeit dieser Prozesse zu verbessern. Die Nutzer sollen in die Lage versetzt werden, informierte Entscheidungen unter Wahrung ihrer Privatsphäre zu treffen.

Die in diesem Bericht vorgestellten Lösungen sollen eine Brücke zwischen der Notwendigkeit einer umfassenden Datennutzung und dem berechtigten Bedürfnis der Nutzer nach Datenschutz und Privatsphäre schlagen. Ziel ist es, ein nutzerfreundliches und transparentes System zu schaffen, das die Akzeptanz von Wearable-Technologien fördert und gleichzeitig den Schutz der individuellen Privatsphäre sicherstellt.

2 Übersicht über den zugrundeliegenden Anwendungsfall

Als Ausgangspunkt für unser Überlegungen dient ein Wearable-basiertes System zur Überwachung der physischen und psychischen Belastung am Arbeitsplatz. Dieser beispielhafte Anwendungsfall weist viele der maßgeblichen Herausforderungen auf, die der Einsatz von Wearables am Arbeitsplatz mit sich bringt. Die daraus abgeleiteten Interaktionskonzepte sind daher auch auf ein breites Spektrum anderer Anwendungsfälle übertragbar.

Unser Anwendungsfall sieht vor, dass der Arbeitgeber seine Mitarbeitenden auf freiwilliger Basis mit Wearables ausstattet, die während der Arbeit eine Reihe von Vital- und Umgebungsparametern erfassen (z. B. Puls, Herzratenvariabilität, Blutsauerstoff-Sättigung, Beschleunigung entlang der Raumachsen, Standort, Umgebungstemperatur, Luftfeuchte oder dergleichen). Das Wearable meldet

diese Daten an eine Smartphone-App des Wearable-Trägers, mit der die Teilnehmer ihre jeweiligen Verarbeitungs- und Datenschutzpräferenzen verwalten können und die als Nutzerschnittstelle für die Vitaldaten-Kontrolle dient.

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

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

Neben der individuellen Rückmeldung an die Teilnehmer erstellt der Analysedienst auch aggregierte, anonymisierte Gruppenberichte. Dazu werden die Teilnehmer in hinreichend große, möglichst homogene Gruppen eingeteilt, und die Daten aller Gruppenmitglieder werden auf freiwilliger Basis über einen festgelegten Zeitraum gesammelt und zu Gruppenstatistiken ohne Personenbezug aufbereitet. Diese Gruppenberichte sind für das Gesundheitsmanagement des Arbeitgebers bestimmt und sollen Auskunft darüber geben, ob bestimmte Gruppen dauerhafter, gesundheitsschädlicher Überlastung ausgesetzt sind. Weist der Gruppenbericht darauf hin, bietet dies dem Arbeitgeber die Gelegenheit, die Arbeitsabläufe und deren Organisation zu überdenken und den Kontakt mit der betroffenen Gruppe aufzunehmen, um die Belastungen zu senken oder geeignete Ausgleichsmaßnahmen zu treffen.

3 Interaktionskonzepte

In diesem Kapitel stellen wir die erarbeiteten Interaktionskonzepte vor, welche darauf abzielen, die informationelle Selbstbestimmung der Nutzer von Wearables zu stärken und eine transparente und nutzerfreundliche Datennutzung zu gewährleisten. Abbildung 1 zeigt einen Überblick über die wichtigsten Lösungsbausteine für die Herausforderungen, die mit der Verarbeitung und dem Schutz personenbezogener Wearable-Daten verbunden sind. Zu den vorgeschlagenen Patterns gehören zum Beispiel

- eine anonyme Registrierung, um das Verknüpfen der erhobenen Daten mit einer Identität zu vermeiden,
- ein edukatives Onboarding, das die Nutzer über die Datennutzung aufklärt,
- ein übersichtliches Privacy Dashboard zur einfachen Verwaltung von Datenschutzpräferenzen,
- Mechanismen zur Datenverfremdung gemäß individueller Abwägung zwischen bestmöglicher Analysequalität und bestmöglichem Privatsphäre-Schutz sowie
- ein Event-Log, das einen nachvollziehbaren Überblick über alle Datenzugriffe und Datenverarbeitungen bietet.

Im Folgenden beschreiben wir diese Konzepte ausführlicher und diskutieren deren Auswirkungen auf die Datensouveränität.

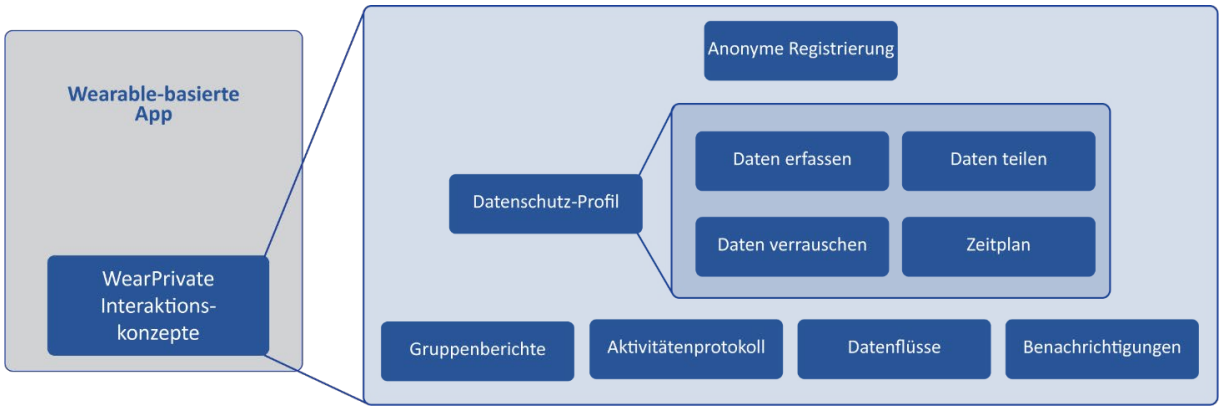

Abbildung 1 Überblick über relevante Aspekte des Interaktionskonzepts

3.1 Registrierung

Viele Dienste, die auf Wearable-Daten basieren, knüpfen die Inanspruchnahme des Dienstes an eine persönliche Registrierung, etwa an die verbindliche Angabe einer persönlichen E-Mail-Adresse, Telefonnummer oder Bankverbindung. Dies vereinfacht das Inkasso bei kostenpflichtigen Dienstleistungen und ermöglicht es dem Dienstleister auf einfache Weise, mit den Dienstnutzern in Kontakt zu treten. Zudem lässt sich so relativ einfach gewährleisten, dass es sich bei einer Anmeldung um einen echten Interessenten handelt und nicht um Vandalismus.

Der Nachteil einer Registrierung mittels Personen- oder Adressangaben ist jedoch, dass dadurch eine vollständig anonyme Nutzung des Dienstes nicht gewährleistet werden kann. Solange das Dienstkonto eines Nutzers mit diesen Angaben verknüpft ist, kann der Nutzer nicht ausschließen, dass die erhobenen Daten eindeutig seiner Person zugeordnet werden können – sei es durch einen nicht vertrauenswürdigen Dienstanbieter oder durch einen IT-Sicherheitszwischenfall in der Verarbeitungskette, bei dem ein Angreifer die vertraulichen Daten des Dienstleisters ausspäht und missbraucht.

Bei einem Anwendungsfall in einem Arbeitnehmerkontext lässt sich das Problem entschärfen, indem der Dienst auf eine personenbeziehbare Nutzerregistrierung verzichtet. Dabei gehen wir davon aus, dass Wearable-basierte Anwendungen zum Arbeits- und Gesundheitsschutz vom Arbeitgeber initiiert und betrieben werden. Da der Arbeitgeber das Messprogramm einrichtet, wird er auch die Kosten dafür tragen. Deshalb kann der Dienstleister seine Dienste mit dem Arbeitgeber abrechnen und benötigt dazu nicht die Kenntnis der individuellen Dienstnutzer.

Daher sieht unser Interaktionskonzept eine anonyme Registrierung mittels Teilnahmecodes vor. Diese Codes sind fälschungssichere digitale Token, die vom Dienstleister erstellt wurden und vom Arbeitgeber zufällig an die Messprogramm-Teilnehmer ausgegeben werden. Dies können etwa QR-Codes sein, die der Teilnehmer zufällig aus einer Lostrommel zieht[1] und unbeobachtet mit seiner App einscannt. Die Wirkungsweise eines Teilnahmecodes entspricht der einer konventionellen Eintrittskarte. Der Teilnehmer weist damit nach, dass sein Arbeitgeber den Dienstleister für den Einlösenden des Codes die erforderliche Teilnahmegebühr entrichtet hat. Bei der Registrierung vergibt der Dienst eine anonyme Teilnehmer-ID als Pseudonym für den Nutzer, unter der alle Stamm- und

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

Vitaldaten zu dieser Person gesammelt und die abgeleiteten Analyseergebnisse abgelegt werden. Soweit der Teilnehmer seine ID nicht gegenüber Kollegen, Arbeitgeber oder Dritten offenbart, lassen sich seine vom Dienst verwalteten Daten nicht ohne Weiteres[2] zu seiner Person zurückverfolgen.

Bei der Erstbenutzung des Teilnahmecodes wählt der Nutzer ein persönliches, nur ihm bekanntes Passwort, mit dem er sich danach als der rechtmäßige Inhaber seiner Teilnehmer-ID ausweisen kann. Selbst bei Kenntnis der Teilnehmer-ID sind die Daten des Teilnehmers für Dritte nur einsehbar, wenn sie das Passwort des Teilnehmers kennen. Sobald die Registrierung erfolgreich abgeschlossen ist, wird der Code für weitere Registrierungen gesperrt, so wie eine Eintrittskarte nach dem Betreten des Veranstaltungsorts entwertet wird. Abbildung 2 zeigt den Ablauf der anonymen Registrierung.

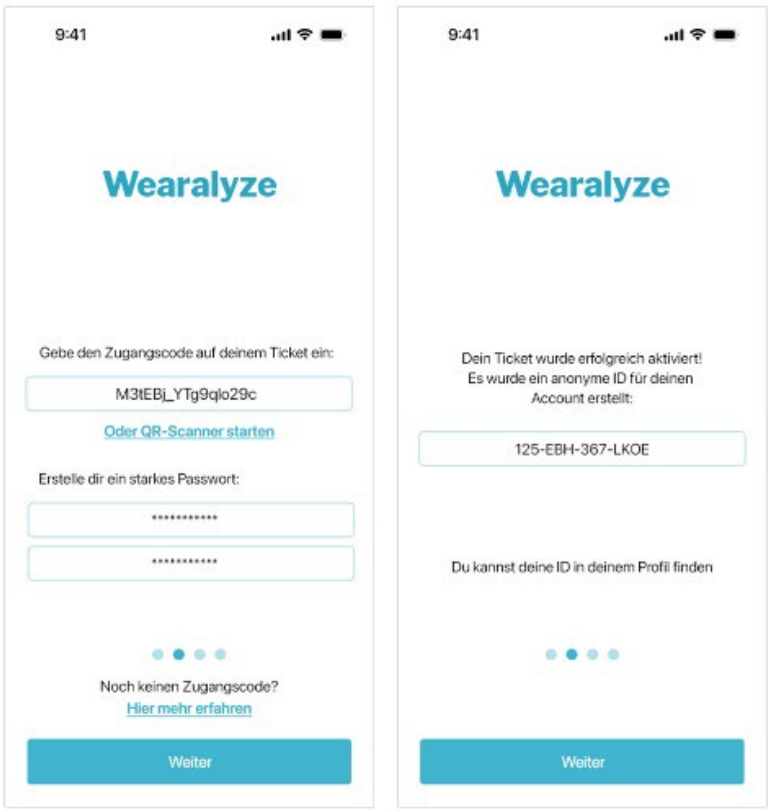

Abbildung 2 Registrierung mittels Teilnehmercode ohne Personenbezug. Im Folgenden kann der Nutzer auf den Dienst mit einer anonymen ID und seinem individuellen Passwort zugreifen, ohne seine wahre Identität zu offenbaren.

Auf diese Weise kann der Analysedienst personenbezogene Datenanalysen bereitstellen und korrekt mit dem Arbeitgeber abrechnen, ohne Wissen darüber, um welche Personen es sich handelt. Wann immer sich ein Teilnehmer mit seiner ID anonym beim Dienstleister anmeldet und sich per Passwort als rechtmäßiger Inhaber dieser Teilnehmer-ID ausweist, kann die Person auf die Konfigurations-

[2] Manche Daten, die mittels Wearables erhoben werden können, sind charakteristisch für den Wearable-Träger. So sind zum Beispiel bestimmte Bewegungsmuster von Mensch zu Mensch so unterschiedlich, dass eine Wiedererkennung möglich ist, wenn man das Muster einer bekannten Person mit dem einer Reihe von Vergleichsproben aus einem anonymen Datenbestand vergleicht. Das Vitaldatenmuster fungiert hier als eindeutiger »Fingerabdruck« der betreffenden Person. Als Gegenmaßnahme gegen mögliche »Fingerprinting«-Angriffe sieht unser Konzept eine Datenverfremdung vor (siehe Abschnitt 3.7)

einstellungen, Daten und Analyseergebnisse des Nutzerkontos zugreifen, das für diese Teilnehmer-ID eingerichtet wurde. Die Person muss sich dabei jedoch nicht zu erkennen geben.

3.2 Onboarding

Onboarding bezeichnet den Prozess der schrittweisen Einführung neuer Anwender in die Nutzung einer App. Ziel des Onboardings ist es, die Nutzer mit den wichtigsten Funktionen und der Bedienung der App vertraut zu machen, um ihnen den Einstieg zu erleichtern und ein positives erstes Nutzungserlebnis zu schaffen. Abbildung 3 zeigt die Onboarding-Sequenz im Überblick.

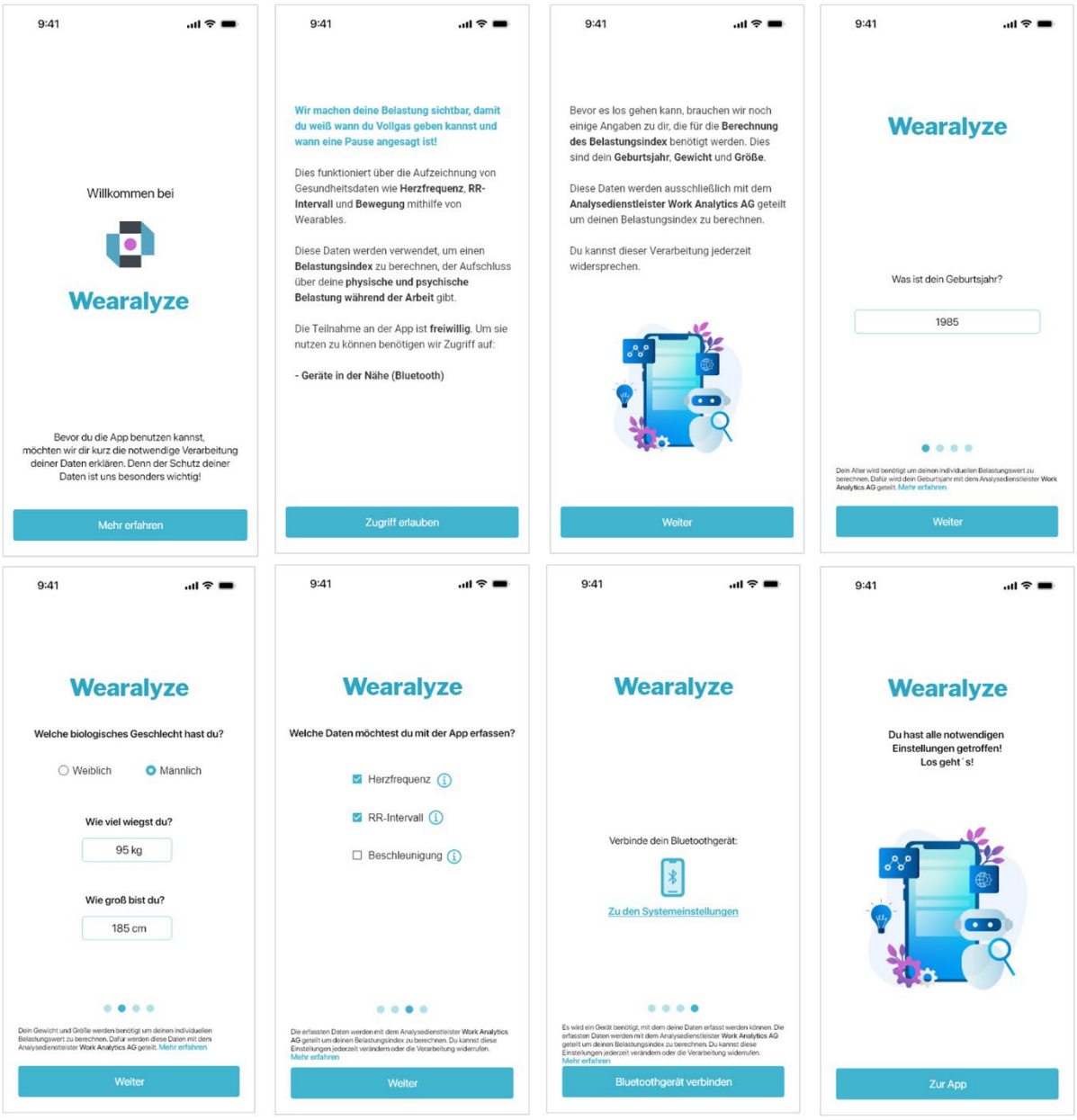

Abbildung 3 Übersicht über die Bildschirmansichten der Onboarding-Sequenz

Im Kontext datenschutzbezogener Interaktionskonzepte dient das Onboarding insbesondere dazu, neue Nutzer über die mit der Nutzung verbundene Verarbeitung ihrer Daten zu informieren und

Vertrauen aufzubauen. Dies soll sicherstellen, dass Nutzer von Anfang an ein klares Verständnis davon haben, welche Daten gesammelt und wie diese von wem verarbeitet werden.

Das Onboarding bietet die erste Gelegenheit, die Nutzer umfassend zu informieren und sie aktiv in den Datenschutzprozess einzubinden. Dabei erfahren sie, welche Daten die App sammelt, warum diese Daten benötigt und wie sie geschützt werden. Ein solches Onboarding soll zudem über die verfügbaren Datenschutzoptionen aufklären und den Nutzern ermöglichen, bewusste Entscheidungen darüber zu treffen, welche Daten sie teilen möchten. Dies trägt wesentlich zur Stärkung des Rechts auf informationelle Selbstbestimmung bei, da die Anwender die Entscheidung über die Nutzung der App auf Basis von fundiertem Wissen treffen können.

Das Onboarding unterstützt das Recht auf Selbstbestimmung und Transparenz, indem alle notwendigen Einwilligungen eingeholt werden, bevor personenbezogene Daten verarbeitet werden. Beispielsweise werden die Nutzer explizit gefragt, ob sie der Aufzeichnung von bestimmten Daten zustimmen. Sie können diese Entscheidungen bewusst treffen und ihre Präferenzen individuell anpassen.

3.3 Stammdatenerfassung

Neben aufklärenden Aspekten werden im Onboarding zudem die benötigten Stammdaten wie Alter, Geschlecht, Größe oder Gewicht abgefragt. Diese Angaben sind notwendig, um den in der App genutzten Belastungsindex zu ermitteln. Um auch hier den Nutzern die größtmögliche Sicherheit in Bezug auf ihre Anonymität zu geben, werden die Daten nur in der Granularität abgefragt, in der sie zur Berechnung wirklich benötigt werden. Dies bedeutet zum Beispiel, dass nicht das genaue Geburtsdatum, sondern lediglich das Geburtsjahr angegeben werden muss. Generell sind bezüglich der Stammdatenerfassung verschiedene Umsetzungen denkbar, die mit unterschiedlichen Vorzügen und Nachteilen verbunden sind:

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

Die Auswahl des Verfahrens hängt vom jeweiligen Anwendungsfall ab. Insbesondere ist zu berücksichtigen, wie sensitiv die angestrebte Datenanalyse auf die Genauigkeit der verwendeten Rohdaten reagiert und welche Qualitätsansprüche die Nutzer an die Genauigkeit der Datenauswertung haben. Im WearPrivate-Projekt haben wir uns für dafür entschieden, die Daten genau abzufragen, den Nutzern aber anzubieten, die Daten auf Wunsch vor der Übermittlung zu verfremden. Dieser Ansatz hat den Vorteil, dass die angebotenen Unschärfegrade von den Entwicklern der Anwendung so festgelegt werden können, dass je nach Verfremdungsgrad vorgegebene Qualitätsstufen gewahrt bleiben. Würde man den Nutzern freistellen, die Genauigkeit ihrer Angaben nach eigenem Gutdünken zu wählen, wäre bei der Datenauswertung keine klare Abschätzung mehr möglich, wie belastbar die Analyseergebnisse auf der Basis verfremdeter Rohdaten sind.[3]

[3] Will man dem Nutzer freistellen, bei der Angabe seiner Stammdaten ein wenig zu flunkern, so sollte die App zumindest darüber informieren, in welchem Ausmaß die Angabe verfälscht sein darf, um eine der drei Qualitätsstufen zu garantieren. Da die Genauigkeitstoleranz je nach Wertebereich schwanken kann, erreicht

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

Der mögliche Grad einer Datenverfremdung hängt stark von dem jeweiligen Stammdatenattribut ab sowie vom Typ der Analysen, in die dieses Attribut einfließen soll. Manche Auswertungen reagieren sensibel auf geänderte Stammdaten, während andere in einem großen Toleranzbereich stabile Ergebnisse liefern. So fließt zum Beispiel in die Berechnung des Body-Mass-Index (BMI) das Körpergewicht linear, die Körpergröße jedoch quadratisch ein:

BMI = Körpergewicht / (Köpergröße * Körpergröße)

Daher verändert sich das Ergebnis einer BMI-Berechnung nur linear mit einer geändertem Gewichtsangabe, aber quadratisch mit einer geänderten Größenangabe. Hier bieten sich also größere Spielräume für eine Verfremdung der Gewichtsangabe als für eine Verfremdung der Größenangabe. Dies muss bei der Umsetzung des Interaktionskonzepts zuvor geprüft werden, um die Stärke der Verfremdung gegen die erzielbare Analysequalität geeignet abzuwägen.

3.4 Datenschutz-Profil

Das Datenschutzprofil ist ein zentrales Interaktionskonzept, das den Nutzern eine transparente Übersicht über die Verarbeitung ihrer Daten bietet. Es ermöglicht ihnen, ihre Datenschutz- und Datennutzungseinstellungen effektiv zu überwachen und zu steuern, indem die wesentlichen Informationen und Einstellungsmöglichkeiten klar und übersichtlich in einem Dashboard dargestellt werden.

Die erfassten Daten, die Zwecke der Datennutzung sowie die aktuellen Einstellungen zur Datenverrauschung und Analysequalität werden in Form von Kacheln übersichtlich dargestellt (Abbildung 4). So können die Nutzer auf einen Blick zu erkennen, ob die bestehenden Einstellungen ihren persönlichen Präferenzen entsprechen und ob sie gegebenenfalls Anpassungen vornehmen sollten. Die Übersichtlichkeit erlaubt es den Arbeitnehmenden, rasch Änderungen vorzunehmen, beispielsweise die Erfassung bestimmter Daten einzuschränken oder die Datenverfremdung zu erhöhen, um den Schutz der Roh- und Analysedaten der jeweiligen Erfassungssituation anzupassen.

Ein wesentlicher Aspekt des Datenschutzprofils ist die Transparenz. Nutzer können sich jederzeit über die Verarbeitung ihrer Daten sowie die damit verbundenen Einstellungen informieren. Dies fördert das Vertrauen in das System und gewährleistet, dass die Datennutzung den tatsächlichen Wünschen des Nutzers entspricht. Des Weiteren fördert das Dashboard die Selbstbestimmung, da es den Nutzern ermöglicht, ihre Datenschutzpräferenzen jederzeit anzupassen und somit die Kontrolle über ihre persönlichen Daten zu behalten.

---

dieser Ansatz schnell seine Grenzen (»Wenn du weniger als 60 kg wiegst, solltest du bei der Angabe deines Körpergewichts um höchstens -7 bis +5 Prozent vom wahren Wert abweichen, bei einem höheren Gewicht um höchstens +/- 4 Prozent.«). Dies gilt insbesondere, wenn neben Gewicht, Körpergröße, Alter und Geschlecht noch weitere Stammdaten benötigt werden und jede Angabe unterschiedliche Genauigkeitsanforderungen für unterschiedliche Wertebereiche und Qualitätsstufen hat.

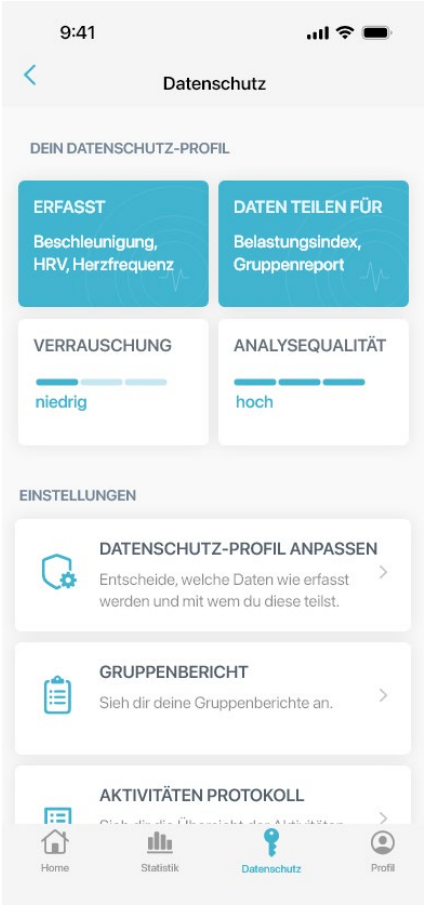

Abbildung 4 Grundansicht der Datenprofileinstellungen mit einer Übersicht über die wichtigsten Konfigurationseinstellungen. Von hier aus kann der Nutzer in die verschiedenen Aspekte verzweigen, die Transparenz und informationelle Selbstbestimmung betreffen, um die Einstellungen seinen Präferenzen anzupassen.

Unterhalb des Dashboards sind weitere Funktionen wie Gruppenberichte, Aktivitätenprotokoll und Benachrichtigungseinstellungen zu finden, wodurch die Seite zum Ausgangspunkt aller datenschutzrelevanten Interaktionen wird. Das Privacy-Dashboard stellt somit ein zentrales Element zur benutzerzentrierten Gestaltung von Datenschutzfunktionen dar, welches eine einfache Bedienung und eine verständliche Darstellung komplexer Prozesse vereint.

3.5 Vital- und Kontextdatenerfassung

Um die Funktionalitäten der App nutzen zu können, müssen persönliche Daten der Nutzer dynamisch erfasst werden. Hierzu zählen Vitaldaten wie beispielsweise der Puls, das sogenannte RR-Intervall (für die Berechnung der Herzratenvariabilität) oder Beschleunigungsdaten, aber gegebenenfalls auch Kontextinformationen wie Standort, Temperatur, Luftfeuchtigkeit oder Lärmpegel. Die Vital- und Kontextdatenerfassung adressiert die datenschutzfreundliche Erfassung solcher Wearable-Daten für das vorgesehene Messprogramm.

Aus Sicht der Datensouveränität gibt es unterschiedliche Ansätze für die Handhabung der Datenerhebung (siehe Abbildung 5). So kann man die Nutzer selbst entscheiden lassen, welche Daten erfasst werden sollen, oder der Arbeitgeber kann die erforderliche Datenerhebungen verbindlich

festlegen.[4] Beide Varianten wirken sich unterschiedlich auf die informationelle Selbstbestimmung sowie den Nutzen der App aus.

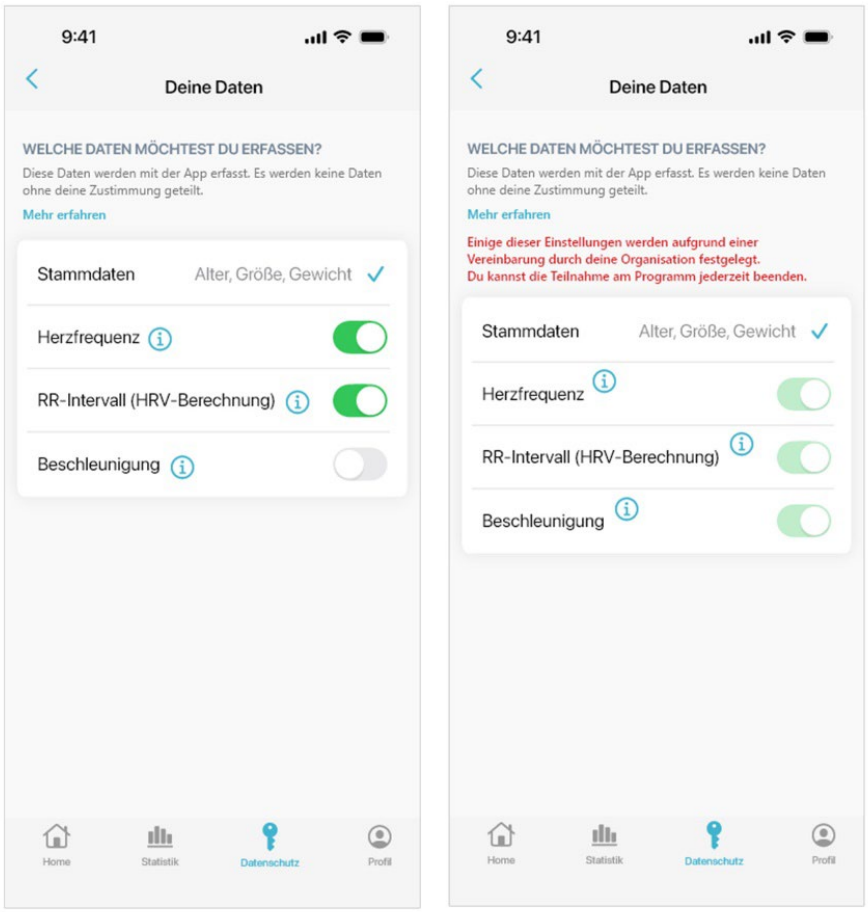

Abbildung 5 Nutzer erhalten eine Übersicht über alle erfassten Rohdaten und können meist selbst bestimmen, welche Daten erfasst werden und welche nicht (links in der Abbildung). Verweigert ein Nutzer die Zustimmung zur Erfassung bestimmter Daten, so weist die App auf mögliche Funktionsbeeinträchtigungen hin. Ist die Auswahl Arbeitgeber-seitig beschränkt und sind gewisse Einstellungen nicht änderbar, verweist die App auf die Freiwilligkeit der Teilnahme und die Möglichkeit, das Messprogramm zu verlassen (rechts in der Abbildung).

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

Die Entscheidung, bestimmte Daten nicht zu erfassen, hat jedoch unmittelbare Auswirkungen auf die Funktionalität der App, wie unser Anwendungsbeispiel illustriert. Eine zu starke Einschränkung der Datenerhebung kann dazu führen, dass die Berechnung eines aussagekräftigen Belastungsindex nicht mehr möglich ist und so der Nutzen der App verloren geht. Demnach ist es wichtig, die Nutzer darüber

[4] Die Zustimmung zu einer Vitaldatenerfassung am Arbeitsplatz muss immer freiwillig erfolgen. Allerdings kann der Arbeitgeber, der seiner Belegschaft ein solches Messprogramm auf freiwilliger Basis anbietet, die Teilnahme an dem Programm an die Bedingung knüpfen, dass sich die Teilnehmer zur Erhebung und Weiterverarbeitung bestimmter Messwerte bereiterklären – etwa, weil sonst die Ziele des Messprogramm nicht erreicht werden können. Es bleibt dann den Betroffenen überlassen, inwieweit sie bereit sind, persönliche Daten preiszugeben, um in den Genuss der Vorteile des Messprogramms zu kommen, oder das Teilnahmeangebot lieber ausschlagen.

zu informieren, inwieweit ihre vorgenommenen Einstellungen die Funktionalität der Anwendung beeinträchtigen.

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

Der transparente Umgang mit der Datenerhebung und die Erläuterung möglicher Konsequenzen dienen der Stärkung des Nutzervertrauens und ermöglichen eine informierte Entscheidung über die Teilnahme am Messprogramm und die Nutzung bestimmter Funktionen. Das Konzept berücksichtigt somit die Anforderungen an Transparenz, wodurch die Selbstbestimmung der Nutzer gestärkt wird.

3.6 Nutzungskontrolle über die Verwendung und Weitergabe von Daten

Ein weiteres Interaktionskonzept befasst sich mit der Datennutzungskontrolle, also der Erteilung von Datenzugriffs- und Datenauswertungsrechten sowie der Festlegung des Empfängerkreises, mit dem die Daten geteilt werden dürfen. Mittels der Funktionalität *Daten teilen* legt der Nutzer fest, für welche spezifischen Zwecke die Weitergabe der Daten zulässig ist (Abbildung 6). In diesem Kontext werden sämtliche verfügbare Optionen aufgelistet, beispielsweise die Nutzung der Daten zur Berechnung des Belastungsindex, für die Teilnahme am Gruppenbericht, für den Erhalt individueller Hinweise oder für weitere Verwendungsmöglichkeiten, etwa die freiwillige Datenspende an Forschungseinrichtungen. Jeder dieser Zwecke wird durch eine präzise Erläuterung ergänzt, wem der Zugriff bei Zustimmung zu welchem Zweck gestattet wird. Dies ermöglicht den Nutzern eine informierte Entscheidung, ob und in welchem Umfang sie die betreffenden Daten teilen möchten.

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

- Die Nutzer können die volle Kontrolle über die Weitergabe ihrer Daten erhalten. Das heißt, sie können selbstbestimmt entscheiden, für welche Zwecke die Daten verwendet werden dürfen. Dies gewährleistet die größtmögliche Freiheit im Umgang mit den eigenen Daten. Es birgt jedoch für den Arbeitgeber das Risiko, dass sich beispielsweise nicht genügend Mitarbeiter für eine Teilnahme am Gruppenbericht entscheiden, wodurch dieser an Aussagekraft verliert oder sogar aufgrund geringer Teilnehmerzahl nicht datenschutzkonform erstellt werden kann.
- Alternativ dazu besteht die Möglichkeit, dass der Arbeitgeber bestimmte Voreinstellungen trifft und damit festlegt, für welche Zwecke die Daten (mindestens) geteilt werden müssen. Ein Beispiel für eine solche Verpflichtung ist die Teilnahme der Mitarbeiter am Gruppenbericht, der Informationen über die aggregierten Daten zur Arbeitsbelastung für eine bestimmte Mitarbeitergruppe enthält. Da dies jedoch die Selbstbestimmung der Betroffenen einschränkt, wird eine transparente Kommunikation angestrebt. Den Nutzern soll dabei

vermittelt werden, warum ihre Wahlmöglichkeit eingeschränkt ist und dass sie jederzeit die Teilnahme am Messprogramm beenden können, wenn sie dem nicht zustimmen wollen.

Die Ausgestaltung dieses Interaktionskonzepts ist von großer Bedeutung für die Transparenz der Datenverarbeitung. Die erklärende Darstellung der jeweiligen Verwendungszwecke und der damit verbundenen Zugriffsrechte ermöglicht den Nutzern eine souveräne Entscheidung bezüglich ihres individuellen Datenschutzbedarfs.

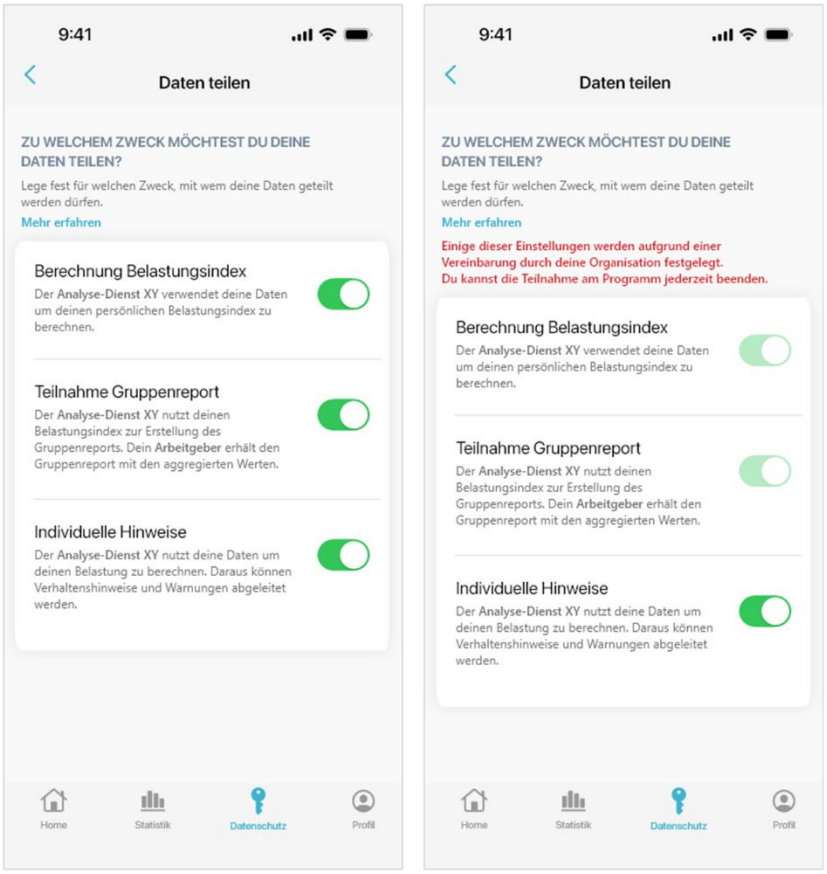

Abbildung 6 Wie bei der Datenerfassung erhalten die Nutzer auch bei der Datennutzung eine vollständige Übersicht über alle möglichen Verwendungszwecke. In der Regel können sie auch selbst bestimmen, welchen dieser Datennutzungen sie zustimmen wollen und welchen nicht. Hat der Arbeitgeber die Auswahlmöglichkeiten aus organisatorischen Gründen beschränkt, so weist die App auf diese Beschränkungen hin sowie auf die Möglichkeit, die freiwillige Teilnahme am Messprogramm jederzeit zu beenden.

3.7 Datenverfremdung

In unserem Demonstrator-Anwendungsfall (vgl. Kapitel 2) streben wir grundsätzlich an, die erfassten Vitaldaten ohne Personenbezug zu verarbeiten. Dazu dient insbesondere das anonyme Registrierungsverfahren (vgl. Abschnitt 3.1), das auf Personenbezüge wie die Angabe von Namen, E-Mail-Adressen oder Telefonnummern verzichtet. Stattdessen werden die Daten einer Person unter einer zufälligen, nutzerspezifischen Teilnehmer-ID verwaltet, also einem Pseudonym, dessen wahre Identität nur dem jeweiligen Nutzer selbst bekannt ist.

Ungeachtet dieser Maßnahme kann man jedoch die Anonymität der Daten nicht unter allen Umständen garantieren. Wenn zum Beispiel ein ambitionierter Hobbyradler in seiner Sportgruppe eine Aufzeichnung seiner Herzratenvariabilität in einer Chatgruppe im Internet veröffentlicht, dann besteht

die Gefahr, dass ein Angreifer diese Aufzeichnung mit den im Messprogramm erfassten Vitaldaten abgleicht, um sie so wieder dem Chatgruppen-Mitglied zuzuordnen und damit deren Urheber zu enttarnen.

Das Risiko eines solchen Datenabgleichs besteht immer dann,

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

Es gibt Untersuchungen, die belegen, dass gewisse Vitaldaten eine Person tatsächlich eindeutig charakterisieren können oder eine Personenzuordnung zumindest drastisch erleichtern, darunter zum Beispiel Bewegungsmuster oder individuelle Merkmale des Herzschlags (siehe dazu Ergebnisbericht D6.1 [4]). Solange die erhobenen Vital- und Analysedaten nicht in fremde Hände geraten und der Analysedienst die Datenschutzbestimmungen einhält oder solange ein Angreifer keine personenbezogenen Vergleichsdaten erheben kann, sind solche »Fingerprinting«-Angriffe jedoch abgewendet. Allerdings besteht ein Restrisiko, dass die Daten durch eine Verarbeitungspanne oder einen Hackerangriff öffentlich werden oder dass ein Mitarbeiter des Dienstleisters als Innentäter in Erscheinung tritt und die Daten missbraucht.

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

Sowohl die Stammdaten als auch die dynamisch erhobenen Vitaldaten sind potenzielle Kandidaten für eine Datenverfremdung. Es gibt verschiedene Optionen, dem Nutzer Kontrolle über die Art und den Grad der Verfremdung zu ermöglichen. Wie in Abschnitt 3.3 am Beispiel der Stammdaten bereits erläutert, haben die Verfahren jeweils spezifische Vorzüge und Nachteile, die je nach Anwendungsfall gegeneinander abzuwägen sind. Dabei ist vor allem zu berücksichtigen, dass mit einer zunehmenden Datenverfremdung eine zunehmende Einbuße an Analysequalität verbunden ist.

Konkret bietet unser Interaktionskonzept den Nutzern drei Verrauschungsstufen zur Auswahl an. Je nach gewählter Stufe ergibt sich eine entsprechende, gegenläufige Qualität der Analysebefunde: Bei schwacher Verrauschung erhält der Nutzer eine hohe Analysequalität; während starke Verrauschung eine niedrige Qualität der Befunde bedingt. Dies wird dem Nutzer in der App visuell zurückgespiegelt, wie in Abbildung 7 dargestellt. Die Datenverrauschung ist technisch so realisiert, dass sich die Verfremdung der Daten langfristig ausmittelt; der Mittelwert der Daten bleibt gleich, um die Analyseergebnisse nicht systematisch zu verschieben.

Das Interaktionskonzept setzt voraus, dass vom Entwickler der Anwendung eine sinnvolle Abstufung gewählt wurde, die den Nutzen der App nicht ad absurdum führt. Um zu ergründen, wie stark die Nutzerdaten verfremdet werden müssen, um einen vorgegebenen Privacy-Effekt zu erzielen, können die Entwickler zum Beispiel auf die Prinzipien der Differential Privacy zurückgreifen. Die so ermittelten Verfremdungsgrade können dann auf Testdaten angewendet werden, um zu sehen, wie stark die gewünschte Verfremdung die Analyseergebnisse verfälscht und damit die Analysequalität schmälert.

Sofern sich im Test sinnvolle Abwägungen zwischen Differential Privacy und Analysequalität ergeben, liefert dies die Grundlage für die im Interaktionskonzept angebotenen Verrauschungsstufen. Näheres zur Anwendung von Differential Privacy findet sich in [1] im Abschnitt 2.3.1.3 sowie im Evaluationsbericht [4].

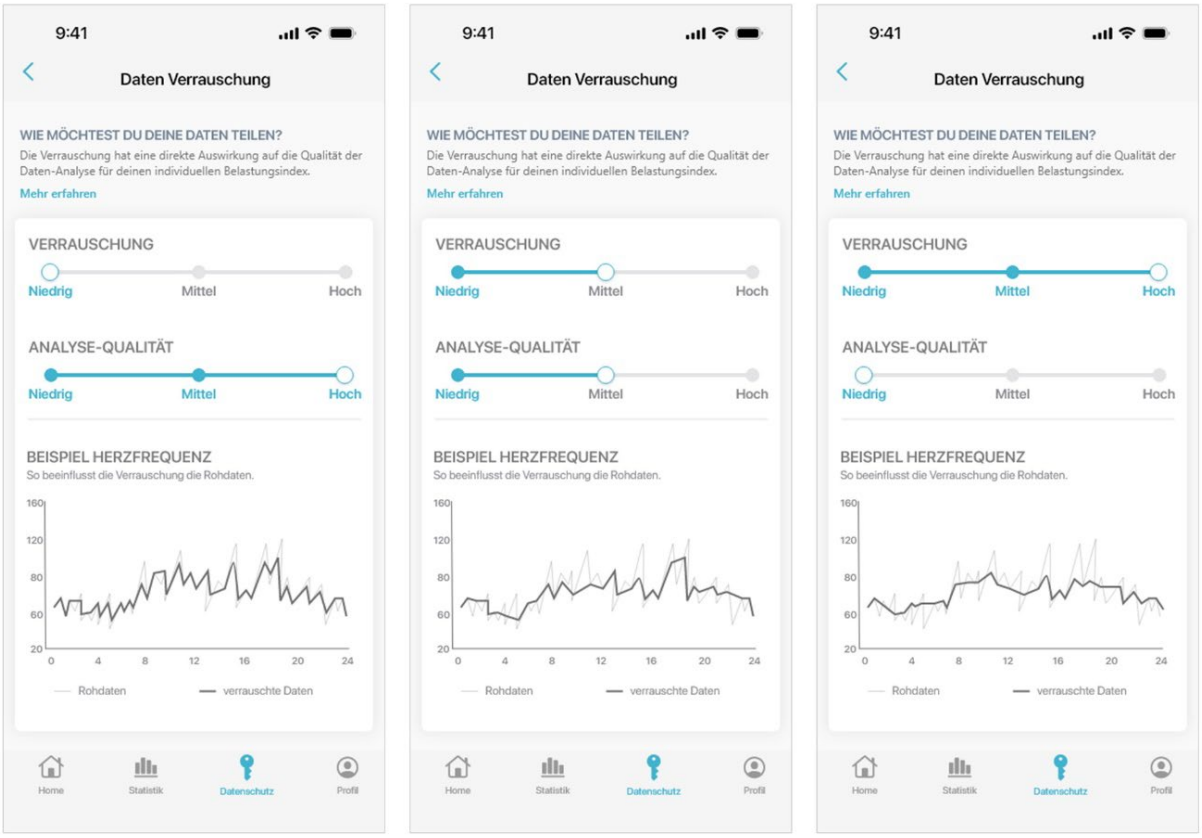

Abbildung 7 Bewusste Verfremdung der gemessenen Stamm- und Vitaldaten, um eine Identifizierung der Person durch einen Datenabgleich mit einer externen personenbezogenen Datenquelle zu erschweren. Da im Allgemeinen die Güte der Analyseergebnisse mit zunehmender Verfremdung der Daten sinkt, bietet die App den Nutzern die Auswahl zwischen drei verschiedenen Verrauschungsstufen und zeigt an, wie die getroffene Wahl die Qualität der Analysen beeinflusst.

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

3.8 Zeit- und ortsabhängige Datenerfassung

In dem im Projekt betrachteten Anwendungsfall werden Vitaldaten im beruflichen Kontext erhoben und nach Einwilligung in aggregierter Form mit dem Arbeitgeber geteilt. Um in einem solchen Szenario,

das die Privatsphäre der Nutzer erheblich berührt, das Vertrauen der Mitarbeiter zu stärken und so ihre Mitwirkung am Messprogramm zu fördern, sollte die Anwendung auf Wunsch sicherstellen, dass keine Daten außerhalb des Arbeitskontexts erhoben und verarbeitet werden. Die zeit- und ortsabhängige Datenerfassung ermöglicht den Nutzern, die Erfassung ihrer Vitaldaten an individuelle zeitliche und örtliche Beschränkungen zu knüpfen.

Bei der zeitabhängigen Datenerfassung kann der Nutzer in einem Tages- und Stundenraster festlegen, zu welchen Zeiten die App automatisiert Daten erfassen darf. Die Aufzeichnungszeiträume können individuell konfiguriert werden, beispielsweise gemäß den persönlichen Arbeitszeiten oder Schichtplänen (Abbildung 8, links). Die App erfasst daraufhin die Vitaldaten ausschließlich in den vorgegebenen Zeitintervallen und verhindert so, dass die Datenerfassung unbeabsichtigt auch in der Freizeit fortgesetzt wird. Gleichzeitig entfällt das Risiko, das manuelle Starten der Erfassung bei Arbeitsbeginn zu vergessen. Ein solcher Automatismus ist besonders nützlich für den Einsatz von Wearables wie etwa Smart Watches, die kontinuierlich getragen werden, also auch in der Freizeit. Ist die Nutzung des Wearables hingegen an eine besondere Berufskleidung gebunden, ergibt sich das Arbeitszeitintervall oft schon durch den Kleiderwechsel.

Eine weitere Möglichkeit ist die ortsabhängige Datenerfassung. Hierbei können Nutzer Orte auf einer Karte definieren, in deren Umkreis die Datenerfassung erfolgen darf (Abbildung 8, rechts). Betritt der Nutzer den Bereich, so startet die Datenerfassung automatisch. Verlässt der Nutzer den Bereich, wird die Datenerfassung automatisch pausiert oder bei längerer Abwesenheit ganz gestoppt. Diese Funktion schützt vor unbeabsichtigter Datenerfassung außerhalb der Arbeitsumgebung.

Die ortsabhängige Erfassung kann auf unterschiedliche Weise kontrolliert werden:

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

Abbildung 8 zeigt, wie sich GNSS-basierte ortbezogene Erfassungsbeschränkungen einfach konfigurieren und anschaulich darstellen lassen.

Eine Zeit- oder Ortsbeschränkung der Wearable-Messungen bietet den Nutzern flexible Möglichkeiten, die Erfassung der Daten zu kontrollieren und ihre Privatsphäre in ihrer Freizeit abzusichern. Je nach beruflicher Situation können die Vorteile des einen oder andere Konzepts überwiegen. Ändern sich die Arbeitszeiten häufig oder weichen sie aufgrund von Urlaub oder Krankheit vom üblichen Tagesablauf ab, so muss der Nutzer bei der zeitbasierten Erfassung gegebenenfalls ständige Anpassungen in der

App vornehmen. Ein häufiger Wechsel des Arbeitsorts würde dagegen die Nutzung der ortsbasierten Erfassung beeinträchtigen.

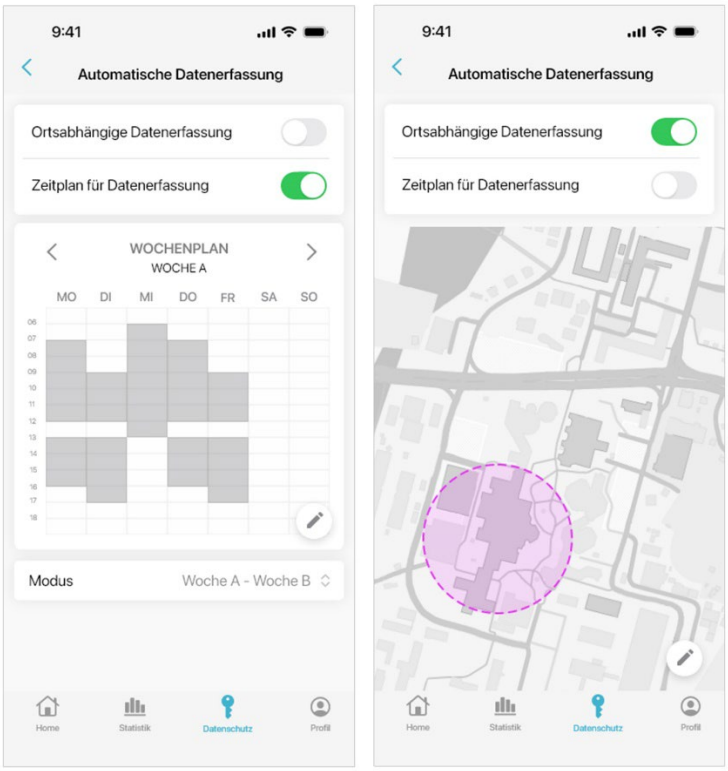

Abbildung 8 Zeitbezogene Einschränkung der Vitaldatenerfassung durch individuellen Wochenplan oder ortsbezogene Einschränken der Vitaldatenerfassung durch Geo-Fencing.

Beide Mechanismen tragen zur Stärkung der informationellen Selbstbestimmung bei, indem sie eine klare, automatisch überwachte Trennung zwischen Arbeitszeit und Freizeit ermöglichen.

3.9 Event-Log

Das Event-Log ist ein weiteres Interaktionskonzept zur Erhöhung der Transparenz bei der Datenverarbeitung. Es dient als detailliertes Protokoll, das alle Ereignisse und Aktionen im Zusammenhang mit der Datenerfassung, -verarbeitung und -weitergabe dokumentiert. Diese Ereignisse werden in chronologischer Reihenfolge angezeigt, so dass der Nutzer einen vollständigen Überblick über alle datenschutzrelevanten Vorgänge erhält (Abbildung 9).

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

Zudem beugt das Event-Log Missverständnissen oder Unsicherheiten in Bezug auf die persönlichen Datenschutzeinstellungen vor. Wenn der Effekt einer Konfigurationseinstellung sich im Event-Log nicht wie beabsichtigt niederschlägt, ist dies ein Warnzeichen für die Anwender: Gegebenenfalls fehlt noch eine wichtige Einstellung in der persönlichen Datenschutzkonfiguration oder die Wirkung einer

Konfigurationsoption wurde falsch eingeschätzt. Dies können die Nutzer zum Anlass nehmen, ihre datenschutzrelevanten Einstellungen noch einmal genauer zu überprüfen und anzupassen.

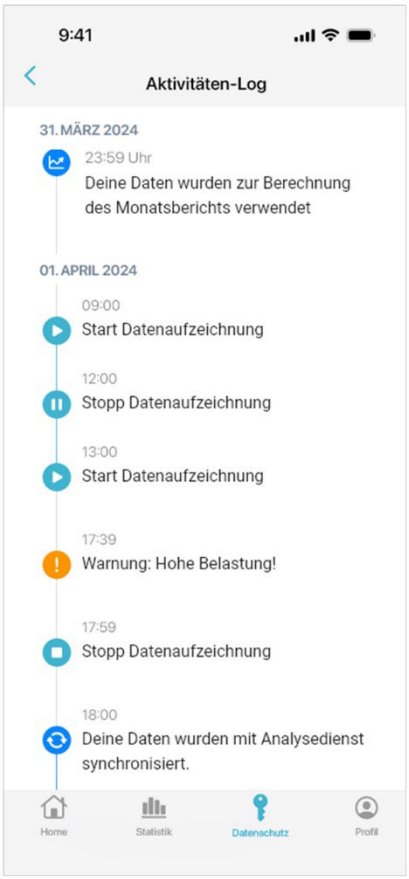

Abbildung 9 Die App erfasst alle Ereignisse, die den Datenschutz und die Privatsphäre betreffen, und zeigt sie in chronologischer Reihenfolge an. Die App-Nutzer können so ihre Vitaldatenerfassung, -verarbeitung und Weiterleitung nachverfolgen, um volle Transparenz über die Datennutzung zu erhalten.

3.10 Begrenzung der Speicherdauer

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

Für ein persönliches, unmittelbares Vitaldaten-Feedback – also der kontinuierlichen Ermittlung eines Momentan-Belastungsindex – genügt es im Prinzip, die Wearble-Messdaten nur über ein kurzes Intervall von wenigen Minuten verfügbar zu halten.[5] Danach können die Roh- und Analysedaten gelöscht werden und sind damit nicht mehr angreifbar.

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

Sieht das Messprogramm am Arbeitsplatz jedoch einen wöchentlichen oder monatlichen Gruppenreport vor, dann müssen die Daten der teilnehmenden Gruppenmitglieder mindestens über diesen Zeitraum aggregiert werden, ehe eine Löschung aus Datenschutzgründen erfolgen kann. Ein datenschutzfreundliches Berechnungskonzept sollte allerdings anstreben, die individuellen Daten der Gruppenmitglieder sofort zu aggregieren und danach nur die aggregierten Werte zu speichern, die Individualdaten jedoch sofort nach deren Aggregierung zu löschen. Die Gangbarkeit dieses Ansatzes hängt jedoch von den Messzielen und dem spezifischen Aggregierungsverfahren ab.

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

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

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

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

Wie bei anderen Einstellungen des Datenschutzprofils kann der Arbeitgeber auch hier die Wahlmöglichkeiten aufgrund betrieblicher oder technischer Gründe einschränken (vgl. etwa Abschnitt 3.6 und Abbildung 6). Die Nutzer müssen sich dann mit beschränkten Selbstbestimmungsoptionen arrangieren oder auf die freiwillige Teilnahme am Messprogramm verzichten.

3.11 Visualisierung der Datenflüsse

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

Dazu wird die Übertragungskette durch eine interaktive, animierte Grafik visualisiert, die den realen Fluss der Daten simuliert. Die Grafik stellt die verschiedenen Akteure dar, die an der Datenverarbeitung beteiligt sind, und sie zeigt auf, welche Akteure Zugriff auf welche Daten erhalten (Abbildung 10).

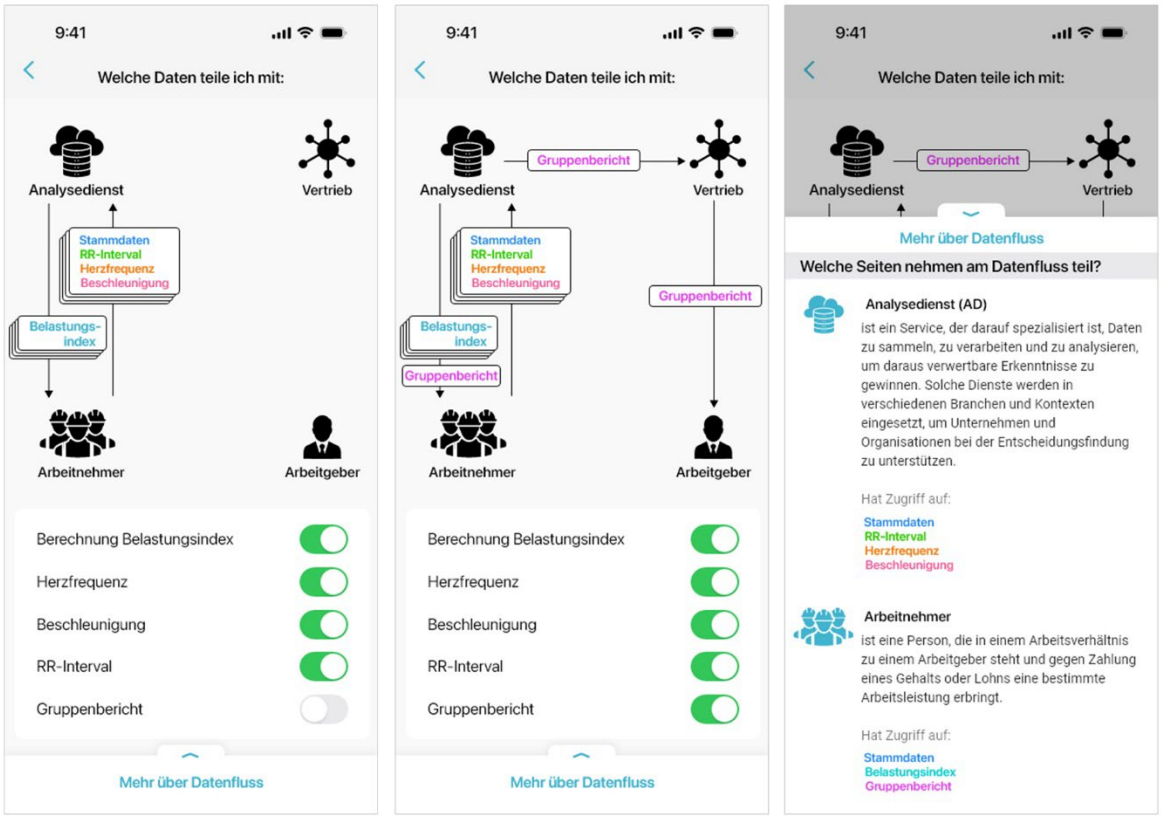

Abbildung 10 Je nach der Auswahl der Daten, die ein Nutzer mit dem Analysedienst oder seinem Arbeitgeber teilt, ergeben sich unterschiedliche Datenflüsse. Um zu verdeutlichen, wie sich die Einstellungen der Nutzer auf ihre Privatsphäre auswirken, stellt die App dar, welche Datenflüsse sich aus den gewählten Einstellungen jeweils ergeben.

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

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

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

4 Transparenzgesichtspunkte des Interaktionskonzepts

Transparenz spielt eine entscheidende Rolle für einen nutzerfreundlichen Datenschutz, da sie Vertrauen schafft und die Nutzer in die Lage versetzt, fundierte Entscheidungen über ihre Daten zu treffen. Transparenz bedeutet in diesem Zusammenhang, dass Unternehmen und Organisationen offen und klar über ihre Datenschutzpraktiken informieren und den Nutzern aufzeigen, wie ihre Daten erhoben, verarbeitet und weitergegeben werden. Bei der Verarbeitung sensibler Daten wird dies zunehmend von Nutzern und im Kontext personenbezogener Daten auch vom Gesetzgeber gefordert [3].

Für die Praxis bedeutet dies vielfach, dass komplexe Sachverhalte und Prozesse so aufbereitet werden müssen, dass diese für Nutzer – auch für IT-Laien – verständlich und interpretierbar sind. Im Kontext unseres Anwendungsfalls haben wir mehrere Funktionen und Ausgestaltungen erprobt, die auf eine Erhöhung der Transparenz abzielen. So werden Nutzer schon zu Beginn der App-Nutzung im *Onboarding* transparent über alle notwendigen Einwilligungen und Datenverarbeitungen aufgeklärt. Hierbei werden den Nutzern relevante Informationen für eine informierte Entscheidung zur Verfügung gestellt und nicht nur nach Zustimmung zur Verarbeitung für erforderliche Daten gefragt. Das *Datenschutz-Profil* dient als zentrale Stelle für datenschutzrelevante Informationen und Einstellungen. Es hat das wesentliche Ziel, den Ist-Zustands der getroffenen Einstellungen und Datenverarbeitungen auf einen Blick zu ermöglichen. So können Nutzer leicht nachvollziehen, wie der aktuelle Schutz ihrer Privatsphäre konfiguriert ist und gegebenenfalls von hier aus schnell Änderungen vornehmen.

In den Bereich *Vital- und Kontextdatenerfassung* sowie *Datenzugriff* können Nutzer jederzeit sehen, welche Daten erhoben und mit wem diese geteilt werden. Jedes Datum und jeder Nutzungszweck ist darüber hinaus mit weitergehenden Informationen angereichert, wie zum Beispiel der Erläuterung, was das RR-Intervall ist und warum es benötigt wird, oder auch, mit wem die Daten geteilt werden, wenn Nutzer der Berechnung des Belastungsindex zustimmen.

Bei der *Datenverfremdung* zielt der Aspekt der Transparenz auf die verständliche Darstellung komplexer und fachspezifischer Datenschutzmechanismen ab. Zu diesem Zweck werden die Auswirkungen der vorgenommenen Einstellungen anhand des Zusammenspiels von Datenverfremdung und Analysequalität dargestellt, die sich gegenseitig beeinflussen. Zudem werden anhand eines beispielhaften Datengraphs die Änderungen vereinfacht visualisiert. Durch diese Maßnahmen ist es auch Laien möglich, komplexe Datenschutzmechanismen und Einstellungsmöglichkeiten sowie deren Auswirkungen nachzuvollziehen.

Im *Event-Log* können Nutzer jederzeit die datenbezogenen Vorgänge einsehen. Dies ermöglicht eine lückenlose Nachvollziehbarkeit der Erfassung, Verarbeitung und Weitergabe der eigenen Daten.

Zudem erläutert die Visualisierung der Datenflüsse transparent und einfach die Auswirkungen der datenbezogenen Einstellungen und Freigaben. Sie ermöglicht es den Nutzern, spielerisch die Gesamtheit der Effekte und des Zusammenspiels verschiedener Optionen zu erkunden.

Zusammenfassend lässt sich festhalten, dass Transparenz einen wesentlichen Bestandteil eines nutzerfreundlichen Datenschutzkonzepts ausmacht. Wie wir in der Evaluation (siehe Ergebnisbericht D6.1 [4]) zeigen konnten, stärkt sie das Vertrauen der Nutzer in die Anwendung und schafft die Voraussetzungen für informierte Datenschutzentscheidungen. Im Rahmen unseres Anwendungsfalls haben wir verschiedene Maßnahmen kombiniert, um die Transparenz zu erhöhen. Dazu zählen klare Einwilligungsprozesse, das Datenschutz-Profil als zentrale Informationsstelle sowie einfache Visualisierungen für Datenverfremdung und Datenflüsse.

5 Selbstbestimmungsgesichtspunkte des Interaktionskonzepts

Basierend auf hoher Transparenz und der damit angestrebten Informiertheit kann angenommen werden, dass Nutzer in der Lage sind, souverän zu entscheiden, wie ihre Daten verwendet werden dürfen. Das Recht, selbst darüber zu entscheiden, welche persönlichen Daten man offenlegt und wie diese verarbeitet werden dürfen, nennt man informationelle Selbstbestimmung [4]. In der Praxis umfasst dies alle Aspekte, die Nutzern eine Einflussnahme auf die Erfassung, Verarbeitung und Weitergabe ihrer Daten ermöglichen. Das Konzept der informationellen Selbstbestimmung wird in unserem Anwendungsfall durch mehrere Funktionalitäten adressiert.

Im Bereich *Vital- und Kontextdatenerfassung* können Nutzer einstellen, welche Daten überhaupt erhoben werden dürfen. Die *zeit- und ortsbasierte Datenerfassung* erlaubt es zudem, die Aufzeichnung auf bestimmte Zeiten (z.B. Arbeitszeiten) oder geographische Orte zu beschränken. Je nach vertraglicher Gestaltung der Nutzung des Wearables im Arbeitskontext haben Nutzer so die volle Kontrolle über die Erfassung genau jener Daten an genau jenen Orten und zu genau jenen Zeiten, die sie zur Messung freigegeben haben.

Bei den Einstellungen zu *Datenzugriffen* können Nutzer genau erkennen und festlegen, für welche Zwecke ihre Daten weitergegeben werden dürfen. So können sie beispielsweise bei entsprechendem Vertragsrahmen selbst entscheiden, ob sie am Gruppenbericht teilnehmen möchten oder ob sie ihre Daten für Forschungszwecke bestimmten Institutionen zur Verfügung stellen wollen.

Ein weiterer Aspekt ist die *Datenverfremdung*. Hier können Nutzer zum Schutz ihrer persönlichen Daten den Grad der Datenverfremdung abhängig von der gewünschten Analysequalität einstellen. Dies ermöglicht den Nutzern, sich gezielt für einen zusätzlichen Schutz ihrer Daten auch für den Fall zu entscheiden, dass die üblichen Zugriffsschutzmechanismen von einem Angreifer überwunden werden sollten.

Schließlich bietet die Funktion zur *Begrenzung der Speicherdauer* zusätzliche Kontrolle darüber, wie lange die erhobenen Daten überhaupt potenziellen Angriffen ausgesetzt sind, bis sie endgültig aus den Systemspeichern gelöscht werden. So kann sichergestellt werden, dass Daten nicht länger aufbewahrt werden, als es individuell als sinnvoll angesehen wird.

Zusammenfassend zeigt sich, dass die beschriebenen Funktionalitäten einzeln und im Gesamten die informationelle Selbstbestimmung stärken, indem Nutzern umfangreiche Einflussmöglichkeiten geboten werden. Diese Mechanismen können jedoch kontextabhängig durch den Arbeitgeber eingeschränkt sein, was die Selbstbestimmung einschränkt. So kann der Arbeitgeber zum Beispiel bestimmte Verarbeitungszwecke und Zugriffsmöglichkeiten verbindlich vorgeben, um die Zwecke des Messprogramms nicht zu beeinträchtigen. Da die Teilnahme an solch einem Programm stets auf Freiwilligkeit basieren muss, können solche Vorgaben gegebenenfalls zu einer geringeren Teilnahmebereitschaft bei den Mitarbeitern führen (siehe Ergebnisbericht D6.1 [4]).

Die Kombination aus hoher Transparenz und detaillierten Einstellungsmöglichkeiten ermöglicht es den Nutzern, fundierte und selbstbestimmte Entscheidungen hinsichtlich der Erhebung, Verarbeitung und Weitergabe ihrer Daten zu treffen. Die Möglichkeit der individuellen Anpassung der Datenerfassung und -nutzung an persönliche Präferenzen, beispielsweise hinsichtlich der zeit- und ortsabhängigen Erfassung, der Kontrolle über Datenzugriffe, der Datenverfremdung sowie der Begrenzung der Speicherdauer, gewährleistet eine effektive Kontrolle und somit den Schutz der Privatsphäre. Darüber hinaus schafft sie auch Vertrauen bei den Nutzern, sich einem Messprogramm unbesorgt anzuschließen.

6 Fazit

Die kontinuierliche Erfassung der Vitaldaten von Belegschaftsangehörigen am Arbeitsplatz berührt die Privatsphäre der Betroffenen in hohem Maße. Es ist daher nicht ganz einfach, Arbeitnehmer für die freiwillige Teilnahme an einem solchen Messprogramm zum Wohle ihrer Gesundheit und ihrer Sicherheit zu gewinnen und sie davon zu überzeugen, dass die Vorteile des Programms mögliche Vorbehalte gegen die Lösung aufwiegen. Dazu muss der Anbieter des Systems deutlich machen, dass er die Datenschutzbelange der Nutzer ernst nimmt und sehr genau bedacht hat. Dem Interaktionskonzept fällt hierbei eine Schlüsselrolle zu.

In Anwendungen ohne besondere Datenschutzanforderungen verfolgt das Interaktionskonzept vor allem folgende Ziele:

- *Verständlichkeit:* Die verfügbaren Systemfunktionen und ihre Wirkungsweise sollen sich dem Nutzer möglichst leicht erschließen. Der Funktionsumfang soll logisch gegliedert sein und die Beziehung zwischen dem zu lösenden Problem und den dazu erforderlichen Systemfunktionen soll möglichst intuitiv herstellbar sein.
- *Ergonomie:* Die Abfolge der Interaktionen soll sich möglichst natürlich aus dem jeweiligen Anliegen des Nutzers an das System ergeben und die notwendigen Schritte sollen in der jeweiligen Bediensituation leicht durchführbar sein.
- *Nutzungserfahrung:* Der Umgang mit dem System soll dem Nutzer eine positive Nutzungserfahrung bieten, die ihn animiert, das System auch weiterhin gerne in Anspruch zu nehmen.

Im Kontext der WearPrivate-Problemstellung – *Datenschutzfreundliche Vermessung und Auswertung persönlicher Daten mit Wearables zur Erhöhung der Arbeitssicherheit* – bleiben diese Anforderungen uneingeschränkt gültig: Gerade während der Arbeit darf eine Wearable-Lösung nicht zu viele körperliche und geistige Anstrengung erfordern und soll die Nutzer durch eine positive Nutzungserfahrung auch dauerhaft an das freiwillige Messprogramm binden. Aufgrund der besondere Datenschutzproblematik eines solchen Programms muss das Interaktionskonzept darüber hinaus aber weitere Anforderungen erfüllen:

- *Vertrauenswürdigkeit:* Die Interaktionen müssen dem Nutzer signalisieren, dass seine möglichen Vorbehalte bei der Gestaltung des Systems bereits erkannt wurden und dass die Entwickler entsprechende Mechanismen vorgesehen haben, um sich mit dessen berechtigten Interessen auseinanderzusetzen.
- *Offenheit:* Das System muss offensiv über die datenschutzrelevanten Aspekte aller Interaktionen informieren und den Nutzer bewusst einbeziehen, wenn Entscheidungen zu fällen sind, die Auswirkungen auf dessen Privatsphäre haben.
- *Kontrolle:* Das Interaktionskonzept muss dem Nutzer volle Kontrolle über seine Datenschutzbelange ermöglichen und ihm das Gefühl vermitteln, jederzeit »den Fahrersitz einzunehmen zu können«, wenn der Schutz seiner Privatsphäre betroffen ist.

Die vorliegenden Konzepte zur Gestaltung von Interaktionen zwischen Nutzern von Wearable-Lösungen am Arbeitsplatz und dem System versuchen, diesen Anforderungen gerecht zu werden und so einerseits einem besseren Arbeits- und Gesundheitsschutz zu dienen, ohne dabei den Anspruch der Belegschaft auf Privatheit zu opfern.

Dazu beschreibt der vorliegende Bericht eine Reihe von Ansätzen, um die *Transparenz* in Bezug auf die Erfassung, den Schutz und die Verwendung persönlicher Daten und die *informationelle Selbstbestimmung* entlang der gesamten Verarbeitungskette dieser Daten zu fördern.

Bei der Gestaltung der Interaktionskonzepte waren wir bemüht, die Nutzer nicht zu überfordern, denn nicht jeder Nutzer ist mit Informationstechnologie oder Datenschutzkonzepten vertraut und nicht jeder Arbeitsplatz bietet ein Umfeld, in dem sich umfangreiche Interaktionen mit einem Mobilgerät leicht durchführen lassen. Daher haben wir im Zweifelsfall einfachen, leicht zu verstehenden und mühelos zu bedienenden Interaktionsmechanismen den Vorzug gegeben vor funktional leistungsfähigeren, aber schwerer beherrschbaren Konzepten.

Quellenverzeichnis

[1] Jannis von Albedyll, Reinhard Schwarz: State-of-the-Art-Bericht zu Privacy-UIs. Ergebnisbericht D4.1, Projekt WearPrivate, Kaiserslautern, November 2022

[2] Bianca Steffes, Philipp Neuschwander, Marcus-Sebastian Schröder: Konzepte für Anonymisierung und Datennutzungskontrolle. Ergebnisbericht D3.2, Projekt WearPrivate, Bremen – Saarbrücken – Kaiserslautern, September 2022

[3] M. Rost, M. und K. Bock: Privacy by Design und die neuen Schutzziele. Datenschutz und Datensicherheit-DuD 35(1), pp. 30–35, 2011

[4] Bianca Steffes et al.: Evaluationsbericht. Ergebnisbericht D6.1, Projekt WearPrivate, Saarbrücken – Bremen – Kaiserslautern, November 2024

[5] Sonja Leischner und Angela Kolbe: Zum Einfluss des Grundrechts auf informationelle Selbstbestimmung auf die Bundesstatistik. WISTA-Wirtschaft und Statistik 76(3), pp. 17–30, 2024