WearPrivate
Kurzbericht zum Teilvorhaben (II. Eingehende Darstellung)

Zuwendungsempfänger: WearHealth GmbH

Förderkennzeichen: 16KIS1514

Vorhabenbezeichnung: WearPrivate

Teilvorhaben: Anonymisierte Wearables-basierte Analytics für HSE

Laufzeit des Vorhabens: 01.09.2021 – 30.11.2024

1. Einleitung

1.1. Problembeschreibung und Zielsetzung

In vielen Unternehmen werden arbeitsbedingte Belastungen nach wie vor überwiegend subjektiv, punktuell und erst im Nachhinein beurteilt. Präventive, alltagsnahe Verfahren fehlen häufig oder scheitern an der Balance zwischen Erkenntnisgewinn und Datenschutz. WearHealth adressiert dieses Spannungsfeld im Rahmen von WearPrivate mit einer DSGVO-konformen, datenschutzfreundlichen und betriebsnahen Lösung, die über Wearables erfasste Vital- und Kontextdaten (insbesondere Herzfrequenz/HR und Herzratenvariabilität/HRV) mit KI auswertet. Ziel ist es, Beschäftigten in Echtzeit verständliche, erklärbare Hinweise zur individuellen Belastung bereitzustellen und HSE-Verantwortlichen ausschließlich anonymisierte Team-Trends zur Prävention zur Verfügung zu stellen – ohne Leistungs- oder Verhaltensüberwachung einzelner Personen zu ermöglichen.

1.2. Abgleich mit der Vorhabenbeschreibung (TVB)

Die ursprüngliche Vorhabenbeschreibung sah einen modularen Cloud-Service mit mobiler App-Anbindung, eine Regel- und Richtlinienbasis zur Datennutzungskontrolle, Mechanismen zur Anonymisierung – optional ergänzt um Differential Privacy – sowie ein HSE-Dashboard vor. Die im Projekt realisierte Lösung entspricht diesen Zielen: Die Cloud-Architektur wurde entworfen und in Betrieb genommen, die Schnittstellen zur App wurden hergestellt, die KI-gestützte Belastungsanalytik auf Basis von HR und HRV integriert und die Transparenz- sowie Selbstbestimmungsfunktionen gemeinsam mit den Verbundpartnern präzisiert und in den Demonstrator überführt. Abweichungen betrafen im Wesentlichen die Reihenfolge der Integration – zunächst die Stabilisierung der Cloud-Dienste, anschließend die App-Integration – sowie die Schwerpunktsetzung einzelner Iterationen; inhaltlich blieb die Zielerreichung unverändert. Die Lösung folgt den im Verbund ausgearbeiteten Schutz- und Gestaltungsprinzipien und ist DSGVO-konform ausgelegt.

1.3. Internationaler Stand der Wissenschaft und Technik

International ist die arbeitsbezogene Nutzung von Wearables durch drei Linien geprägt: (a) biomedizinische Verfahren zur Ableitung mentaler und physischer Beanspruchung aus HR/HRV-Merkmalen in Zeit- und Frequenzdomäne; (b) architektonische und regulatorische Ansätze zu Privacy-by-Design, Datensparsamkeit und Rollen-/Zwecktrennung; sowie (c) Verfahren des statistischen Datenschutzes wie Differential Privacy, die den Nutzwert individueller Rückmeldungen mit einem überprüfbaren Schutzbudget (ε) in Einklang bringen. Für die ergonomische und arbeitswissenschaftliche Einordnung werden international anerkannte Normen herangezogen, u. a. ISO 10075-1/-2/-3 (psychische Arbeitsbelastung), ISO 8996 (metabolische Wärmeproduktion/Energieumsatz) und ISO 6385 (ergonomische Grundsätze). Die vorliegende Lösung ordnet sich in diesen Stand ein, überführt die Konzepte in eine betriebstaugliche Cloud-/App-Architektur und ergänzt sie um nutzerzentrierte Transparenz- und

Steuerungsmechanismen (Privacy-Dashboard, Ereignislog, Visualisierung von Datenflüssen), sodass internationale Leitlinien praktisch anwendbar werden.

2. Arbeitspakete gemäß TVB, Plan und Umsetzung

Im Folgenden werden die Arbeitspakete mit ihren originalen Bezeichnungen aus dem TVB dargestellt und jeweils dem tatsächlichen Vorgehen gegenübergestellt. Der Text legt dar, was geplant war, was umgesetzt wurde, welche Anpassungen sich als notwendig erwiesen und welche Ergebnisse jeweils erzielt wurden. Die Bezugnahmen auf Meilensteine orientieren sich an den im TVB vorgesehenen Sprints und Projektmonaten (MS1 bis MS6)

AP1: Anforderungen an den Datenschutz bei Wearables

Planungsseitig sollte dieses Arbeitspaket die technischen und organisatorischen Anforderungen an Datenschutz, Sicherheit und informationelle Selbstbestimmung methodisch erheben und in verwertbare Spezifikationen überführen. Dazu gehörten die Definition der Rollen und Rechte, die Festlegung von Einwilligungs- und Widerrufsprozessen, Regelungen zur Speicherbegrenzung sowie die Festlegung von Datenflüssen für Rohdaten, abgeleitete Metriken und aggregierte Ausgaben. In der Umsetzung führte WearHealth gemeinsam mit den Partnern strukturierte Interviews, Workshops und Dokumentenanalysen durch. Aus diesen Arbeiten ergab sich eine belastbare Grundlage für die Cloud-Architektur, die Datennutzungskontrolle und die App-seitige Nutzerführung. Besonderes Gewicht lag auf der anonymen Registrierung mittels Teilnahme- bzw. Gruppentoken, auf der Trennung von Identitäts- und Messdaten sowie auf einer klaren Zweckbindung jeder Datenverarbeitung. Bereits in frühen Iterationen wurden Visualisierungen der Datenflüsse und ein Ereignisprotokoll als klickbare Prototypen erprobt, um Verständlichkeit und Akzeptanz abzusichern und so den Übergang in die technischen Pakete zu beschleunigen. Das Arbeitspaket erreichte seine Ziele termingerecht im Umfeld von MS1 und bildete die Grundlage für Architektur, rechtlichen Rahmen und technische Umsetzung.

AP2: Datenschutzrechtlicher und ethischer Rahmen

Nach TVB sollte AP2 die rechtlichen und ethischen Leitplanken so aufbereiten, dass sie direkt in Architektur- und Produktentscheidungen überführt werden konnten. Unter Federführung der Universität des Saarlandes wurden die einschlägigen Regelwerke und Gesetze sowie deren praktische Implikationen analysiert. Daraus resultierten klare Anforderungen an Transparenz, Betroffenenrechte, Rechenschaftspflichten und technische wie organisatorische Maßnahmen. Für WearHealth bedeutete dies, die App mit einem Privacy-Dashboard auszustatten, leicht verständliche Erläuterungstexte zu pflegen, ein maschinenlesbares Ereignislog bereitzustellen und Widerrufs- sowie Löschfunktionen ohne Hürde zugänglich zu machen. Für die Cloud wurden Datenminimierung und zweckgebundene Verarbeitungspfad-Trennung verbindlich festgeschrieben; Protokollierung und Mandantentrennung wurden so umgesetzt, dass Auditierbarkeit und Nachvollziehbarkeit jederzeit gegeben sind. Die Ergebnisse aus AP2 flossen in API-Design, Architekturentscheidungen und die Ausgestaltung der Interaktion ein und wurden mit den Erkenntnissen aus der Evaluation rückgekoppelt. Damit erfüllte AP2 den Plan und konkretisierte die jurischen und ethischen Anforderungen für die technische Umsetzung.

AP3: Technische Umsetzung des Datenschutzes

Dieses Arbeitspaket sah im TVB die Auswahl und Härtung der Cloud-Plattform, den Entwurf der IT-Architektur mit Kommunikationsprotokollen, Schnittstellen, Datenbanken, Analysediensten, Verschlüsselungs- und Anonymisierungsmechanismen sowie die Etablierung eines sicheren Entwicklungs- und Betriebsverfahrens vor. WearHealth validierte dafür einen Zielaufbau auf AWS und setzte die Trennung der Datenpfade nach Zweck strikt um: Rohdaten, abgeleitete Metriken und aggregierte Ausgaben wurden in getrennten Bereichen verarbeitet und gespeichert, sodass die Rückführung von Aggregaten auf Einzelpersonen ausgeschlossen blieb. Die Kommunikation zwischen App und Cloud wurde Ende-zu-Ende verschlüsselt, die Zugriffskontrolle tokenbasiert realisiert und im

API-Gateway durch Ratenbegrenzung sowie Protokollhärtung ergänzt. Die Datennutzungskontrolle wurde als Policy-basierter Querschnitt in die Pipeline integriert; nach MYDATA-Prinzipien mit einem zentralen Policy Decision Point (PDP), Policy Enforcement Points (PEP) an Ingestion, Verarbeitung und Ausgabe sowie einem Policy Information Point (PIP) für kontextabhängige Entscheidungen; auf Ebene der individuellen Rückmeldungen wurde eine Option zur Differential-Privacy-geschützten Verarbeitung vorgesehen, ohne die Nutzbarkeit der Hinweise unvertretbar zu beeinträchtigen. In Abweichung vom ursprünglichen Ablauf wurden zunächst die Kern-Cloud-Dienste stabilisiert und erst danach die App in die produktionsnahen Schnittstellen integriert. Diese Reihenfolge reduzierte Integrationsrisiken, erlaubte eine frühzeitige Last- und Stabilitätsprüfung und beschleunigte die spätere Gesamtzusammenführung. Die im TVB vorgesehenen Zwischenstände – Definition der Technologien, Implementierungsbeginn in Testumgebungen, API-Dokumentation, Performance- und Stabilitätsprüfungen – wurden erreicht und dokumentiert.

AP4: Transparenz und Selbstbestimmung für Endverbraucher

AP4 sollte die im Verbund entwickelten Konzepte zu Transparenz und Selbstbestimmung in technische Funktionen überführen und so gestalten, dass sie im Alltag verstanden, bedient und akzeptiert werden. Aus den juristischen und organisatorischen Vorgaben wurden für die App konkrete, niedrigschwellige Funktionen abgeleitet. Das Privacy-Dashboard ermöglicht den Nutzenden die feingranulare Steuerung der Datennutzung; die Aufzeichnung lässt sich zeit- und ortsabhängig konfigurieren; ein Ereignisprotokoll zeigt wesentliche Vorgänge in nachvollziehbarer Form; Widerruf und Löschung sind unmittelbar erreichbar. Auf Cloud-Seite wurden die korrespondierenden Kontrollpunkte so implementiert, dass Nutzereinstellungen deterministisch und auditierbar wirken und in allen Teilprozessen respektiert werden. Die Funktionsentwürfe wurden in wiederkehrenden Gesprächen und Tests mit Nutzenden geschärft; Formulierungen, Ikonografie und Reihenfolge der Schritte wurden so angepasst, dass Missverständnisse minimiert und die Freiwilligkeit gestärkt wurden. Die im TVB vorgesehenen Einbindungen in die analytischen Sichten des Dashboards wurden umgesetzt, indem Präferenzen und Freigaben auch in aggregierten Ansichten reflektiert, aber nie individualisiert wurden.

AP5: Umsetzbarkeit und Demonstratoren

Gemäß TVB sollte WearHealth die Umsetzbarkeit der anonymisierten Analytik belegen, einen praxistauglichen Analytik-Service in der Cloud bereitstellen und ein Web-Dashboard entwickeln, das die relevanten Team-Trends visualisiert. In der Umsetzung wurden zunächst die Anforderungen potenzieller Anwendender systematisch erhoben und zu einem nutzbaren KPI-Set verdichtet. Auf dieser Grundlage entstand ein Cloud-basierter Analytikdienst, der an die Wearable-Datenanbindung der App gekoppelt ist, die Daten regel- und zweckgebunden verarbeitet und daraus Trendverläufe sowie Verteilungen ableitet. Das Dashboard stellt diese Ergebnisse in einer für HSE-Verantwortliche verständlichen Form dar und achtet durchgehend auf Mindestgruppengrößen und Aggregationsgrenzen, um Re-Identifikationen sicher auszuschließen. Während der Entwicklung wurden die Anzahl und Komplexität der Kennzahlen bewusst begrenzt, um Verständlichkeit und Präventionstauglichkeit zu erhöhen. Export- und Berichtsfunktionen wurden so implementiert, dass sie die betriebliche Praxis unterstützen, ohne personenbezogene Detailansichten zu eröffnen. Der Demonstrator diente im weiteren Verlauf als Referenz für die Evaluation und als Kommunikationsmittel in Richtung Stakeholder.

AP6: Evaluation

Das TVB sah die Validierung von Nutzbarkeit, Datenschutzwirkung und technischem Mehrwert vor, ergänzt um Sicherheits- und Robustheitsprüfungen. In der Durchführung wurden technische Tests der Kommunikationsprotokolle, Latenzen und Fehlerszenarien mit nutzerzentrierten Untersuchungen kombiniert. Eingangsbefragungen erfassten Vorerfahrungen mit Wearables, Einstellungen zur Datenteilung und Vorbehalte gegenüber arbeitsbezogenen Messprogrammen. Auf dieser Basis wurden Interaktionsmuster – Privacy-Dashboard, Ereignislog, Visualisierung von Datenflüssen,

Speicherbegrenzung – iterativ erprobt. Die App-seitige Hinweislogik wurde im Hinblick auf Verständlichkeit und Erklärbarkeit verfeinert, insbesondere bei mentalen Belastungen. Parallel wurden Cloud-Prozesse, API-Aufrufe und Fehlerpfade getestet und optimiert. Ein Schwerpunkt lag auf der Sensitivität der KI-Analytik gegenüber Differential-Privacy-Rauschen: Stärkere Rauschanteile können HRV-basierte Merkmale erhöhen und damit die Belastung unterschätzen. Dies wurde durch DP-bewusstes Training, Kalibriermaßnamen und konservative Schwellen adressiert, sodass die Schutzwirkung erhalten bleibt und zugleich ein praxistauglicher Nutzwert erzielt wird. Abschließend zeigte der integrierte Demonstrator, dass die Lösung technisch stabil arbeitet, inhaltlich nachvollziehbare Hinweise liefert und durch die gestalteten Transparenz- und Kontrollfunktionen auf Akzeptanz stößt.

AP7: Wissenstransfer

Der Wissenstransfer umfasste die Aufbereitung der Ergebnisse für Fachpublika und potenzielle Anwender sowie den Austausch im Konsortium und mit externen Interessenten. WearHealth trug mit Präsentationen und Demonstrationen zu Architektur, Datennutzungskontrolle, DP-Sensitivität und UX-Design bei. Rückmeldungen aus Praxis und Forschung wurden gesammelt, ausgewertet und in die Roadmap überführt. Diese Aktivitäten dienten gleichermaßen dem fachlichen Diskurs und der Vorbereitung der Verwertung.

AP8: Projektmanagement

Die Koordination des Verbunds und der eigenen Entwicklungsaktivitäten folgte einem agilen Vorgehen mit abgestimmten Meilensteinen, Backlogs und regelmäßigen Besprechungen. Für WearHealth bedeutete dies, Abhängigkeiten zwischen Cloud-Diensten, App-Integration, Analytik und Dashboard transparent zu steuern und Risiken frühzeitig zu adressieren. Der während der Laufzeit erfolgte Wechsel eines App-Partners wurde ohne inhaltliche Zielabweichung aufgefangen; Zeitpläne wurden angepasst, ohne den vorgesehenen Funktionsumfang zu schmälern. Das Paket erfüllte die Planvorgaben und trug dazu bei, dass MS1 bis MS6 erreicht wurden.

3. Technische Umsetzung im Verbundkontext

Die Lösung trennt Identitäts- und Messdaten vollständig, setzt anonyme Registrierungstokens ein und hält die Rollen Analyse und Distribution strikt auseinander. Die Cloud behandelt Rohdaten, abgeleitete Metriken und aggregierte Ausgaben in eigenen Verarbeitungspfaden und stellt sicher, dass individuelle Hinweise ausschließlich an die jeweilige App zurückfließen.

Die Datennutzungskontrolle wirkt als Querschnittsmechanismus durch die gesamte Pipeline: Richtlinien bestimmen, welche Verarbeitungen in welchem Umfang zulässig sind; die App spiegelt diese Entscheidungen in bedienbaren Schaltern und verständlichen Erläuterungen. Für das individuelle Feedback kommen Modelle zum Einsatz, die Herzfrequenz und Herzratenvariabilität in Zeit- und Frequenzdomäne mit Kontextinformationen verknüpfen und daraus einen kontinuierlichen

Belastungsindex sowie die Klassen Mental, Physical, Mixed und Recovery ableiten. Die Optionalität von Differential Privacy wurde so ausgelegt, dass das Schutz-Nutzen-Verhältnis gewahrt bleibt; verbleibende Effekte werden durch DP-bewusstes Training, Kalibrierung und textliche Einordnung abgefedert. Architektur und Betrieb folgen einem sicheren Lebenszyklus; Verschlüsselung im Transit und in Ruhe, Secret-Management, Monitoring und Protokollierung sind etabliert, auditierbar und stärken die DSGVO-Konformität der Gesamtlösung.

4. Evaluation und Nutzerstudien

Die Evaluation fokussierte sechs Schwerpunkte: Datenschutzwirkung, Integration der mobilen App, MYDATA-gestützte Policy-Durchsetzung, anonymisierte Berichte, Stabilität des Cloud-Services und Wirksamkeit der Privatsphäre-Einstellungen.

Im Hinblick auf die Datenschutzwirkung wurde überprüft, ob die gestalteten Transparenz- und Steuerungsmechanismen ihre intendierte Wirkung entfalten. Prototypische Visualisierungen der Datenflüsse, ein Ereignisprotokoll und ein konsistentes Privacy-Dashboard erwiesen sich als geeignet, Freigaben verständlich zu machen und die Steuerbarkeit für Nutzende zu erhöhen. Die Eingangsbefragung bestätigte, dass Freiwilligkeit und klare Grenzen zwischen individueller Rückmeldung und aggregierten Teamberichten zentrale Akzeptanztreiber sind; entsprechend wurden Mindestgruppengrößen, Aggregationsgrenzen und Speicherbegrenzungen technisch verankert und nachvollziehbar kommuniziert.

Die Integration der mobilen App in die Cloud wurde Ende-zu-Ende evaluiert. Der Kopplungs- und Datenfluss – Pairing, Einwilligung, verschlüsselte Übertragung, temporäre Zwischenspeicherung und Wiederaufnahme nach Verbindungsabbrüchen – zeigte sich stabil. Latenz- und Fehlerszenarien wurden systematisch getestet; die Schnittstellen liefern die für Echtzeit-Hinweise erforderlichen Laufzeiten. Gleichzeitig wurde die Nutzerführung in der App, insbesondere die Abfolge von Onboarding, Gerätepaarung, Freigabenauswahl und Widerruf, anhand beobachteter Hürden sprachlich und visuell verfeinert.

Die MYDATA-Integration wurde in der Praxis bewertet. In Testszenarien mit variierenden Freigaben, Zeitfenstern und Zweckbindungen entschieden Policies deterministisch und reproduzierbar; die Durchsetzung erfolgte an PEPs entlang der Pipeline. Die App spiegelte den jeweils wirksamen Policy-Zustand, sodass Nutzende die Konsequenzen ihrer Auswahl unmittelbar sehen konnten. Audit-Trails ermöglichten die Nachvollziehbarkeit und untermauerten die Rechenschaftsfähigkeit der Lösung.

Die anonymisierten Berichte für HSE wurden daraufhin geprüft, ob Aggregationen und Mindestgruppengrößen eine Rückführung auf Einzelpersonen verhindern – auch in Randfällen mit geringer Datenmenge. Die Darstellung von Trends und Verteilungen unterstützt präventive Entscheidungen, ohne personenbezogene Leistungskennzahlen abzuleiten. Rückmeldungen aus den Evaluationen bekräftigten, dass diese Form der Berichterstattung als fair, zweckmäßig und DSGVO-konform wahrgenommen wird.

Zur Stabilität des Cloud-Services wurden Verfügbarkeit, Fehlertoleranz, Wiederanlaufverhalten nach Netzunterbrüchen sowie Ende-zu-Ende-Latenzen in Last- und Fehlerszenarien geprüft. Die Dienste hielten die Grenzwerte für Echtzeit-Hinweise ein und starteten nach Störungen kontrolliert neu.
Die Wirksamkeit der Privatsphäre-Einstellungen wurde gesondert betrachtet. Änderungen an Einwilligungen und Zweckbindungen wirkten deterministisch entlang der Pipeline, wurden an den PEPs strikt durchgesetzt und waren in der App unmittelbar sichtbar; das Ereignisprotokoll zeichnete relevante Aktionen nachvollziehbar auf.
Begleitend wurden die KI-basierten Workload-Algorithmen iterativ verbessert. Neben robusterem Artefakt-Handling und kontextsensitiveren Merkmalen spielte die DP-Sensitivity eine zentrale Rolle: Rauschung kann HRV-Metriken erhöhen und damit Belastung unterschätzen. Durch DP-aware Training, Kalibrierung und angepasste Mindestfenster wurden diese Effekte reduziert, ohne den Schutzgedanken aufzugeben. Insgesamt bestätigte der integrierte Demonstrator, dass die Lösung technisch stabil arbeitet, inhaltlich nachvollziehbare und datenschutzgerechte Hinweise liefert und durch die gestalteten Transparenz- und Kontrollfunktionen auf Akzeptanz stößt.

5. Notwendigkeit und Angemessenheit der geleisteten Arbeiten

Die Arbeiten waren notwendig, weil eine betriebliche Nutzung von Wearables ohne Datenschutz-by-Design und nachvollziehbare Datennutzungskontrolle weder rechtlich noch sozial tragfähig wäre. Die Angemessenheit ergibt sich aus der gewählten Tiefe: Eine sichere, auditierbare Cloud-Architektur, robuste Kommunikationsprotokolle, erklärbare Analytik und benutzbare Transparenzfunktionen sind Voraussetzungen dafür, dass Beschäftigte freiwillig teilnehmen und HSE-Verantwortliche präventiv handeln. Die iterative Validierung mit realen Nutzergruppen und die explizite Trennung zwischen individuellem Feedback und aggregierten HSE-Trends adressieren Akzeptanz- und Missbrauchsrisiken. Die Orientierung an Normen – insbesondere an der ISO-10075-Reihe, ISO 8996 und ISO 6385 – verankert die Lösung zusätzlich im Stand der Technik und erleichtert die Übertragbarkeit in verschiedene Branchen. Die Lösung ist in allen Schritten auf DSGVO-Konformität ausgelegt.

6. Notwendigkeit und Angemessenheit der geleisteten Arbeiten

Kurzfristig werden der Cloud-Service mit den HR/HRV-basierten Modulen und das HSE-Dashboard in das WearHealth-Portfolio überführt. Für Anwender entsteht ein unmittelbarer Nutzen in Form früher erkannter Überlastungen, besserer präventiver Entscheidungen und nachvollziehbarer, anonymisierter Entscheidungsgrundlagen für das Betriebliche Gesundheitsmanagement. Mittelfristig ist die Ausweitung auf zusätzliche Wearables geplant, flankiert von einer breiteren, DP-aware trainierten Modellbasis und konfigurierbaren Belastungsprofilen je Branche und Schichtmodell. Die Mandantenfähigkeit und die vorgesehenen Exporte sowie Integrationen in bestehende EHS- und BGM-Systeme schaffen die Grundlage für eine skalierbare Verwertung. Vertriebsseitig ist ein DSGVO-konformes SaaS-Modell vorgesehen, das durch Einführungs-, Schulungs- und Datenschutz-Workshops flankiert wird.

7. Bekannt gewordenen Fortschritts auf diesem Gebiet bei anderen Stellen

Im Verlauf dieses Projekts erhielt WearHealth keine Informationen über Fortschritte in diesem Bereich von anderen Stellen.

8. Bekannt gewordenen

Im Verlauf dieses Projekts erhielt WearHealth keine Informationen über Fortschritte in diesem Bereich von anderen Stellen.

Projektmanagement

Die Koordination des Verbunds und der eigenen Entwicklungsaktivitäten folgte einem agilen Vorgehen mit abgestimmten Meilensteinen, Backlogs und regelmäßigen Besprechungen. Für WearHealth bedeutete

ng von Nutzbarkeit, Datenschutzwirkung und technischem Mehrwert vor, ergänzt um Sicherheits WearHealth die Umsetzbarkeit der anonymisierten Analytik belegen, einen praxistauglichen

a)
b) mit API und App-Anbindung. Die Plattform erfasst Wearable-Daten über die mobile App, verarbeitet sie in nahezu Echtzeit und stellt – ausschließlich nach Einwilligung – anonymisierte Analysen und Trends bereit. Die Architektur und Dienste wurden auf AWS entworfen, abgesichert und in Betrieb genommen.
c) Datenschutz „by design“ mit Datennutzungskontrolle und klarer Transparenz. Die Verbundkonzepte zu Datennutzungskontrolle (Policy-basierte Steuerung der Verarbeitung/Nutzung/Weitergabe) bilden das Rückgrat der Lösung. Auf Nutzerseite wurden Privacy-Einstellungen und Nachvollziehbarkeit (z. B. Ereignisprotokoll, Visualisierung von Datenflüssen, Speicherbegrenzung) realisiert, damit Beschäftigte die Datennutzung verstehen und steuern können.
d) Differential Privacy für individuelles Feedback – mit geprüfter Sensitivität. Für vitale und kontextuelle Daten wurden DP-Mechanismen konzipiert und im Verbund evaluiert. Die Sensitivitätsanalyse zeigt, wie sich unterschiedliche ε-Werte auf Klassifikations-/Erkennungsqualität auswirken – eine Grundlage, um Schutz und Nützlichkeit zielgruppengerecht auszubalancieren.
e) Dashboard für HSE-Manager mit anonymisierten Team-Einblicken. Das Web-Dashboard (Node.js) stellt aggregierte Belastungsindikatoren und Trendverläufe teambezogen dar. Gruppenberichte unterstützen das betriebliche Gesundheitsmanagement dabei, Überlastungen zu erkennen und präventive Maßnahmen abzuleiten, ohne individualisierbare Leistungsdaten offenzulegen.
f) Integration, Tests und Optimierungen. Die Cloud-API wurde für die App geöffnet, Datenübertragung und -verarbeitung getestet und Sicherheitsmechanismen (u. a. Verschlüsselung, Protokollhärtung) ergänzt. In der Evaluation wurden Kommunikationsprotokolle, Cloud-Prozesse und die App-Interaktion überprüft und iterativ verbessert; Nutzergruppen und Validierungsszenarien wurden gemeinsam mit den Partnern festgelegt.
g) KI-getriebene Workload-Algorithmen (HR/HRV). Die Analytik wurde dahingehend erweitert, dass aus Herzfrequenz (HR) und Herzratenvariabilität (HRV) des über die App verbundenen Wearables ein Belastungsindex sowie Belastungsklassen (z. B. MENTAL, PHYSICAL, MIXED, RECOVERY) in nahezu Echtzeit abgeleitet und als Hinweise in der App bzw. als Trends im Dashboard bereitgestellt werden. Bei aktivierter Differential Privacy zeigt sich eine systematische Unterschätzung der Belastung (durch tendenziell erhöhte HRV-Werte); dies kann durch DP-bewusstes Training der KI kompensiert werden.

9. Zusammenarbeit mit anderen Forschungseinrichtungen

Das Teilvorhaben profitierte von enger, arbeitsteiliger Kooperation: Fraunhofer IESE verantwortete u. a. Sicherheitsarchitektur, bedrohungsgeleitete Anforderungserhebung und die Systematik der Datennutzungskontrolle; Universität des Saarlandes (UdS) entwickelte Anonymisierungs-/Aggregationskonzepte und bewertete rechtlich-ethische Aspekte; neusta mobile solutions (NMS)

verantwortete die mobile App und trug zur Gesamtintegration des Demonstrators bei. Die gemeinsame Ausgestaltung von Transparenz-/Selbstbestimmungskonzepten, die Jahrestreffen 2022 (Bremen) und 2023 (Kaiserslautern) sowie fortlaufende Abstimmungen stellten Konsistenz von Architektur, Datenschutz und Usability sicher.

10. Kurzfazit

Das WearHealth-Teilvorhaben liefert einen pragmatisch einsetzbaren, abgesicherten Cloud-Service mit App-Schnittstelle und anonymisiertem HSE-Dashboard, verankert in Datennutzungskontrolle und Differential Privacy. Damit ist eine allgemein verständliche, datenschutzfreundliche Nutzung von Wearables im Arbeitskontext möglich mit unmittelbarem Mehrwert für Mitarbeitende (Feedback/Empfehlungen) und Arbeitgeber (präventive Team-Einblicke), ohne Leistungsüberwachung zu ermöglichen.