WearPrivate

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

Ergebnisbericht D3.1

IT-Sicherheitsarchitektur und Datenschutzkonzept

Version	1.0
Datum	25.11.2024
Verfasser	Marcus-Sebastian Schröder (neusta) Reinhard Schwarz (IESE) Philipp Neuschwander (IESE) Bianca Steffes (UdS) Ajla Hajric (UdS) Esteban Bayro-Kaiser (WearHealth)

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

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

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Ansprechperson

Marcus-Sebastian Schröder
neusta mobile solutions GmbH
Konsul-Smidt-Str. 24
28217 Bremen

E-Mail: m.schroeder@neusta.de

Inhaltsverzeichnis

Liste der Abkürzungen

AES	Advanced Encryption Standard
AG	Arbeitgeber
AN	Arbeitnehmer
AWS	Amazon Web Services
DSGVO	Datenschutzgrundverordnung (EU-Verordnung 2016/679)
ID	(zufällige) Identitätsnummer des Anwenders
GID	Gruppen-Identitätsnummer, welcher der AN zugeordnet ist
GPS	Global Positioning System
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PMP	Policy Management Point
PXP	Policy Execution Point
SDK	Software Development Kit
SOC	Service Organization Control (Cybersecurity Compliance Framework, American Institute of Certified Public Accountants)
SQL	Structured Query Language
TLS	Transport Layer Security

1 Einleitung

Dieser Bericht beschreibt eine Sicherheits-Gesamtarchitektur für einen Wearable-basierten Arbeits- und Gesundheitsschutz. Der Schwerpunkt des Architekturkonzeptes liegt auf der Erfüllung der Datenschutz- und Selbstbestimmungsanforderungen, die in den voranstehenden Arbeitspaketen ermittelt wurden. Der einfacheren Lesbarkeit halber wird in diesem Dokument daher zunächst ein Überblick über die relevanten technischen Anforderungen gegeben. Im Anschluss daran werden die daraus resultierenden Entscheidungen hinsichtlich der Architekturgestaltung dargelegt.

Der Aspekt der Nutzerinteraktion und deren Beitrag zu Transparenz und Selbstbestimmung sind in diesem Dokument nicht betrachtet. Hierfür sei auf den Ergebnisbericht D4.2 „Interaktionskonzept“ verwiesen.

Hinweis: *Die in diesem Dokument hergeleiteten Anforderungen sind mit Verweisen auf Bedrohungen (in der Form »T_...«) versehen, auf die sich die Anforderung jeweils bezieht, sowie mit Verweisen auf die resultierenden formalen Requirements (in der Form »R_...«), in denen sich die Anforderung letztendlich widerspiegelt. Die T- und R-Verweise sind in der Anforderungstabelle des Ergebnisberichts D1.1 (Anforderungsbericht) dokumentiert [18].*

2 Technisch-Organisatorische Maßnahmen für die App

Dieser Abschnitt dokumentiert die verschiedenen Anforderungen an die App, speziell solche, aus denen technisch-organisatorische Maßnahmen erwachsen.

2.1 Integrität und Vertraulichkeit

2.1.1 Verschlüsselte Speicherung

Zur Persistierung von Daten in iPhone-Anwendungen stellt Apple das CoreData-Framework als Teil des eigenen Software Development Kits (SDK) zur Verfügung. CoreData erlaubt die Definition eines Datenmodells, das vom Framework während der Laufzeit für den Entwickler transparent in und aus einem Store gelesen und geschrieben werden kann. Dieser Store kann entweder rein *in Memory* sein oder auf dem Dateisystem als SQL, XML oder binär repräsentiert vorliegen. In der Praxis üblich ist die Repräsentation als SQL-Datei, da diese im Vergleich zu XML deutlich höhere Geschwindigkeit bietet und im Vergleich zur Binärrepräsentation erlaubt, nur Teile des Objektgraphen im Speicher zu halten[1].

Um die SQL-Datei mit den persistierten Objekten zu schützen, gibt es Mechanismen auf mehreren Ebenen. Das Betriebssystem selbst bietet bei der Erstellung des Stores an, mittels der Option *NSPersistentStoreFileProtectionKey* eine der Optionen aus *FileProtectionType*[2] zu setzen. Die Option *complete* führt dabei zu einer Verschlüsselung der Datei, solange das Gerät startet oder gesperrt ist. Sollte ein Zugriff auch nötig sein, falls das Gerät gesperrt ist (z. B. falls ein Zugriff erfolgen soll, während

[1] https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/CoreData/PersistentStoreFeatures.html

[2] https://developer.apple.com/documentation/foundation/fileprotectiontype

die Anwendung im Hintergrund Daten hoch- oder herunterlädt), so sorgt die Option *completeUnlessOpen* für eine Verschlüsselung, solange die Datei nicht geöffnet ist.

Während dieser Mechanismus vor einem Auslesen etwa eines entwendeten Geräts schützt, ist ein Zugriff während der aktiven Nutzung des Geräts hiermit dennoch möglich. Dieses wiederum würde normalerweise durch die Sandboxing-Mechanismen des Betriebssystems verhindert werden, doch auf Geräten mit Jailbreak (siehe Abschnitt 2.1.3) ist diese Sicherheit nicht gegeben.

In der Vergangenheit wurde diesem Problem teilweise mit dem Einsatz des Frameworks EncryptedCoreData[3] begegnet, das einen verschlüsselnden SQL-Store bereitstellt. Aus heutiger Sicht ist der Einsatz dieses Frameworks nicht länger empfehlenswert, da das letzte Update zum gegenwärtigen Zeitpunkt sechs Jahre zurückliegt; aktuelle Erkenntnisse über Best Practices und Exploits in kryptographischen Verfahren sind also nicht in das Projekt eingeflossen. Weiterhin besteht das Risiko, dass künftige SDK- oder Betriebssystemupdates zu Inkompatibilitäten führen können, die ohne einen Maintainer im Zweifelsfall vom Nutzer des Frameworks selbst behoben werden müssten.

Stattdessen ist die Prüfung des Geräts auf einen aktiven Jailbreak und gegebenenfalls die Unterbindung der Nutzung der Anwendung ratsam, um diesen Angriffsvektor auszuhebeln. Für Details hierzu sei auf den entsprechenden Abschnitt verwiesen.

Zur Vorbeugung gegen Datenlecks (T_AN15) aufgrund nichtautorisierter Zugriffe auf das Smartphone ergibt sich somit folgende Anforderung (R_AN32b):

Anforderung 1 *Beim Persistieren von Dateien ist ein FileProtectionType zu setzen, der so hoch wie für die vorgesehene Nutzung noch technisch möglich ist.*

2.1.2 Auditing von Frameworks

Der Einsatz von Frameworks ist eine beliebte Maßnahme zur Senkung der Entwicklungszeit einer Anwendung. Grundsätzlich erscheint es naheliegend, nicht für jede Anwendung das Rad neu zu erfinden, sondern bestehende Arbeiten zu nutzen, die unter einer hinreichend liberalen Lizenz für die Allgemeinheit bereitgestellt wurden.

Gleichzeitig bedeutet das Einbinden eines fremden Frameworks aber auch: Auf jedem Gerät, auf dem unsere Anwendung später installiert wird, wird Code ausgeführt, der nicht von uns geschrieben wurde. Dies bedeutet Kontrollverlust auf der Entwicklerseite, der potenziell dramatische Ausmaße haben kann (T_E1). Teilweise mitigiert wird dies bei Open Source Frameworks, die bei hinreichend großer Popularität genügend Kompetenzen und Motivation in ihrer Community haben können, um diese auf Korrektheit zu überprüfen.

Grundsätzlich sollte aber bei der Entwicklung der WearPrivate-App an erster Stelle das Ziel stehen, möglichst wenige externe Abhängigkeiten einzubinden (R_E1). Alle Abhängigkeiten, die eingebunden werden, müssen als Quellcode vorliegen (R_E3), der dann als Paket in das WearPrivate-Projekt integriert wird. Dadurch wird der Quellcode erst beim Erzeugen des App-Binaries übersetzt und kann vorher auf unerwünschtes Verhalten, zum Beispiel Kontaktaufnahme mit Servern, die nicht unter unserer Kontrolle stehen, überprüft werden (R_E2). Es ist aber auch in diesem Fall darauf zu achten, dass nicht innerhalb des Frameworks noch eine statische Bibliothek mit vorkompiliertem Code genutzt wird – dies ist zum Beispiel bei manchen Projekten so, die aus lizenztechnischen Gründen keinen

[3] https://github.com/project-imas/encrypted-core-data

Quellcode weitervertreiben dürfen. Auch in diesem Fall muss dann die Nutzung des problematischen Frameworks unterbleiben.

Anforderung 2 *Der Einsatz externer Frameworks muss so gering wie möglich gehalten werden. Eingesetzte Frameworks müssen auf unerwünschtes Verhalten überprüft werden.*

2.1.3 Prüfen auf Jailbreaks

Ein Jailbreak ist ein Exploit, der durch eine Rechteausweitung das Ausführen von Software erlaubt, die normalerweise durch die Sicherheitsmechanismen des Betriebssystems an der Ausführung gehindert werden würde. Im konkreten Bezug auf das iOS-Betriebssystem, für das wir den Demonstrator entwickeln, bedeutet dies, dass Software ausgeführt werden kann, die:

- nicht über den AppStore bezogen wurde und daher nicht der normalen Prüfung von Apple auf bösartiges Verhalten unterzogen wurde und die
- mehr als die für die Allgemeinheit freigegebenen Programmierschnittstellen verwendet. Hierdurch wird insbesondere der Zugriff auf Ressourcen außerhalb der Sandbox möglich, auf die normale Anwendungen beschränkt sind.

Auf einem System mit Jailbreak ist also denkbar, dass fremde Anwendungen Lesezugriff auf den Sandbox-Container der WearPrivate-App haben und die dort abgelegten Daten auslesen und in irgendeiner Form weiterverarbeiten (T_E2).

In einem Blog-Artikel „iOS Jailbreak Detection in 2023“ [11] gibt Eidinger einen Überblick über den zum Zeitpunkt der Erstellung dieses Dokuments aktuellen Stand an Möglichkeiten zu Jailbreaks und über Möglichkeiten, diese zu erkennen.

Für die Entwicklung der WearPrivate-App setzen wir gegenwärtig auf iOS 16 als minimale Systemvoraussetzung. Dieses wird von 46 Geräten unterstützt, von denen für nur 10 nach aktuellem Wissensstand ein Jailbreak existiert.

In einem BSD-2 lizensierten Swift-Paket[4] werden die gängigsten Mechanismen zur Erkennung von Jailbreaks zur Einbindung in eigene Anwendungen zur Verfügung gestellt. Gleichzeitig weist Eidingers Artikel jedoch darauf hin, dass wiederum Gegenmaßnahmen existieren, um Mechanismen zur Erkennung von Jailbreaks auszuhebeln. Diese seien allerdings oft keine allgemein einsetzbaren Lösungen, sondern müssten konkret auf eine anzugreifende Anwendung zugeschnitten werden.

Bei der Entscheidung, ob man für eine Anwendung eine Jailbreak-Erkennung implementieren sollte, sei weiterhin auch zu beachten, dass laufender Aufwand betrieben werden müsse, um auf dem Stand der Technik von Jailbreaks zu bleiben und Gegenmaßnahmen aktuell zu halten. Dazu komme der finanzielle und organisatorische Aufwand, Test- und Entwicklungsgerät zu beschaffen und zu pflegen, mit denen die technische Funktionsfähigkeit verifiziert werden kann.

Angesichts des in Abschnitt 2.1.1 aufgezeigten Angriffsszenarios sollte eine Jailbreak-Erkennung in der WearPrivate-App zum Einsatz kommen (R_E4). Dass eine grundlegende Implementierung nicht von Grund auf vorgenommen werden muss, sondern als Swift-Paket verfügbar ist, erleichtert die Umsetzung dieser Entscheidung. Für die Entscheidung, wieviel Aufwand in dem Projekt in die Umgehung von Erkennungsgegenmaßnahmen gesteckt werden sollte, sind zum gegenwärtigen Zeitpunkt nicht ausreichend Daten vorhanden.

[4] https://github.com/securing/IOSSecuritySuite

Anforderung 3 *Das Package IOSSecuritySuite soll zur Erkennung von Jailbreaks in unsere Anwendung integriert sein und deren Nutzung auf kompromittierten Geräten verhindern.*

2.1.4 Button für Unterbrechung implementieren

Um sicherzustellen, dass keine unerwünschten Nutzerdaten in die Analyse gelangen (T_AN16), soll die graphische Benutzungsschnittstelle jederzeit klar kommunizieren, ob die aktuellen Daten in der App erfasst werden (R_AN34). Gleichzeitig soll ein einfach zu erkennendes und zu bedienendes Element in der Benutzungsschnittstelle stets die Möglichkeit geben, die Datenerfassung zu beenden oder wieder neu zu starten (R_AN35).

Eine Möglichkeit, diese beiden Anforderungen zu erfüllen, könnte das auf den Apple-Plattformen nativ verfügbare Toggle[5]-Element sein. Dieses sollte mindestens auf der Hauptseite in der App platziert werden – durch Benutzbarkeitsstudien könnte geklärt werden, ob dieser Schalter mehreren oder allen Bildschirmen in der App zu sehen sein sollte.

Je nachdem, wie genau die Daten erhoben werden, muss bei der Implementierung darauf geachtet werden, dass wirklich alle vom Wearable ausgelesenen Daten dahingehend überprüft werden, dass sie nicht von einem Zeitpunkt stammen, an dem die Erhebung deaktiviert war. Dies könnte beispielsweise passieren, wenn das Wearable Daten zunächst intern aggregiert und erst mit Verzögerung an die App sendet – möglicherweise auch als Teil eines Caching-Mechanismus, falls eine Zeitlang keine Kommunikation mit der App möglich ist. Innerhalb der App sollte die Datenverarbeitung daher nach dem Opt-In-Prinzip implementiert werden: Der Toggle ist beim ersten Start der App ausgestellt und muss von der Nutzerin aktiv eingeschaltet werden. Die Zeiträume, in denen die Nutzerin den Toggle zur Verarbeitung auf „aktiv“ gestellt hat, sollen innerhalb der App protokolliert werden. Die vom Wearable eingehenden Daten müssen dann dahingehend gefiltert werden, dass sie innerhalb dieses Zeitraums liegen. Falls ja, dürfen sie weiterverarbeitet werden; falls nein, müssen sie sofort verworfen werden.

Anforderung 4 *Nur Daten aus den von der Nutzerin per Toggle freigegebenen Zeiträumen dürfen weiterverarbeitet werden.*

2.2 Interaktion und Integration

2.2.1 Initial deaktivierte Push-Mitteilungen

Push-Mitteilungen sind auf der iOS-Plattform von Haus aus initial deaktiviert. Bevor sie an eine App gesendet oder von dieser lokal ausgelöst werden können, ist die Zustimmung der Nutzer nötig (T_AN20). Diese wird durch einen systemeigenen Mechanismus eingeholt, der auf Anforderung der Anwendung einen Systemdialog mit den Optionen „Zustimmen“ und „Ablehnen“ anzeigt (R_AN54). Einzig der Begründungstext, der in diesem Dialog angezeigt wird, ist anpassbar.

Es gilt als Best Practice in der UX-Gestaltung, diese Zustimmung erst zu dem Zeitpunkt abzurufen, ab dem das Zustellen von Mitteilungen für die Nutzerin relevant wird (R_AN54). Typischerweise geht dem eine konkrete Handlung der Nutzerin voraus (Beispiel: in einer Kalender-App wird zum ersten Mal die Option gewählt, eine Erinnerung im Vorfeld zu einem Termin zu geben). Teilweise schalten Apps vor dem Auslösen der Systemabfrage noch einen eigenen Bildschirm vor, in dem detaillierter erklärt wird,

[5] https://developer.apple.com/design/human-interface-guidelines/components/selection-and-input/toggles

welche Arten von Mitteilungen es gibt und wodurch sie ausgelöst werden. Hiermit soll der Nutzerin Kontext für eine fundierte Entscheidung bei der Beantwortung des Systemdialogs gegeben werden.

Als Kontrast zu dieser Vorgehensweise ist das Dark Pattern zu nennen, sofort nach dem ersten Start der Anwendung nach der Genehmigung für Mitteilungen zu fragen. Hierdurch ist es für die Nutzer praktisch gar nicht absehbar, wann, wie oft und welche Mitteilungen sie von der App erhalten werden. Allerdings führt dieses Vorgehen mittlerweile auch zunehmend dazu, dass die Genehmigung dann einfach nicht erteilt wird.

Anforderung 5 *Die Anforderung zur Erlaubnis von Push-Mitteilungen soll erst zu einem angemessenen Zeitpunkt ausgelöst werden und bei der UX-Konzeption soll berücksichtigt werden, dass die Nutzer vor dieser Anfrage angemessen über die Konsequenzen informiert werden.*

2.2.2 Keine Gesundheitsdaten in Push-Mitteilungen

Mit der Nutzung von Push-Mitteilungen gehen zwei mögliche Gefährdungen des Datenschutzes einher (T_AN17). Zum einen können unerwartet auf dem Bildschirm erscheinende und verbleibende Nachrichten ungewollt private Informationen für eventuelle weitere Betrachter des Geräts zugänglich machen. Zum anderen ist bei der Nutzung von Remote Push-Mitteilungen – also solchen, die ihren Ursprung nicht in der Anwendung haben, sondern über einen entfernten Server ausgelöst werden – ebenfalls das Risiko geben, dass die involvierten Betreiber der Infrastruktur Einblick in persönliche Informationen bekommen können, da die übertragenen Inhalte nicht Ende-zu-Ende-verschlüsselt sind.

Um beiden Problemen zu begegnen, dürfen Push-Mitteilungen nicht genutzt werden, um sensitive Daten direkt anzuzeigen (R_AN55). Bei der Gestaltung der App und des Benachrichtigungskonzeptes ist darauf zu achten, höchstens eine allgemein gehaltene Nachricht oder Handlungsaufforderung, beispielsweise „Öffnen Sie die WearPrivate-App für aktuelle Informationen“ anzuzeigen.

Anforderung 6 *Push-Mitteilungen dürfen keine sensitiven Daten anzeigen.*

2.3 Betrieb und Nutzung

2.3.1 Prüfung des Vertriebswegs

iOS-Anwendungen können grundsätzlich über mehrere Wege auf ein Gerät aufgespielt werden. Diese möglichen Vertriebswege unterschieden sich teils erheblich in der Komplexität für den Benutzer, die damit möglichen Geschäftsmodelle, der gewährleisteten Integrität sowie der technischen Voraussetzungen.

Die Auslieferung über den Apple AppStore stellt sicherlich den für den Anwender am einfachsten handhabbaren Vertriebsweg dar. Der AppStore ist auf jedem iOS-Gerät verfügbar und durch den Überprüfungsprozess seitens Apple ist für Nutzer eine gewisse Sicherheit gegeben, dass eine darüber bezogene App kein schadhaftes Verhalten aufweist und auch nur im Rahmen der erlaubten Schnittstellen auf Daten zugreifen wird. Andererseits birgt dieser Überprüfungsprozess allerdings auch das unternehmerische Risiko, erst mit Einreichung der Anwendung die endgültige Antwort zu erhalten, ob Apple das entwickelte Produkt tatsächlich in den Katalog aufzunehmen bereit ist.

Der Gegenpol zu diesem Ansatz ist die Auslieferung über die App-Repositories, die nach einem Jailbreak zur Verfügung stehen. Diese obliegen keiner Art von Review und Kontrolle (T_E1, T_E2). Dies könnte einer App beispielsweise erlauben, Daten über den Nutzer aus anderen als den offiziellen Schnittstellen zu beziehen. Aufgrund der in Abschnitt 2.1.3 beschriebenen Sicherheitsrisiken, die ein Jailbreak mit sich bringt, ist dieser Ansatz für WearPrivate aber inakzeptabel.

Gegenwärtig zeichnet sich die Möglichkeit ab, dass die iOS-Plattform im Laufe des Jahres 2024 in Europa für alternative AppStores geöffnet werden muss. Sollte dies innerhalb der Projektlaufzeit geschehen, sollten die sich hieraus ergebenden Möglichkeiten auf ihre Eignung für WearPrivate überprüft werden. Bis dahin soll jedoch gelten (R_E5):

Anforderung 7 *Die App soll über den AppStore vertrieben werden.*

2.3.2 Datensicherung

Nach dem Prinzip der Datensparsamkeit soll die WearPrivate App nicht mehr Daten als nötig lokal vorhalten (R_AN32). Grundsätzlich wird die App nur ein paar grundlegende Parameter (Session Keys, Nutzerdaten wie Gewicht u. ä.) sowie Cachedateien für die Wiederholung von Uploads abspeichern. Letztere werden nach erfolgreichem Upload direkt gelöscht. Weiterhin ist der langfristige Nutzen von einem Datenausschnitt sehr gering. Für die Datenanalyse und insbesondere die Echtzeitwarnung ist es nicht kritisch, im Nachhinein (möglicherweise Wochen später) noch einzelne Datenpakete nachgereicht zu bekommen.

Die Daten der App sind daher so zu markieren, dass sie von Backups ausgenommen werden (R_AN32c).[6] Hierdurch werden einige Angriffsvektoren (kompromittiertes Cloud-Backup, unverschlüsseltes lokales Backup) ausgeschlossen (T_AN15).

Anforderung 8 *Die Daten der App müssen von Backups ausgeschlossen werden.*

2.4 Privacy by Default

2.4.1 Periodisch Daten löschen

Die App soll so wenig Daten wie möglich lokal vorhalten, um die Gefährdung durch eventuelle Angriffe minimal zu halten (R_AN32). Daten, die von Wearables eintreffen, sollen zwar in der App zwischengespeichert werden, bis ein erfolgreicher Upload stattfinden konnte. Danach sollen diese aber umgehend gelöscht werden.

Analysedaten, die vom Backend bereitgestellt werden, sollen für jede Betrachtung erneut angefordert und nicht lokal vorgehalten werden.

Anforderung 9 *Die App soll so wenig Daten wie möglich vorhalten.*

2.4.2 State-of-the-Art Privacy-UI

Nutzer sollen stets klar erkennen können, welche Daten von ihnen wann geteilt werden. Die Einstellungen des Systems sollen ihnen auf eine verständliche Art und Weise erlauben, dieses Verhalten nach den eigenen Wünschen anzupassen (R_AN36c, R_AN35).

Sowohl die visuelle Gestaltung als auch die verwendeten Texte (Aufforderungen, Erklärungen usw.) sollen dieses Ziel unterstützen. Bei der Konzeption und Ausarbeitung soll der aktuelle Stand der Forschung zu diesem Thema berücksichtigt werden.

Anforderung 10 *Nutzer sollen stets klar erkennen können, welche ihrer Daten wann geteilt werden.*

[6] https://developer.apple.com/documentation/foundation/optimizing_your_app_s_data_for_icloud_backup

2.5 Umgang mit Ausnahmesituationen

2.5.1 Pushnachricht an Nutzer

Die Anwender des WearPrivate-Systems sollen gemäß des Projektkonzepts möglichst anonym gegenüber dem Analysedienst sein (T_AN1, T_AN2). Insbesondere soll dieser nicht in der Lage sein, einzelne Anwender persönlich zu identifizieren. Es dürfen also auch keine Kontaktdaten, beispielweise E-Mail-Adressen oder Telefonnummern, zu einem anonymisierten Anwender vorliegen (R_AN2, R_AN3).

Gleichzeitig ist durch die DSGVO eine Mitteilungspflicht im Fall von Datenschutzlecks gegeben (T_AN17). Um die Nutzer des Systems im Falle eines solchen Ereignisses informieren zu können, muss die App entsprechende Möglichkeiten hierzu bereitstellen. Denkbar ist dies als Pushnachricht, die dann an alle Nutzer des Systems ausgestrahlt wird, kombiniert mit einer Anzeige in der App um auch die Nutzer zu erreichen, die Pushnachrichten deaktiviert haben (R_AN35b).

Anforderung 11 *Ein Benachrichtigungsmechanismus für Ausnahmesituationen muss in der App integriert sein.*

3 Technisch-Organisatorische Maßnahmen für den Analyseservice

Die folgenden Anforderungen stellen die wesentlichen technischen und organisatorischen Maßnahmen dar, die der Analyseservice implementieren muss, um die Einhaltung der Datenschutz-Grundverordnung (DSGVO) sicherzustellen. Dabei wird AWS als Cloud-Service-Anbieter eingesetzt, der durch seine umfangreichen Zertifizierungen und Sicherheitsstandards (z. B. ISO 27001, ISO 27017, ISO 27018, SOC 2/3) eine DSGVO-konforme Infrastruktur bereitstellt. Diese Maßnahmen gewährleisten Integrität, Vertraulichkeit und Verfügbarkeit der verarbeiteten Daten und minimieren Datenschutzrisiken durch klare Prozesse und sichere Systemintegration.

3.1 Integrität und Vertraulichkeit

3.1.1 Zugangskontrolle

- Der Zugriff auf personenbezogene Daten ist ausschließlich autorisierten Personen gestattet, die durch ein rollenbasiertes Berechtigungssystem, Passwortschutz und Zwei-Faktor-Authentifizierung geschützt sind.
- Zugangsdaten werden ausschließlich in einem SOC2-zertifizierten Passwort-Manager gespeichert.

3.1.2 Datenverschlüsselung

- Daten werden während der Übertragung mittels TLS 1.2/1.3 verschlüsselt.
- Gespeicherte Daten in der Cloud sind durch AES-256-Verschlüsselung gesichert.
- AWS als Datenhost erfüllt DSGVO-Standards und hält Zertifizierungen wie ISO 27001 (Informationssicherheitsmanagement), ISO 27017 (Sicherheit in der Cloud), ISO 27018 (Datenschutz in der Cloud) und SOC 2/3 ein.

3.1.3 Pseudonymisierung und Datenminimierung

- Daten werden pseudonymisiert verarbeitet, sodass Rückschlüsse auf Einzelpersonen nicht möglich sind.

- Es werden ausschließlich Daten erhoben, die für die Erbringung der spezifischen Dienstleistung erforderlich sind.

3.1.4 Trennungskontrolle

- Kundendaten werden in AWS-Datenbanken gespeichert und sind mandantenfähig organisiert. Die Mandantentrennung wird durch eindeutige Mandanten-IDs sichergestellt, sodass jeder Kunde nur Zugriff auf seine eigenen Daten hat.

3.2 Interaktion und Integration

3.2.1 Sichere Integration

- Schnittstellen zwischen dem Analyseservice und externen Systemen erfolgen ausschließlich über dokumentierte APIs mit TLS-Verschlüsselung.
- Jede Datenübertragung wird protokolliert, um die Nachvollziehbarkeit zu gewährleisten.

3.2.2 Hosting und Infrastruktur

- Die Infrastruktur wird vollständig durch AWS bereitgestellt. Alle Server sind in Rechenzentren innerhalb der EU (z. B. Frankfurt am Main) gehostet.
- AWS garantiert durch sein Data Processing Addendum, dass Daten ausschließlich in der festgelegten Serverregion verarbeitet werden.
- Die AWS-Rechenzentren verfügen über umfassende Sicherheitsmaßnahmen, darunter Zutrittskontrollen, redundante Stromversorgung und Notfallsysteme.

3.2.3 Systemübergreifende Sicherheit

Alle Systeme, die mit dem Analyseservice interagieren, müssen strenge Sicherheits- und Datenschutzanforderungen erfüllen, bevor sie integriert werden.

3.3 Betrieb und Nutzung

3.3.1 Benutzerfreundliche Anwendungen

- Mobile App und Dashboard sind intuitiv gestaltet und bieten datenschutzfreundliche Voreinstellungen.
- Benutzer erhalten regelmäßige Schulungen zum sicheren Umgang mit den Anwendungen.

3.3.2 Protokollierung und Monitoring

- Systemaktivitäten werden automatisch protokolliert, einschließlich Zugriffe, Änderungen und Datenübertragungen.
- Protokolldaten werden regelmäßig überprüft, um Sicherheitsvorfälle frühzeitig zu erkennen.

3.3.3 Backup- und Wiederherstellungsverfahren

- AWS stellt ein automatisiertes Backup-System bereit, das regelmäßige Snapshots der Datenbanken erstellt.
- Backups werden in redundanten AWS-Zonen gespeichert, um die Wiederherstellung im Falle eines Ausfalls sicherzustellen.

3.4 Privacy by Default

3.4.1 Datensparsame Voreinstellungen

- Standardmäßig werden nur die minimal erforderlichen Daten erfasst und verarbeitet.
- Analyseprozesse sind so konzipiert, dass personenbezogene Daten nicht länger als nötig gespeichert werden.

3.4.2 Anonymisierung von Daten

- Vor der Analyse werden, wo möglich, personenbezogene Daten anonymisiert, um Datenschutzrisiken zu minimieren.

3.4.3 Einhaltung von Datenschutzprinzipien

- Prozesse und Systeme werden regelmäßig überprüft und aktualisiert, um den Prinzipien der Datenminimierung und Zweckbindung zu entsprechen.

3.5 Umgang mit Ausnahmesituationen

3.5.1 Vorfallmanagement

- Sicherheitsvorfälle werden gemäß einem festgelegten Incident-Response-Plan bearbeitet.
- Betroffene Personen und zuständige Behörden werden im Falle einer Datenschutzverletzung unverzüglich informiert.

3.5.2 Schulungen zu Notfallszenarien

- Mitarbeiter werden regelmäßig in den Prozessen geschult, die im Falle von Datenschutz-vorfällen anzuwenden sind.

3.5.3 Zentrale Ansprechpartner

- Ein Datenschutzbeauftragter oder Ansprechpartner ist jederzeit erreichbar, um bei Vorfällen oder Datenschutzfragen Unterstützung zu leisten.

4 Schutzmaßnahmen resultierend aus der Prozesssicht

Betrachtet man die gesamte Prozesskette einer Wearable-Nutzung am Arbeitsplatz, beginnend bei der Einführung des Systems, der Einwilligung zur Teilnahme an der Systemnutzung bis zur Beendigung des Wearable-Einsatzes, so ergeben sich verschiedene, zum Teil auch nicht-technische Anforderungen an die Prozessgestaltung, die im Folgenden beleuchtet werden sollen.

4.1 Erhebung einer Einwilligung

Die Verarbeitung personenbezogener Daten ist grundsätzlich nur zulässig, wenn ein Erlaubnistatbestand vorliegt, der dies rechtfertigt. Im Ergebnisbericht D2.1 [17], Kapitel 4, haben wir ausführlich dargelegt, welche rechtlichen Grundlagen dafür in Frage kommen.

Ein möglicher Erlaubnistatbestand wäre die Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses unter Berufung auf § 26 Abs. 3 S. 1 BDSG iVm. § 3 Abs. 1 ArbSchG. Die Berufung auf diese Bestimmung erfordert jedoch eine Verhältnismäßigkeitsprüfung, bei der Legitimität, Geeignetheit, Erforderlichkeit und Angemessenheit der Vitaldatenerfassung zum Zwecke

des Arbeits- und Gesundheitsschutzes gegenüber dem Recht des Betroffenen auf Schutz seines allgemeinen Persönlichkeitsrechts sorgfältig abzuwägen sind. Der Ausgang einer solchen Prüfung ist ungewiss, da der Arbeits- und Gesundheitsschutz bei den allermeisten Arbeitsstätten bisher auch ohne Vitaldatenerfassung in ausreichendem Maße gewährleistet ist. Die Nutzung von Wearables für eine genauere Überwachung der physischen und psychischen Mitarbeiterbelastung kann daher auch als verzichtbare Bonusleistung angesehen werden, die aber eine verpflichtende Teilnahme an einem solchen Messprogramm nicht ausreichend rechtfertigt.

Wahrscheinlicher und voraussichtlich auch vielversprechender ist eine freiwillige Einwilligung der Betroffenen nach § 23 Abs. 3 S. 2, Abs. 2 BDSG als rechtliche Grundlage für den Wearable-Einsatz am Arbeitsplatz. Eine solche Einwilligung ist, wie im Ergebnisbericht D2.1 beschrieben nach Art. 4 Nr. 11 DSGVO, „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Genauere Voraussetzungen für eine rechtsgültige Einwilligung sind im Ergebnisbericht D2.1, Abschnitt 4.1, eingehender beschrieben. Aus dieser Analyse ergibt sich, dass an den Anwendungsfall des WearPrivate-Projekts hohe Anforderungen zu stellen sind, da es sich um die Erfassung von Vitaldaten handelt, noch dazu im Kontext eines Beschäftigungsverhältnisses, was den Nachweis der Freiwilligkeit erschwert. Daraus ergibt sich insbesondere (siehe Ergebnisbericht D2.1, Abschnitt 4.1.5), die Informiertheit der Arbeitnehmer sicherzustellen. Der Arbeitgeber muss also darlegen, welche Daten zu welchen genauen Zwecken erhoben werden und wer diese Daten in welcher Form nutzen darf. Darüber hinaus sind die Einwilligungen ausdrücklich einzuholen und nicht auf bloßes konkludentes Verhalten zu stützen. Zum Nachweis der Einwilligung empfiehlt sich eine schriftliche Dokumentation. Wird die Einwilligung auf § 26 Abs. 3 S. 2, Abs. 2 BDSG gestützt, ist nach § 26 Abs. 2 S. 3 BDSG die schriftliche oder elektronische Einholung der Einwilligung verpflichtend, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Den Arbeitnehmern ist freie Wahl hinsichtlich der Nutzung der Wearables zu geben. Arbeitnehmer, die nicht in die Teilnahme an dem Messprogramm einwilligen, dürfen keine Nachteile erleiden. Im Idealfall ist die Datenerfassung so gestaltet, dass man einem Mitarbeitenden die Teilnahme oder Nichtteilnahme an der Vitaldaten-erfassung nicht eindeutig nachweisen kann, was einer Diskriminierung von Personen, die sich dem Messprogramm verweigert haben, wirksam vorbeugt.

Angesichts dieser hohen Anforderungen an den Einwilligungsprozess erscheint es sinnvoll, die Einwilligung im Rahmen einer ausdrücklichen Informationsveranstaltung einzuholen, in der sich die Mitarbeitenden umfassend über die verwendete Technologie, die Wirkungsweise des Systems sowie den beabsichtigten Zweck und Nutzen des Messprogramms informieren können. Würde die Aufklärung der Nutzer nur individuell über entsprechende Informationsschnittstellen der mobilen App erfolgen und jeder Nutzer würde sich nur individuell informieren, wäre der Erfolg der Aufklärungsmaßnahme nur schwer zu gewährleisten und nachzuweisen. Angesichts dieser Vorbehalte plädieren wir im WearPrivate-Projekt eher für eine nichttechnische organisatorische Maßnahme, um die Voraussetzungen für eine rechtsgültige Einwilligung der Betroffenen zu schaffen und die Einwilligung nachweislich korrekt einzuholen.

Anforderung 12 *Vor der Einführung einer Wearable-basierten Vitaldatenerfassung zum Zwecke des Arbeits- und Gesundheitsschutzes muss der Arbeitgeber die Belegschaft umfassend über die geplante Maßnahme und deren Zwecke, die eingesetzten Mittel und ihre Wirkungsweise, die dabei erhobenen Daten und deren Verwendung sowie die Empfänger der aus dem Messprogramm abgeleiteten Informationen informieren.*

Anforderung 13 *Basierend auf den vermittelten Informationen gemäß Anforderung 12 ist von den Mitarbeitenden eine informierte, freiwillige, ausdrückliche und ggf. schriftliche oder elektronische Einwilligung zur Teilnahme an der Vitaldatenerfassung mittels Wearables und deren Auswertung zum Zwecke des Gesundheits- und Arbeitsschutzes einzuholen. Diese Einwilligung ist zu dokumentieren.*

In Ergänzung dazu sollte die WearPrivate-App Verweise auf alle notwendigen Informationen bereithalten, damit die Nutzer die genauen Bedingungen und Folgen des Wearable-Einsatzes jederzeit nachlesen und bei Bedarf ihre Einwilligung zurückziehen können (R_AN36a, R_AN36c).

Anforderung 14 *Alle Informationen, die der Arbeitgeber gemäß Anforderung 12 den Betroffenen vermittelt hat, müssen von der mobilen WearPrivate-App vom Nutzer bei Bedarf jederzeit abrufbar sein.*

Beruht der Erlaubnistatbestand auf einer freiwilligen Einwilligung des Betroffenen, so muss dieser in der Lage sein, seine Einwilligung jederzeit zu widerrufen. Wird die Einwilligung auf § 26 Abs. 3 S. 2, Abs. 2 BDSG gestützt, ist der Betroffene in Textform über sein Widerrufsrecht aufzuklären. Im Falle eines Wearable-Messprogramm können die Teilnehmenden im Prinzip jederzeit die Nutzung der Wearables einstellen. Allerdings ist zu klären, was dann mit den bisher gesammelten Daten geschehen soll. Daher ist es wichtig, eine Funktion für einen Widerruf am besten auch explizit in der WearPrivate-App bereitzustellen (R_AN36c).

Anforderung 15 *Die Mobil-App für die Teilnahme an einem Vitaldaten-Messprogramm zum Zwecke des Arbeits- und Gesundheitsschutzes muss eine Funktion bereitstellen, mit der ein Nutzer seine Einwilligung zur Teilnahme an dem Messprogramm jederzeit widerrufen kann.*

Die ausdrückliche Erhebung einer Einwilligung stellt sicher, dass alle Nutzer der WearPrivate-Lösung genau wissen, worauf sie sich einlassen, und sich auf Basis umfassender Informationen bewusst für oder gegen eine solche Lösung entscheiden können (T_AN18).

4.2 Verhinderung der Zuordnung von Daten zu einer Person

Um den Schutz der Privatsphäre zu gewährleisten (T_AN1 – T_AN10, T_AN15), ist es nötig, die Zuordnung von Daten, welche die App an das Analysesystem übermittelt, zu einer Person hinreichend zu erschweren. Dazu trägt die ins Auge gefasste Dienststruktur auf unterschiedliche Weise bei:

- Datenschutzfreundliche Registrierung der Dienstnutzer
- Untergliederung der Verarbeitungskette und Rollentrennung
- Verlagerung von Verarbeitungsschritten in Bereiche mit besseren Datenschutzeigenschaften
- Interventionsmöglichkeiten der Nutzer entlang der Verarbeitungskette
- Anonymisierung der Kommunikationsendpunkte und geschützte Datenübertragung

Im Folgenden erläutern wir die zugrundeliegenden Architekturkonzepte und ihren jeweiligen Beitrag zu Datenschutz und Datensicherheit. Ausgangspunkt der Betrachtungen ist die Dienststruktur für Wearable-gestützte Arbeitnehmer-Belastungsreports, wie sie derzeit (in etwa) vom Projektpartner WearHealth betrieben wird. Abbildung 1 zeigt den Aufbau dieses Dienstes in seiner grundlegenden Struktur.

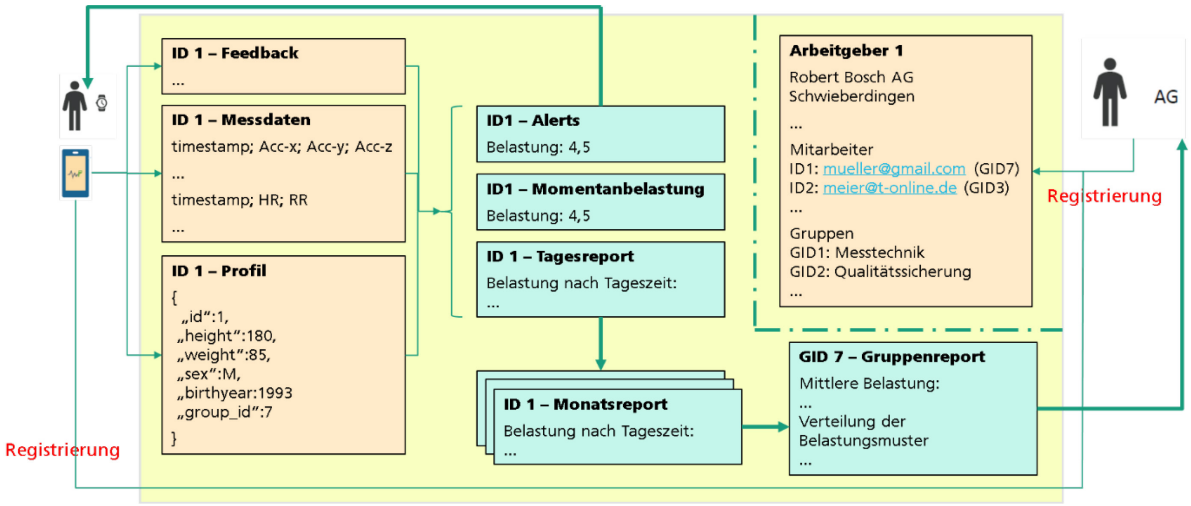

Abbildung 1 Schematische Übersicht über die bestehende Dienststruktur des WearHealth-Dienstes zur Ermittlung von Belastungen am Arbeitsplatz

Der von WearHealth gewählte Ansatz sieht vor, dass sich der Arbeitgeber beim Dienst registriert und dabei die Mitarbeiter, die den Dienst in Anspruch nehmen sollen, mit ihrer E-Mail-Adresse und ihrer organisatorischen Gruppenzugehörigkeit im Unternehmen meldet. Der Dienstbetreiber sendet den nominierten Arbeitnehmern per E-Mail-Nachricht Zugangsberechtigungen zu, und die vorgesehenen Teilnehmer registrieren sich damit beim Dienst. Bei der Registrierung gibt der Arbeitnehmer zudem einige relevante Profildaten an, die für die Berechnung eines Belastungsindikators relevant sind, wie etwa Geschlecht, Alter, Körpergewicht und Körpergröße.

Der Datenverarbeitungsprozess nach erfolgreicher Registrierung ist dann wie in seinen Grundzügen wie folgt:

1. Das vom Arbeitnehmer getragene Wearable übermittelt die gemessenen Vital- und Kontextdaten mittels Bluetooth-an das persönliche Smartphone des Arbeitnehmers, und dieses überträgt diese Rohdaten weiter an den Dienst.
2. Der Dienst bestimmt aus den übermittelten Rohdaten einen abstrakten Belastungsindikator und gegebenenfalls – bei kritischer Belastung oder anderen Anzeichen für eine Gefährdung des Teilnehmerwohls – eine Warnung in Form einer Pushnachricht. Die so ermittelten Informationen zur Momentanbelastung werden dem Teilnehmer auf seinem Smartphone angezeigt.
3. Die Momentanbelastungen eines jeden Teilnehmers werden über den Tagesverlauf in geeigneten Intervallen aggregiert; aus den Tagesverläufen können je nach Bedarf Tages-, Wochen, oder Monatsreports erstellt werden, die dem Teilnehmer (und nur diesem) auf seinem Smartphone bereitgestellt werden können.
4. Die individuellen Monatsreports aller Mitglieder einer vom Arbeitgeber zuvor definierten Gruppe werden monatlich zu einem Gruppenbericht aggregiert. Der Arbeitgeber erhält für jede von ihm benannte Gruppe einen Report, der die Belastungssituation in der Gruppe anhand abstrahierter Belastungsindikatoren widerspiegelt.

Die hier beschriebene Dienststruktur hat einige Vorteile:

- Der Dienstanbieter hat über die E-Mail-Adresse einen direkten Kanal zu den Teilnehmern. Dies ermöglich ein sehr einfaches Registrierungsverfahren und stellt sicher, dass nur die

vorgesehenen Teilnehmer an dem Messprogramm teilnehmen, ohne dass Trittbrettfahrer den Dienst unentgeltlich in Anspruch nehmen und dabei das Messergebnis verfälschen.

- Der Rückkanal ermöglicht darüber hinaus auch Komfortfunktionen wie zum Beispiel Passwort- oder Account-Recovery.
- Der gesamte Dienst wird monolithisch von einem einzigen Unternehmen betrieben, was den technischen, organisatorischen und juristischen Aufwand des Dienstleisters minimiert und so eine bestmögliche Wirtschaftlichkeit verspricht.

Im Hinblick auf Datenschutz und Datensicherheit hat die Lösung jedoch folgende Nachteile:

- Die E-Mails-Adresse aller Teilnehmer ist dem Dienstleister bekannt (T_AN2, T_AN3), was eine vollständig anonyme Dienstnutzung verhindert und nicht den Datenschutzrichtlinien des Bundesinstituts für Arzneimittel und Medizinprodukte entspricht, die für digitale Gesundheitsanwendungen Freischaltcodes ohne personenidentifizierende Merkmale fordern (siehe [1], Abschnitt 6.5, Erläuterungen zu DMN_1.1b, S. 30).
- Während der Analyse der Vital- und Profildaten werden Individuen und Gruppen zwar nur unter einen Pseudonym (der Teilnehmer-ID und Gruppen-ID) geführt. Die Pseudonymtabelle, die Pseudonyme wieder den Personen-identifizierenden E-Mail-Adressen den Gruppennamen zuordnet, liegt aber beim Dienstleister und ist dort nur durch technisch-organisatorische Maßnahmen von den Rohdaten getrennt.

Bedenkt man zudem, dass der Dienstleister den Namen und Standort des Arbeitgebers kennt, so sind die beim Dienstleister insgesamt gespeicherten Daten geeignet, die wahre Identitäten der Teilnehmer zu ermitteln. Dies birgt die Gefahr eines Innentäterangriffs (T_AN8). Aber auch ein Hacker, der erst einmal in die IT-Systeme eingedrungen ist, könnte mit einiger Wahrscheinlichkeit dann auch die internen Datenschutzbarrieren überwinden, die personenbeziehbaren Daten zusammenführen und so sensitive, personenbezogene Gesundheitsdaten erbeuten.

4.2.1 Registrierung

Um die Gefahren durch Innentäter (T_AN8) oder erfolgreiche Hackerangriffe zu reduzieren, sollte der Personenbezug der verarbeiteten Daten minimiert werden. Ein wichtiger Schritt dazu ist die Bereitstellung eines anonymen Registrierungsverfahrens, dass die Re-Identifizierung der Teilnehmer anhand ihrer Registrierungsinformationen (T_AN3) verhindert (R_AN6, R_AN7):

Anforderung 16 *Arbeitnehmer benötigen für die Teilnahme am Messprogramm nur einen anonymen Freischaltcode ohne personenidentifizierende Merkmale. Eine Erfassung von Namen, Adressen, E-Mail-Adressen, Telefonnummern oder anderen personenbezogenen Angaben über die Teilnehmer beim Dienstleister erfolgt nicht. Die teilnehmenden Individuen am Messprogramm werden vom Dienstleister nur unter einer zufällig vergebenen ID-Nummer geführt; ihre wahre Identität bleibt dem Dienstleister verborgen.*

Eine praktische Umsetzung dieser Anforderung könnte wie folgt aussehen (vgl. [9], Abschnitt 8.4):

1. Der Dienstleister erstellt Freischaltcodes in Form von fälschungssicheren Tickets.
2. Der Arbeitgeber erwirbt diese Tickets für seine Arbeitnehmer, ohne diese gegenüber dem Dienstleister zu benennen.
3. Der Dienstleister kennt nur die Kontaktdaten des Arbeitgebers für die Geschäftsabwicklung, nicht aber die seiner Mitarbeiter.

4. Der Arbeitgeber verteilt die Tickets zufällig unter den Arbeitnehmern, die am Messprogramm teilnehmen.
5. Die Arbeitnehmer registrieren sich anonym und werden im Folgenden unter einer zufällig gewählten ID als ihrem Pseudonym und einem zugeordneten, von Teilnehmer wählbaren Passwort geführt: Nur der betreffende Arbeitnehmer kennt seine wahre Identität, die seinem individuellen Pseudonym zugeordnet ist.
6. Der Dienstleister verifiziert anhand der Gültigkeit des Tickets, dass der anonyme Teilnehmer zur Teilnahme berechtigt ist und dass seine Diensterbringung (durch den Ticketverkauf) für diesen Teilnehmer vergütet wird.
7. Jeder Freischaltcode, der zur Registrierung verwendet wurde (d.h. jedes eingelöste Ticket) verliert mit der Registrierung seine Gültigkeit. Teilnehmer weisen ihre gültige Registrierung im weiteren Verlauf der Dienstnutzung mit ihrer ID und ihrem Passwort nach.
8. Der weitere Kontakt zwischen Dienstleister und Teilnehmer erfolgt ausschließlich über eine anonyme Kommunikationsverbindung, die der Teilnehmer nach Bedarf mit dem Dienst aufbaut. Aus Sicht dies Dienstanbieters ist die nicht-personalisierte Smartphone-App der einzige Kontaktpunkt. Die Identität des Smartphone-Nutzers oder andere, potenziell personenbeziehbare Daten wie die IP-Adresse des Smartphones bleiben dem Dienst verborgen (R_AN3).

4.2.2 Trennung von Teilnehmer- und Geschäftsdaten

Auch mit der anonymen Registrierung der Teilnehmer bleibt ein Restrisiko bestehen, die die Vital- und Profildaten starke Rückschlüsse auf die Identität des Teilnehmers zulassen (T_AN4), sofern man die Gruppenmitglieder der Analysegruppen kennt. Da der Dienstleister den Arbeitgeber und die Namen der Analysegruppen (zur benutzerfreundlichen Aufbereitung der Gruppenreports) kennt, könnte er unter Umständen einzelne Gruppenteilnehmer ermitteln und sie anhand der Mess- und Profildaten re-identifizieren.

Um diesen Rückschluss zu erschweren, sollte man daher den Analysedienst von den Vertriebsprozessen des Dienstleisters abtrennen (, R_WH3, R_WH4, R_AN8, R_AN10, R_AN19, R_AN20), wie in Abbildung 2 dargestellt.

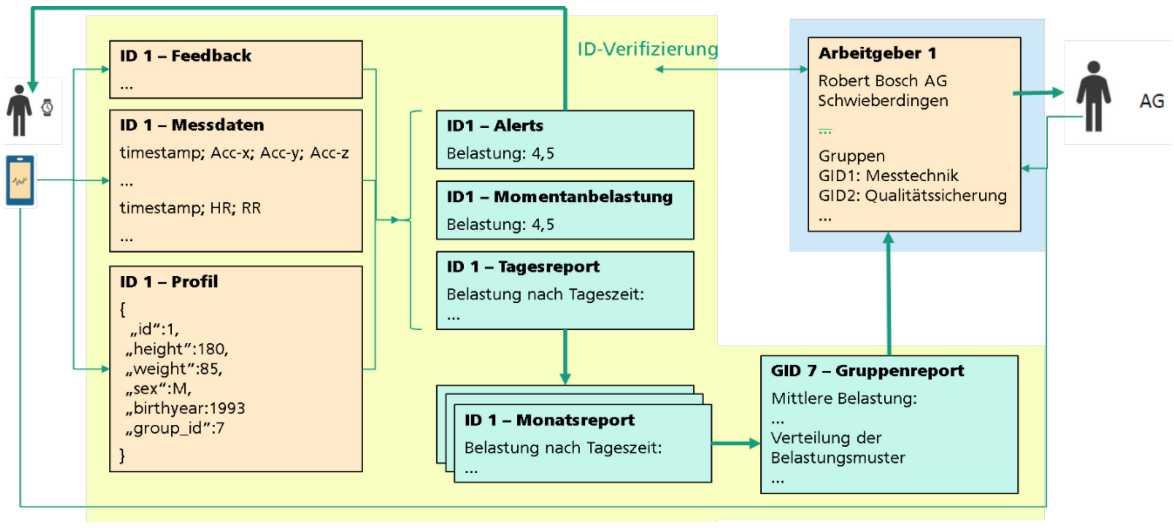

Abbildung 2 Trennung von Analysedienst und Vertrieb. Die Trennung verhindert, dass der Analysedienst (gelb hinterlegt) Kenntnis des Arbeitgebers oder der Gruppen hat. Umgekehrt hat der vertrieb (blau hinterlegt) keine Kenntnis mehr von Vital- und Profildaten oder auch nur von abgeleiteten individuellen Belastungsverläufen.

Anforderung 17 *Die Gesamtdienstleistung »Belastungsmessprogramm für Arbeitnehmergruppen« soll in zwei unabhängige Teildienste unterteilt werden: (1) einen Analysedienst, der die Rohdaten anonymer Teilnehmer zu Gruppenberichten für anonyme Gruppen verdichtet; (2) einem Vertrieb, der die Geschäftsabwicklung mit dem Arbeitgeber übernimmt (z. B. Vertragskonditionen, Bereitstellung anonymer Teilnahmetickets, Ticketverifikation und Entwertung, Lieferung der Ergebnisse, Inkasso, Kundenbetreuung).*

Sind Analysedienst und Vertrieb getrennte, unabhängige Instanzen (R_WH3, R_WH4), so kann der Vertrieb selbst auf Bitten des Arbeitgebers nichts dazu beitragen, den Gruppenreport wieder bis auf die Belastungsverläufe einzelner Individuen aufzulösen, die der Arbeitgeber unter den Teilnehmern der Analysegruppe leicht ausmachen könnte. Insbesondere hat der Vertrieb keinerlei Einblick mehr in die unverarbeiteten Rohdaten oder Profile einzelner Teilnehmer, sondern sieht nur das Endresultat der Analyse, den über einen längeren Zeitraum und über mehrere Teilnehmer aggregierten und zu Belastungsindikatoren abstrahierten Gruppenreport (R_AN19). Mithin wäre der Vertrieb dann auch kein sehr lohnendes Angriffsziel mehr für Innentäter oder Hacker.

Umgekehrt kennt der Analysedienst zwar die sensitiven Vitaldaten der anonymen Teilnehmer, hat aber selbst keine Kontextinformationen zu Teilnehmern, ihrem Arbeitgeber oder ihrer Analysegruppe, die er zur Re-Identifizierung nutzen könnte (R_AN18). Entsprechend könnte ein Innentäter oder ein Hacker die Rohdaten des Analysedienstes auch nicht ohne Weiteres missbrauchen, um einzelne Teilnehmer zu kompromittieren.

Um eine noch weitere Entkopplung zwischen Individualdaten und Gruppenreport zu erzielen, kann bei Bedarf die Gruppenbildung strikt von der Erstellung der Individualanalysen getrennt werden.

Anforderung 18 *[optional] Nutzer sollen gegenüber dem Analysedienst nicht ihre Gruppen-ID offenlegen. Stattdessen aggregiert der Analysedienst die Daten eines Individuums zu Individualreports. Diese gibt er an eine gesonderte Instanz weiter, den Gruppenintegrator. Der Gruppenintegrator aggregiert die erhaltenen Individualreports zu Gruppenreports, die er dann an den Vertrieb weiterleitet. Zu diesem Zweck teilt jeder individuelle Nutzer dem Gruppenaggregator (unter Umgehung des Analysedienstes) anonym seine ID und seine GID mit.*

Der Gruppenintegrator kann die Gültigkeit von ID und GID vom Vertrieb bestätigen lassen und die Daten ungültiger IDs oder GIDs verwerfen. Abbildung 3 zeigt das Prinzip der Trennung in drei unabhängige Parteien. Wie man sieht, ist die Gruppen-ID in dieser Variante nicht mehr Bestandteil des Nutzerprofils.

Gegenüber der Zweiteilung nach Abbildung 2 liefert die Dreiteilung nur noch einen verhältnismäßig geringen zusätzlichen Identitätsschutz. Ob sich der organisatorische Aufwand, hier eine zusätzliche Verarbeitungsinstanz in der Prozesskette vorzusehen, müssen weitere Untersuchungen erst ergeben. Die Trennung soll aber zumindest dadurch vorbereitet werden, dass man die Übergabeschnittstelle von den individuellen Monatsreports zu den aggregierten Gruppenreports in der Prozesskette klar erkennbar und leicht auftrennbar gestaltet

Ein Vorteil dieser Variante könnte aber auch sein, dass der individuelle Nutzer bis zuletzt die Kontrolle darüber behält, ob er dem Gruppenaggregator seine Gruppen-ID offenlegen will. Tut er dies nicht, bleibt er im Gruppenreport unberücksichtigt.

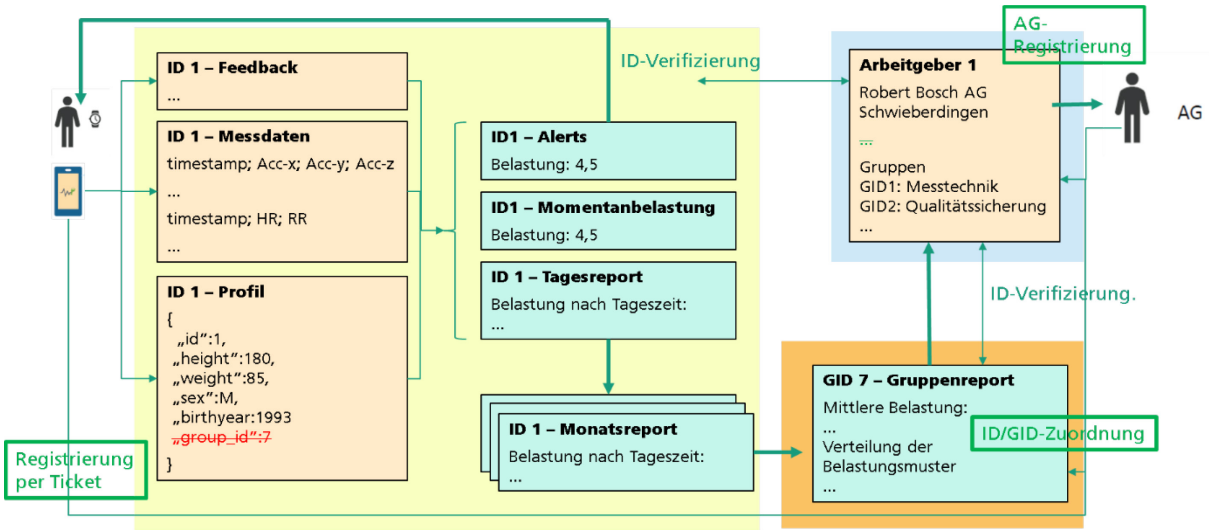

Abbildung 3 Prinzip der Trennung von Analysedienst, Gruppenintegrator und Vertrieb

5 Datennutzungskontrolle

Für eine umfassende Kontrolle der Datennutzung im Gesamtsystem empfiehlt sich eine Integration der Kontrollmechanismen in alle Komponenten der Verarbeitungskette [14]. Gemäß den jeweiligen Datennutzungsregeln können dann entsprechende Maßnahmen in den Komponenten durchgeführt und der regelkonforme Umgang mit den Daten entlang der gesamten Verarbeitungskette sichergestellt werden. Darüber hinaus bietet eine Integration in allen Systemkomponenten den Vorteil, dass Maßnahmen – abhängig von den technischen Möglichkeiten – möglichst früh in der Systemkette greifen können, also beispielsweise sensible Daten erst gar nicht oder zumindest nicht ohne vorherige Anonymisierung übermittelt werden. Das zahlt unter anderem auf den Verarbeitungsgrundsatz der Datensparsamkeit ein und folgt dem Need-to-know-Prinzip.

MYDATA Control Technologies (kurz MYDATA) ist eine technische Lösung für Datennutzungskontrolle des Fraunhofer IESE. MYDATA kann in Software integriert werden, um Datenflüsse entsprechend den konfigurierten Datennutzungsregeln zu kontrollieren. Im Kontext von WearPrivate haben wir uns für die Integration der technischen Lösung MYDATA entschieden. Für weitere Informationen, Hintergründe und Details zum Thema Datennutzungskontrolle und MYDATA verweisen wir auf [14].

Nachfolgend beschreiben wir konzeptionell die Integration und Positionierung der MYDATA-Komponenten im Gesamtsystem. Die wesentlichen Komponenten des Gesamtsystems, in denen Datennutzungskontrolle technisch verankert werden soll, sind:

1. das Wearable des Arbeitnehmers
2. die App auf dem Smartphone des Arbeitnehmers
3. das System des Analyseanbieters in der Cloud

Abbildung 4 stellt die wesentlichen Komponenten und Datenflüsse des Gesamtsystems dar sowie die darin integrierten MYDATA-Komponenten zur technischen Kontrolle der Datennutzungen. Gepunktete Linien bezeichnen Informationsflüsse; hierbei kennzeichnen Linien mit der Farbe Magenta die Informationsflüsse der besonders schützenswerten Gesundheitsdaten des Arbeitnehmers, über die wir ihm Kontrolle ermöglichen möchten, und Linien mit der Farbe Grün Informationsflüsse, die der Transparenz und Selbstbestimmung des Arbeitnehmers dienen.

Auf dem Wearable kann ein Policy Enforcement Point (PEP) integriert werden, der die Übertragung der vom Wearable erfassten Daten an das Smartphone kontrolliert. Weiterhin bedarf es eines Policy Decision Points (PDP), der die für das Wearable relevanten Richtlinien (Policies) auswertet, und eines Policy Management Points (PMP), der die für das Wearable relevanten Richtlinien technisch verwaltet.

Ähnlich sieht es für die App auf dem Smartphone des Arbeitnehmers aus. Auch hier werden PEP, PDP und PMP benötigt, um die Datennutzungen zu kontrollieren (z. B. die Übertragung von Daten an den Analysedienst). Zusätzlich gibt es hier einen Policy Administration Point (PAP) als Teil eines Privacy Dashboards. Mit dem PAP kann der Arbeitnehmer die Richtlinien festlegen, die im Gesamtsystem (also entlang der gesamten Verarbeitungskette) technisch durchgesetzt werden sollen. Beispielsweise kann er konfigurieren, dass das Wearable keine Bewegungsdaten an die App auf dem Smartphone übertragen soll, dass die App die Daten vor der Übertragung an den Analysedienst mittels Differential Privacy schützen soll und dass der Analysedienstleister diese ausschließlich zum Zwecke der individuellen Belastungsmessung, nicht jedoch für den Gruppenbericht verwenden soll.

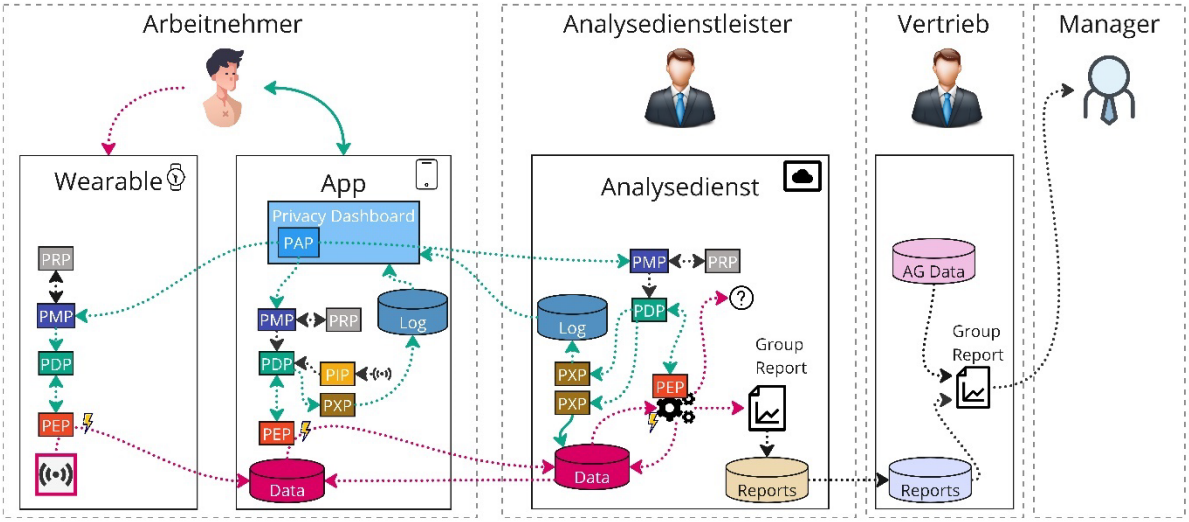

Abbildung 4 Integration und Positionierung der MYDATA-Komponenten im Gesamtsystem

Entsprechend interagiert der PAP mit den PMPs im System und stellt dort entsprechende Richtlinien bereit. Weitere Komponenten auf dem Smartphone des Arbeitnehmers können Policy Information Points (PIPs) und Policy Execution Points (PXPs) sein. Ein PIP kann beispielsweise Kontextinformationen für die Richtlinienauswertung bereitstellen. Ein Beispiel dafür ist die aktuelle GPS-Position des Smartphones. Mit dieser ließen sich dann beispielsweise Richtlinien mit Geo-Fences umsetzen (z. B. „Übertrage meine Daten nur, wenn ich mich auf dem Werksgelände befinde“). Ein PXP könnte beispielsweise Protokolleinträge anfertigen oder Mitteilungen versenden. PXPs werden durch den PDP entsprechend den Richtlinien angesteuert. Durch geeignete Richtlinien können damit Datennutzungen protokolliert werden. Diese Protokolle können im Privacy Dashboard dargestellt werden und dem Arbeitnehmer Einblick in die tatsächlich erfolgten Nutzungen seiner Daten geben.

Ähnlich sieht es im System des Analyseanbieters aus. Auch hier gibt es die Grundkomponenten PEP, PDP und PMP. PEPs werden an relevanten Stellen der Verarbeitungslogik im Analysedienst integriert, um dort die Datennutzungen technisch zu kontrollieren. So kann ein PEP beispielsweise die Verarbeitung der Gesundheitsdaten zum Zweck der individuellen Belastungsmessung zulassen, jedoch zum Beispiel eine Verwendung für den Gruppenbericht unterbinden. Neben einem PXP zur richtliniengesteuerten Protokollierung von Datennutzungen könnte ein weiterer PXP integriert werden, der die Gesundheitsdaten (z. B. historische Rohdaten oder Belastungsverläufe) löschen kann. Mit einem solchen PXP könnte der Arbeitnehmer beispielsweise eine regelmäßige Löschung seiner

Daten per Richtline vorschreiben, um eine ungewünscht lange Historienbildung durch den Analysedienst zu verhindern. Im konzipierten System kann der Arbeitnehmer frei entscheiden, ob seine Daten für den Gruppenbericht verwendet werden dürfen, und diese Entscheidung wird zum Zeitpunkt der Erstellung des Gruppenberichts technisch berücksichtig und durchgesetzt. Sobald ein Gruppenbericht erstellt wurde, kann ein Arbeitnehmer seine Entscheidung für den jeweiligen Gruppenbericht nicht mehr rückwirkend ändern, sondern nur mit Wirkung für die Zukunft und den nächsten Gruppenbericht, denn seine Daten wurden – entsprechend den zum Zeitpunkt der Gruppenberichterstellung gültigen Richtlinien – für die Erstellung des Berichts entweder verwendet oder nicht.

Die effektive Durchsetzung der Datennutzungskontrolle in den Komponenten der Systemkette erfordert eine korrekte Integration der Kontrollmechanismen an allen relevanten Stellen. Hierbei können – bewusst oder unbewusst – Fehler gemacht werden. Wiederkehrende Sicherheitskontrollen der Software und externe Reviews können dazu beitragen, die korrekte Integration der Kontrollmechanismen und deren Effektivität sicherzustellen.

6 Schutzmaßnahmen durch Datenaggregierung und -anonymisierung

Sowohl die Aggregation als auch Anonymisierung von Daten sollen im Kontext des Projekts WearPrivate darauf überprüft werden, ob sie spezifische Bedrohungen für die Privatheit der Nutzenden reduzieren können. Diese Bedrohungen sollen im Folgenden näher erläutert und darauf eingegangen werden, welche Maßnahmen und Entscheidungen dem Nutzer zu Gebote stehen, um sich vor ihnen zu schützen.

6.1 Bedrohungen

Auch wenn der Nutzer sich durch technische und organisatorische Maßnahmen im System anonym anmelden kann, so ermöglicht dies bloß eine Anonymität in der Kommunikation. Es ist nicht auszuschließen, dass die übermittelten Daten in sich ebenfalls eine Identifizierung des Nutzers ermöglichen und somit die Anonymität gefährden können. Aus der Analyse der möglichen Bedrohungen sind folgende zwei Bedrohungsbereiche als relevant hervorgegangen:

6.1.1 Datenleck

Beim Analysedienstanbieter oder dem Cloudanbieter kann es zu einem Datenleck kommen (T_AN15). Derartige IT-Sicherheitsvorfälle können aufgrund von mangelnden Sicherheitsvorkehrungen, aber auch ohne Eigenverschulden des Analysedienstanbieters auftreten, etwa aufgrund eines Zero-Day-Exploits oder fehlender Vorkehrungen auf Seiten des Cloudanbieters. Vor allem bei Cloudanbietern mit einem amerikanischen Mutterkonzern (wie etwa Amazon Web Services) besteht die Problematik, dass sie in bestimmten Fällen Daten gegenüber Behörden offenlegen müssen.

Als Folge eines Datenlecks kann es zum Verlust der Privatheit der Nutzer kommen (T_AN10, T_AN15), was die Offenlegung der Identität der Nutzer bedeuten kann. Vor allem in kleinen Nutzergruppen (T_AN5), die zu klein für einen Gruppenreport sind, sind die Chancen hoch, dass die Daten zu einer Identifizierung genutzt werden können – auch ohne weitere Hilfsmittel. Kann ein Nutzer identifiziert werden, so können ihm schlimmstenfalls (negative) betriebliche Konsequenzen drohen, falls der Arbeitgeber diese Identifizierung vornimmt und die gefundenen Informationen zum Arbeitsverhalten oder Gesundheitszustand eines Nutzers nicht seinen Wünschen entsprechen. Diese Gefahr der

Identifizierung erhöht sich zudem, wenn die derart offengelegten Daten mit anderen öffentlichen Daten zusammengeführt werden und so eine noch größere Menge an Personen identifiziert werden kann (T_AN4). Derartige öffentliche Daten können etwa durch das Teilen von Sportaktivitäten über eine Fitness-App, aber auch durch ein Datenleck bei Dritten entstehen.

Ein Datenleck auf Seiten des Analysedienstes (T_AS4) oder des Arbeitgebers (T_AG6) führt zu einem Reputationsschaden und einem Vertrauensverlust der Arbeitnehmer in den Dienst. Ein Datenleck von personenbezogenen Daten muss zudem nach Art. 34 DSGVO den betroffenen Personen mitgeteilt werden und kann – unter anderem für den Analysedienst – starke negative Folgen mit sich bringen, wie etwa den Verlust von Kunden oder Probleme, neue Kunden zu gewinnen. Daher wird die Bedrohung durch Datenlecks als äußerst relevant im Kontext von WearPrivate angesehen.

6.1.2 Vorsatz

Ein böswilliger Analysedienstleister könnte die Daten in Kombination mit weiteren Informationen, wie einem Datenleck bei einem Drittanbieter oder der Zusammenarbeit mit dem Arbeitgeber, nutzen, um Arbeitnehmer zu identifizieren (T_AN8). Zudem hat der Nutzer keine Garantie, dass Arbeitgeber und Analysedienstleister nicht kollusiv zusammenwirken. Die Konsequenzen daraus entsprechen denen, die bereits bzgl. eines Datenlecks beschrieben wurden. Ein Abmildern dieser Bedrohung kann das Vertrauen der Nutzer sowie auch anderer Stakeholder wie dem Betriebsrat erhöhen und zu mehr Akzeptanz führen. Die Bedrohung durch vorsätzliches Offenlegen persönlicher Daten wird im Kontext von WearPrivate ebenfalls als relevant angesehen, wobei jedoch die Problematik eines Datenlecks im Vordergrund bleibt.

6.2 Selbstbestimmung des Arbeitnehmers

Ein Teilziel der IT-Sicherheitsarchitektur ist es, die informationelle Selbstbestimmung der Nutzer – der Arbeitnehmer im Kontext von WearPrivate – in Bezug auf die beschriebenen Bedrohungen zu stärken und zu fördern. Den Nutzern soll es ermöglicht werden, informierte Entscheidungen über die Nutzung ihrer Daten zu treffen und so die potenzielle Gefahr durch die oben beschriebenen Bedrohungen zu reduzieren. Vor allem bei Dienstleistungen auf der Basis von Wearable-Daten, die größtenteils personenbezogene Daten darstellen, kann jedoch die Entscheidung, Daten nicht zur Verfügung zu stellen, zu einer Unmöglichkeit der Bereitstellung der Dienstleistungen führen.

Ein Ansatz, die Nutzung derartiger Dienste zu ermöglichen und gleichzeitig die personenbezogenen Daten der Nutzer zu schützen, liegt etwa in der Veränderung von Daten. Dies kann durch verschiedene Methoden erreicht werden, wie etwa Anonymisieren (R_AN11) oder Aggregieren (R_AN17). Derartige Veränderungen an den Daten können jedoch auch zu einem Verlust der Datenqualität führen, was wiederum eine verminderte Qualität einer Dienstleistung auf diesen Daten zur Folge haben kann. Da jedoch nicht pauschal für alle Nutzer im Vorhinein bestimmt werden kann, in welchem Grade sie einen Qualitätsverlust der Daten akzeptieren möchten, soll dem Nutzer im Projektkontext die Wahl selbst überlassen werden.

Anforderung 19 *Den Nutzern sollen drei verschiedene Varianten für die Übertragung ihrer Daten zu Verfügung stehen (R_AN11b):*

1. *Das **Versenden der unveränderten Rohdaten**. Dies bietet die höchste Datenqualität und damit zusammenhängend auch die höchste Genauigkeit des Analyse-Ergebnisses. In diesem Fall werden jedoch keine Schutzmaßnahmen für die Daten getroffen, um die identifizierten Bedrohungen zu mildern.*

2. *Das **Versenden von leicht geschützten Daten**. Durch Anonymisierungs- und Aggregationsmethoden sollen die versendeten Daten leicht verändert werden, um die Bedrohungen der Nutzer zu verringern. Dadurch wird die Datenqualität ein wenig verschlechtert, was zu Beeinträchtigungen der Genauigkeit der Analysen führen kann.*
3. *Das **Versenden von stark geschützten Daten**. Durch Anonymisierungs- und Aggregationsmethoden sollen die versendeten Daten derart verändert werden, dass sie die identifizierten Bedrohungen der Nutzer stark verringern. Dadurch wird die Datenqualität stärker als in Variante 2 beeinträchtigt, was zu einer weiteren Verschlechterung der Analysegenauigkeit führen kann.*

Bei der Entscheidung, welche dieser Schutzstufen die Nutzer wählen möchten, sollten die Nutzer jedoch möglichst unabhängig sein:

Anforderung 20 *Der Arbeitnehmer soll eine geschützte Verarbeitung seiner Daten wählen können, auch wenn diese einen Verlust der Qualität des Dienstes mit sich bringt. (R_AN11b)*

Sollten die Nutzer befürchten, dass die Nutzung einer bestimmten Schutzstufe oder eine komplette Ablehnung des Systems zu negativen Konsequenzen führen, könnten sie eine Einstellung wählen, die nicht ihren Wünschen entspricht, sondern etwa dem, was der Arbeitgeber oder andere Arbeitnehmer von ihnen erwarten. Um eine derartige Situation zu verhindern, soll im Projekt der Arbeitgeber zu keinem Zeitpunkt eine Information darüber erhalten, welche der oben aufgezeigten Varianten gewählt wurde.

6.3 Schutz der Daten

Um die Daten zu schützen, sollen Methoden der Anonymisierung oder Aggregation genutzt werden. Der Anwender tauscht mit dem Dienst im Kontext von WearPrivate im Grundsatz folgende Daten aus:

- **Angaben zum Nutzerprofil** (z. B. Geburtsjahr, Körpergröße, Gewicht, Geschlecht):
  Solche Informationen dienen dazu, die Analyse zu schärfen, denn die gemessenen Vitaldaten müssen je nach Nutzerprofil unterschiedlich interpretiert werden.
- **Wearable-Messdaten** (z. B. Vitaldaten, Beschleunigungswerte):
  Unter Umständen sind einzelne Vitaldaten wie etwa die Herzratenvariabilität sehr individuell und können ähnlich wie ein Fingerabdruck eindeutig einem bestimmten Individuum zugeordnet werden.[7] Sonstige Daten liefern nähere Informationen zum Kontext der Vitaldatenmessung, die womöglich ausreichen könnten, auf den Urheber zurückzuschließen.

6.3.1 Schutz der Profildaten

Um die Anonymität des Nutzers hinsichtlich seiner Profildaten zu stärken, sollen die Angaben im Nutzerprofil geschützt werden.

Anforderung 21 *Charakteristische Profildaten des Nutzers sollen vor einer Übermittlung an den Analysedienst verfremdet werden, um eine Identifizierung des Nutzers anhand der Profildaten zu erschweren. (R_AN11)*

[7] Inwieweit Vitaldaten ein charakteristisches individuelles Merkmal sind, muss in genaueren Untersuchungen noch ergründet werden. Wir treffen vorläufig die vorsichtige Annahme, dass eine Identifizierung anhand der Vitaldaten möglich ist, soweit keine weiteren Schutzvorkehrungen getroffen werden.

Ein dafür nutzbares Verfahren ist k-Anonymität [13] (nähere Erläuterungen zu k-Anonymität im Projektkontext sind in [14] zu finden). k-Anonymität verfolgt dabei den Gedanken, dass jeweils k Nutzer nicht in ihren identifizierenden Attributen unterscheidbar sein sollen. Folglich müssen diese Attribute angeglichen werden. Als Verfremdungsverfahren um diese Angleichung zu erreichen, kommen folgende Ansätze in Frage:

- **Generalisierung:** Statt eines genauen Wertes (z. B. Alter) wird nur eine generellere Attributklasse (z. B. 25 <= Alter < 35) übermittelt. Dazu sind folgende Spezialfälle ebenfalls denkbar:
  - **Prädikatbildung:** Auf dem Attributwert wird ein Prädikat angewendet (z. B. P(A) ::= A < 18). Anstelle des Attributwerts A wird nur der Prädikatwert {TRUE oder FALSE} an den Dienst übermittelt.
  - **Vorverarbeitung:** Mehrere Attribute werden bereits in der App miteinander verknüpft. Anstelle der individuellen Werte wird nur das Verknüpfungsergebnis an den Dienst übermittelt (z. B. anstelle von Köpergröße und Gewicht nur der Body-Mass-Index des Nutzers).
- **Unterdrückung:** Wenn einzelne Werte zu einer zu starken Verzerrung der Daten anderer Nutzer führen (Ausreißer) kann es sinnvoll sein, diese Daten zu entfernen. Das hat jedoch zur Folge, dass die besagte Person, deren Daten unterdrückt wurden, keine Analyseergebnisse erhalten kann.

Im Projekt WearPrivate empfehlen wir, eine k-Anonymität mit mindestens k=3 zu erreichen.

Anforderung 22 *Die Daten der Nutzer auf dem Smartphone sollen bereits so sehr verändert werden, dass mindestens drei Nutzer jeweils dieselbe Kombination aus Geburtsjahr, Geschlecht, Größe und Gewicht haben. (R_AN11)*

Da eine Unterdrückung von Daten dazu führen würde, dass betroffene Nutzer den Dienst nicht nutzen können, kommt für eine sinnvolle Umsetzung hier nur die Generalisierung der Nutzerdaten in vordefinierte Klassen in Frage. Die Definition dieser Klassen hängt stark von der vorhandenen Nutzerbasis ab und muss folglich dem Dienst überlassen werden: Würden im Vorhinein Klassen definiert werden, so könnte es passieren, dass die Nutzung dieser Klassen keine k-Anonymität bietet. Würde etwa das Geburtsjahr stets in zehn-Jahres-Spannen eingeteilt werden (Beispiel einer Klasse wäre die Jahresspanne »1990–1999«) und die Nutzerbasis aus einem Nutzer, der nach 2000 geboren wurde, und einer beliebigen Anzahl Nutzern bestehen, die vor 2000 geboren wurden, so würde k-Anonymität nicht erreicht werden. Auch die App kann die Definition der Klassen nicht durchführen, da sie keine gemeinsame Nutzerbasis des Dienstes verwaltet.

Eine Definition der Klassen durch den Dienst bringt jedoch die Frage mit sich, wie der Dienst diese Klassen definieren kann, ohne dass die Nutzer ihre personenbezogenen Daten ungeschützt offenlegen müssen. Daher ist eine Erstellung dieser Klassen durch die Nutzergruppe und ohne den Dienst zu empfehlen. Ein Vorschlag für ein Protokoll, welches diese Gruppen derart erstellen kann, ist im Zusatzdokument „Anonyme Erstellung von Nutzergruppen für k-Anonymität“ zu finden.

6.3.2 Schutz der Messdaten

Im Kontext des Projekts sollen verschiedene Messdaten erhoben werden. Diese Daten sollen möglichst wenige Rückschlüsse auf die Identität der Nutzer ermöglichen:

Anforderung 23 *Die gemessenen Rohdaten (Vital- und Kontextdaten) des Nutzers sollen vor einer Übermittlung an den Analysedienst verfremdet werden, um eine Identifizierung des Nutzers anhand der Rohdaten zu erschweren. (R_AN11)*

Im Folgenden sollen exemplarisch die Gefahren für die Privatsphäre, als auch die Schutzmöglichkeiten dieser Daten anhand von Beschleunigungs- und Herzratenvariabilitätsdaten analysiert werden.

6.3.2.1 Beschleunigungsdaten

Beschleunigungsmesser in Wearables und Smartphones messen in festen Zeitabständen die Bewegungen, die ein Gerät im dreidimensionalen Raum zurückgelegt hat. Zu jedem Zeitpunkt der Messung liegen dabei jeweils die Beschleunigung in x-, y- und z-Richtung vor, die seit dem vorherigen Messzeitpunkt festgestellt wurden. Beschleunigungsdaten ermöglichen etwa das Erkennen von Stürzen [4] oder auch der Gangart [8] und können daher für den Arbeitsschutz hilfreich sein.

Die Daten können jedoch auch zur eindeutigen Identifizierung von Arbeitnehmern genutzt werden und hierdurch Eingriffe in deren Privatsphäre begründen. Smartwatches etwa, die am Handgelenk getragen werden, ermöglichen es festzustellen, wann ihre Träger essen [15] oder rauchen [12] und geben somit detaillierte Auskünfte über ihr Verhalten. Unter anderem anhand der Gangart ist es zudem möglich zu bestimmen, ob [5] und wie viel [1] Alkohol ein Nutzer getrunken hat. Zudem lassen sich durch Beschleunigungsdaten von Geräten innerhalb eines Autos Schlüsse über den Fahrstil des Fahrers ziehen – etwa, ob er energisch [16] oder angetrunken fährt [3].

Auch Daten, die sich von Beschleunigungsdaten ableiten lassen, können eine Identifizierung von Personen ermöglichen: So hat sich gezeigt, dass Gangart [10] oder Kopfbewegungen [6] für Menschen derart eindeutig sind, dass sie eine klare Zuordnung zu einer Person ermöglichen. Über die Beschleunigungsdaten von Smartphones ist es zudem möglich, das Eintippen von Texten oder auch PINs über den Screen zu rekonstruieren [7].

Im Kontext des Projektes wurde evaluiert, ob es möglich ist, Bewegungsdaten derart zu schützen, sodass die Wahrscheinlichkeit einer Identifizierung von Personen reduziert, dabei jedoch gleichzeitig nicht die sinnvolle Nutzung der Daten zum Zwecke des Arbeitsschutzes verhindert wird. Eine exemplarische Analyse anhand des Anwendungsfalls der Sturzerkennung ist im Evaluationsbericht D6.1 zu finden. Daraus lässt sich die Empfehlung ableiten:

Anforderung 24 *Bewegungsdaten sollen mit Differential Privacy geschützt werden, wobei für den Parameter ε ein Wert unter 4 gewählt werden sollte. (R_AN11)*

Zu klären ist hier jedoch, ob Beschleunigungsdaten, die nach dieser Maßgabe geschützt worden sind, noch einen ausreichenden medizinischen Nutzen im Sinne des Gesundheits- oder Arbeitsschutzes haben, wie er im WearPrivate-Projekt angestrebt wird. Dies ist Gegenstand weiterer Evaluationen im Arbeitspaket 6 des Projekts.

6.3.2.2 Herzratenvariabilitätsdaten

Ähnlich wie Beschleunigungsdaten bergen auch Daten zur Herzratenvariabilität (HRV) einiges Potential, den Messvorgang eindeutig einer bestimmten Person zuzuordnen oder aus den Messdaten weitreichende Schlüsse über das persönliche Verhalten des Betroffenen zu ziehen. Idealerweise sollten daher auch HRV-Daten geeignet verfremdet werden (R_AN11), etwa nach dem in Anforderung 24 vorgeschlagenen Verfahren.

Auch hier ist jedoch unklar, inwieweit solche Verfremdungs- und Anonymisierungstechniken den Wert der gemessenen Daten beeinträchtigen. Gerade bei der Herzdatenvariabilität besteht der begründete Verdacht, dass selbst eine geringe Verfremdung zu deutlichen Fehlinterpretationen führen kann. Der

Grad solcher Beeinträchtigungen und der Spielraum, der aus medizinischer Sicht für Anonymisierungstechniken bleibt, soll im weiteren Projektverlauf noch genauer analysiert werden.

Quellenverzeichnis

[1] Z. Arnold, D. Larose and E. Agu (2015): Smartphone Inference of Alcohol Consumption Levels from Gait. International Conference on Healthcare Informatics, Dallas, TX, USA, 2015, pp. 417–426 https://doi.org/10.1109/ICHI.2015.59

[2] Bundesinstitut für Arzneimittel und Medizinprodukte (2022): Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz. https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.html

[3] J. Dai, J. Teng, X. Bai, Z. Shen and D. Xuan (2010): Mobile phone based drunk driving detection. 4th International Conference on Pervasive Computing Technologies for Healthcare, Munich, Germany, 2010, pp. 1–8 https://doi.org/10.4108/ICST.PERVASIVEHEALTH2010.8901

[4] Lim, Dongha & Park, Chulho & Kim, Nam & Kim, Sang-Hoon & Yu, Yun Seop (2014): Fall-Detection Algorithm Using 3-Axis Acceleration: Combination with Simple Threshold and Hidden Markov Model. Journal of Applied Mathematics. https://doi.org/10.1155/2014/896030

[5] J. Killian (2018): Smartphone-Based Intelligent System: Training AI to Track Sobriety Using Smartphone Motion Sensors. The Ohio State University

[6] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist and M. Gruteser (2016): Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), Sydney, NSW, Australia, pp. 1–9 https://doi.org/10.1109/PERCOM.2016.7456514

[7] Emmanuel Owusu, Jun Han, Sauvik Das, Adrian Perrig, and Joy Zhang (2012): ACCessory: password inference using accelerometers on smartphones. In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (HotMobile '12), Association for Computing Machinery, New York, NY, USA, Article 9, pp. 1–6 https://doi.org/10.1145/2162081.2162095

[8] A. Sant'Anna and N. Wickström (2010): A Symbol-Based Approach to Gait Analysis From Acceleration Signals: Identification and Detection of Gait Events and a New Measure of Gait Symmetry," in IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 5, pp. 1180-1187, Sept. 2010 https://doi.org/10.1109/TITB.2010.2047402

[9] S. Polst, B. Steffes, S. Salemi, P. Neuschwander, R. Schwarz (2024): Anforderungsdokument (Version 2.0). Ergebnisbericht D1.1, WearPrivate-Projekt

[10] A. Primo, V. V. Phoha, R. Kumar and A. Serwadda (2014): Context-Aware Active Authentication Using Smartphone Accelerometer Measurements. *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Columbus, OH, USA, pp. 98–105 https://doi.org/10.1109/CVPRW.2014.20

[11] Marco Eidinger (2023): iOS Jailbreak Detection in 2023. Blog-Artikel https://blog.eidinger.info/ios-jailbreak-detection-in-2023 (zuletzt abgerufen am 15. Februar 2023)

[12] Nazir Saleheen, Amin Ahsan Ali, Syed Monowar Hossain, Hillol Sarker, Soujanya Chatterjee, Benjamin Marlin, Emre Ertin, Mustafa al'Absi, and Santosh Kumar (2015): PuffMarker: a multi-sensor approach for pinpointing the timing of first lapse in smoking cessation. In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15). Association for Computing Machinery, New York, NY, USA, pp. 999–1010 https://doi.org/10.1145/2750858.2806897

[13] L. Sweeney (2002): k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), pp. 557–570

[14] M.-S. Schröder, B. Steffes, P. Neuschwander (2024): Konzepte für Anonymisierung und Datennutzungskontrolle. Ergebnisbericht D3.2, WearPrivate-Projekt

[15] Edison Thomaz, Irfan Essa, and Gregory D. Abowd (2015): A practical approach for recognizing eating moments with wrist-mounted inertial sensing. In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15). Association for Computing Machinery, New York, NY, USA, pp. 1029–1040 https://doi.org/10.1145/2750858.2807545

[16] R. Vaiana et al. (2014): Driving Behavior and Traffic Safety: An Acceleration-Based Safety Evaluation Procedure for Smartphones. Modern Applied Science, 8 (2014), pp. 88–96

[17] Simone Salemi (2024): Datenschutzbericht. Ergebnisbericht D 2.1, WearPrivate-Projekt

[18] Reinhard Schwarz (2024): D1.1_ Anforderungstabelle_final. Ergebnisbericht D1.1, WearPrivate-Projekt