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

Ergebnisbericht D2.2

Maßnahmenkatalog

Version	1.0 (final)
Datum	03.08.2022
Verfasser	Bianca Steffes (Universität des Saarlandes)
	Simone Salemi (Universität des Saarlandes)

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

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

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Ansprechperson

Prof. Dr. Christoph Sorge

Universität des Saarlandes Campus
Gebäude C 3.1
66123 Saarbrücken

Tel: +49 (0) 681 302 -5120
E-Mail: christoph.sorge@uni-saarland.de

Bianca Steffes, MSc.
Universität des Saarlandes Campus
Gebäude C 3.1 Raum 0.08
66123 Saarbrücken

Tel: +49 (0) 681 302 -4723
E-Mail: bianca.steffes@uni-saarland.de

Dip.-Jur. Simone Salemi
Universität des Saarlandes Campus
Gebäude C 3.1 Raum 0.30
66123 Saarbrücken

Tel: +49 (0) 681 302-4726
E-Mail: simone.salemi@zrd-saar.de

Inhaltsverzeichnis

1. Einleitung

Für die in D2.1 identifizierten Anforderungen werden Lösungsbausteine zusammengetragen und zum Teil im Projekt auch neu entwickelt, um diese Anforderungen technisch umzusetzen. Das Systemkonzept wird sich dieser Bausteine bedienen.

Im Deliverable 2.1 trägt die UdS die rechtlichen sowie sozialen und ethischen Anforderungen an die Umsetzungen im Projekt WearPrivate zusammen. Im ersten Sprint entstand insoweit ein Datenschutzbericht, in welchem die rechtlichen Besonderheiten und Herausforderungen des Projekts identifiziert und erläutert wurden. Aus diesen Ausführungen gehen Anforderungen hervor, die mit Hilfe technischer Lösungen zu erfüllen sind. Der vorliegende Maßnahmenkatalog dient dazu, die richtigen Lösungsmaßnahmen für gefundene Probleme zu identifizieren. Hierzu werden die rechtlichen sowie sozialen Herausforderungen aufgezeigt und beschrieben, wie die technischen Maßnahmen zur Lösung und Verbesserung beitragen können.

2. Sozialer Druck

2.1 Beschreibung

Da es im Projekt WearPrivate um den Wearable-Einsatz am Arbeitsplatz geht, sind insbesondere auch soziale Besonderheiten und Probleme zu betrachten. Das bestehende Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer kann einen Einfluss auf Entscheidungen des Arbeitnehmers haben.

So ist zu befürchten, dass manche Arbeitnehmer dem Einsatz eines Wearables am Arbeitsplatz nur aus Angst vor negativen Folgen zustimmen. Auch durch die Beteiligung vieler Kollegen kann beim Arbeitnehmer das Gefühl entstehen, er müsse ebenfalls teilnehmen, um einen negativen Eindruck zu vermeiden.

2.2 Rechtliche Anforderung

Das Ziel des Wearable-Einsatzes am Arbeitsplatz ist die Sammlung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO (siehe Deliverable 2.1). Wird die Datenverarbeitung auf eine Einwilligung, Art. 9 Abs. 2 lit. a DSGVO, gestützt, so ist eine essentielle materiell-rechtliche Voraussetzung der Einwilligung deren freiwillige Erteilung. Unter „Freiwilligkeit“ ist nur echte Wahlfreiheit zu verstehen, die nur dann vorliegt, wenn der betroffenen Person keine negativen Folgen bei Ablehnung der Einwilligung drohen. Einwilligungen, die im Rahmen des Arbeitsverhältnisses eingeholt werden, richten sich nach § 26 Abs. 2 BDSG. Aus § 26 Abs. 2 S. 1, 2 BDSG geht hervor, dass bei der Erteilung einer Einwilligung im Beschäftigungsverhältnis die Freiwilligkeit besonders im Fokus steht. Durch das Machtungleichgewicht und Abhängigkeitsverhältnis, das zwischen Arbeitgeber und Arbeitnehmer herrscht, kann die Freiwilligkeit des betroffenen Arbeitnehmers gehemmt sein. Daher schreibt § 26 Abs. 2 BDSG auch vor, dass alle Umstände des Einzelfalls bei der Bewertung der Freiwilligkeit zu beachten sind. Bei dieser Bewertung ist insbesondere der soziale Druck, der durch den Arbeitgeber oder auch die Arbeitskollegen ausgeübt werden kann, zu beachten.

2.3 Technische Maßnahme zur Umsetzung (M 1)

Abhilfe kann durch die Anonymisierung der Daten geschaffen werden. Auf diese Weise wird sichergestellt, dass der Arbeitgeber nicht direkt darüber informiert wird, wer welche gesundheitlichen Probleme hat. Gleichzeitig kann durch die Anonymisierung auch verschleiert werden, wer sich dagegen entschieden hat, das Wearable am Arbeitsplatz zu tragen. Eine weitere Möglichkeit ist es, unterschiedliche Grade der Anonymisierung zu nutzen.

Baustein B 1, B 2 und B 3:

3. Forschungszwecke

3.1 Beschreibung der Anforderung

Im Rahmen eines Forschungsprojektes werden auch Daten zur Evaluierung der gefundenen Lösungen erhoben. Bevor Endergebnisse publiziert werden, werden Studien, Nutzerbefragungen und Tests durchgeführt, mittels derer man zum bestmöglichen Ergebnis gelangen will. Bei der Evaluierung können auch personenbezogene Daten erhoben werden.

3.2 Rechtliche Besonderheiten

Art. 89 DSGVO regelt Garantien und Ausnahmen bei Verarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken. Gemäß Art. 89 Abs. 1 DSGVO sind bei der Verarbeitung zu den genannten Zwecken technische und organisatorische Maßnahmen zu ergreifen, um die Grundsätze der DSGVO umzusetzen. Mit § 27 BDSG hat der deutsche Gesetzgeber ferner eine eigene Regelung auf Bundesebene geschaffen, die die Verarbeitung von Daten zu Forschungszwecken genauer regelt. Da für Landesuniversitäten (auch die UdS) die jeweiligen Landesdatenschutzgesetze einschlägig sind, ist vorrangig vor § 27 BDSG das saarländische Landesdatenschutzgesetz (SDSG) zu betrachten. § 23 SDSG behandelt die Datenverarbeitung zu Forschungszwecken. Laut § 23 Abs. 1 S. 1 SDSG ist die Verarbeitung insbesondere möglich, wenn der Zweck der Forschung auf **andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann**, und wenn das öffentliche, insbesondere das wissenschaftliche oder historische Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person am Unterbleiben der Verarbeitung **erheblich überwiegt**. Die Erforderlichkeit der Datenerhebung kann dann verneint werden, wenn auch die Erhebung von Daten in anonymer Form möglich gewesen wäre. Daher sind die Daten, die zu Forschungszwecken erhoben werden müssen, möglichst in anonymisierter Form zu verarbeiten.

3.3 Technische Maßnahme zur Umsetzung (M 2)

An dieser Stelle können die erarbeiteten Anonymisierungskonzepte relevant werden. Die Anonymisierung kann auch in unterschiedlichen Stärkegraden ausgeführt werden. Zudem sollten grundlegende Maßnahmen der IT-Sicherheit angewendet werden, die die Daten schon bspw. bei der Anonymisierung schützen.

Baustein B 1, B 2, B 3 und B 4:

4. Weitergabe von Daten an Dritte

4.1 Beschreibung der Anforderung

Personenbezogene Daten können nicht ohne Rechtsgrundlage an Dritte weitergegeben werden. Dritte sind im Sinne der DSGVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten, Art. 4 Nr. 10 DSGVO. Im Rahmen des Projektes WearPrivate ist die Weitergabe von den mittels Wearables erhobenen Daten denkbar und unter Umständen sogar erforderlich.

4.2 Rechtliche Besonderheiten

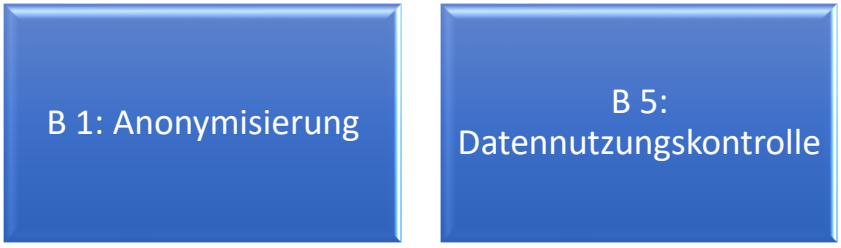
Die Offenlegung von Daten durch die Übermittlung gehört nach Art. 4 Nr. 2 DSGVO zu den Verarbeitungsarten der DSGVO. Ohne Rechtsgrundlage ist die Übermittlung von Daten an Dritte daher nicht erlaubt.

4.3 Technische Maßnahmen zur Umsetzung (M 3)

Auf anonyme oder anonymisierte Daten finden die DSGVO keine Anwendung.[1] Die Übermittlung anonymer/anonymisierte Daten erfordert mithin nicht zwangsläufig eine Rechtsgrundlage. Zudem kann den Mitarbeitern eine Entscheidungsmöglichkeit gegeben werden, ob und welche Daten an wen weitergeleitet werden sollen.

[1] Siehe hierzu D 2.1, Erwägungsgrund 26 zur DSGVO.

Baustein B 1 und B 5:



5. Klassische IT-Sicherheit

5.1 Beschreibung der Anforderung

Bei der Nutzung von digitalen Diensten und Software besteht stets die Gefahr eines Programmfehlers oder einer Sicherheitslücke. Werden etwa Daten in ihrer Verarbeitung nicht geschützt oder durch bei der Speicherung unzureichend abgesichert, können sie von Dritten abgefangen oder ausgelesen werden. Zudem können über die Zeit hinweg in genutzten Software-Bibliotheken oder hardwareeigener Software neue Sicherheitslücken auftauchen. Eine solche Gefahr wird zwar nicht unmittelbar vom Hersteller einer App oder anderer Software erzeugt, es obliegt ihm jedoch die Pflicht, entsprechende Softwareupdates und Patches einzubinden.

5.2 Rechtliche Besonderheiten

Aus Art. 32 DSGVO geht hervor, dass die Sicherheit der Verarbeitung von personenbezogenen Daten zu gewährleisten ist. Unter Berücksichtigung des Risikos für die Rechte der betroffenen Personen sind technische und organisatorische Maßnahmen zu ergreifen. In Art. 32 Abs. 1 lit. a – d DSGVO werden beispielhaft Maßnahmen wie die Verschlüsselung oder Pseudonymisierung von Daten (lit. a) aufgezählt, die in Betracht kommen. Damit sollen die Schutzziele der IT-Sicherheit eingehalten werden.

5.3 Technische Maßnahmen zur Umsetzung (M 4)

Die Schutzziele der IT-Sicherheit (Authentizität, Vertraulichkeit, Integrität, Verfügbarkeit) können durch verschiedene Schutzmaßnahmen erreicht werden. Bei der Konzeption, Erstellung und dem Betrieb von Anwendungen wie Apps oder anderer Software sollte darauf geachtet werden, Datenschutz und IT-Sicherheit von Beginn an einzuplanen. Zudem können externe Reviews des Codes und der technischen und organisatorischen Maßnahmen mit möglichen Zertifikaten des erreichten Schutzniveaus durchgeführt werden oder der Code öffentlich als Open-Source-Projekt zur Verfügung gestellt werden. Ein IT-Sicherheitskonzept sollte auch einen festgelegten Prozess beinhalten, wie auf einen Sicherheitsbruch reagiert werden muss und wie die Software regelmäßig auf ein fortbestehendes Sicherheitsniveau überprüft werden kann.

Bausteine B 1, B 4, B 6, B 7, B 8 und B 9:

6. Rückmeldung an den Arbeitgeber

6.1 Beschreibung der Anforderung

Geplant ist, dass der Arbeitgeber eine Rückmeldung hinsichtlich der aufgezeichneten Daten erhält, um entsprechend darauf reagieren zu können. Es gibt verschiedene Möglichkeiten, wie diese Rückmeldung aussehen könnte.

Gruppe

Der Arbeitgeber könnte eine Rückmeldung über eine Gruppe von Arbeitnehmern erhalten. Er erhält in diesem Fall einen Gruppenwert und kann daher einzelne Werte der Arbeitnehmer nicht abstrahieren.

Einzelpersonen ohne Zuordnung zu den realen Personen

Der Arbeitgeber könnte auch eine Rückmeldung über die Daten von Einzelpersonen erhalten, ohne dass er wissen kann, wer diese Einzelperson ist.

6.2 Rechtliche Besonderheiten

Die Erhebung von Daten im Beschäftigungsverhältnis wird in § 26 BDSG geregelt. Soweit keine Einwilligung der Arbeitnehmer nach § 26 Abs. 2 BDSG eingeholt wird, kann die Verarbeitung sensibler personenbezogener Daten auch dann gerechtfertigt werden, wenn die Verarbeitung zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt, § 26 Abs. 3 S. 1 BDSG. Im Rahmen einer Verhältnismäßigkeitsprüfung werden die betroffenen Interessen gegeneinander abgewogen und in einen angemessenen Ausgleich gebracht. In der Abwägung sind sämtliche Umstände des Einzelfalls miteinzubeziehen, wie etwa das Abhängigkeitsverhältnis, das zwischen Arbeitgeber und Arbeitnehmer herrscht. Grundsätzlich ist

immer das mildeste aller gleichgeeigneten Mittel zu wählen, um ein Ziel zu erreichen. Gerade was die Rückmeldung der Daten an den Arbeitgeber angeht, ist daher zu prüfen, wie detailliert diese sein muss. Können die durch den Wearable-Einsatz angestrebten Ziele auch durch einen Gruppenwert oder anonymisierte Daten erreicht werden, ist die Erforderlichkeit der Rückmeldung besonders detaillierter Daten zu verneinen.

6.3 Technische Maßnahmen zur Umsetzung (M 5)

Das Erstellen von Ergebnissen für eine Gruppe an Personen lässt sich über das Aggregieren erreichen. Dabei sind jedoch nur bestimmte Aggregatfunktionen (etwa Minimum, Maximum, Median, etc.) möglich. Die Aggregation kann dabei über einen vertrauenswürdigen Dritten (Trusted Third Party) oder in einer geheimen Berechnung zwischen den Mitarbeitern stattfinden. Eine Rückmeldung an den Arbeitgeber, ohne einen Rückschluss auf die sendende Person zu erhalten, lässt sich durch Methoden der anonymisierten Kommunikation erreichen.

Bausteine B 1, B 10 und B 11:

7. Wahl des Schutzgrades

7.1 Beschreibung der Anforderung und rechtliche Besonderheiten

Eines der wesentlichen Ziele des Projektes WearPrivate ist die Erhaltung der Selbstbestimmung der Arbeitnehmer bei der Datenerhebung durch Wearables. Dieses Ziel wird bestenfalls erreicht, wenn dem Arbeitnehmer größtmögliche Freiheiten bei der Auswahl der Umstände der Datenverarbeitung gewährt werden.

7.2 Technische Maßnahme zur Umsetzung

Methoden des technischen Datenschutzes können durch Parametrisierung ein unterschiedliches Schutzniveau anbieten. Die Parametrisierung von Anonymisierungsmethoden erlaubt es, die Wahrscheinlichkeit, dass die zugehörige Anonymisierung gebrochen werden kann, zu erhöhen oder zu reduzieren.
Mit sinkender Wahrscheinlichkeit des Brechens der Anonymisierung sinkt jedoch zumeist auch der Informationsgehalt und die Nutzbarkeit der Daten. In Kombination mit der Komplexität der Anonymisierungsmethode (etwa auf Grundlage von Differential Privacy) ist die Wahl des optimalen Parameters daher selten trivial. Zudem können unterschiedliche Methoden des Schutzes grundlegend bereits einen unterschiedlich hohen Grad an Sicherheit mit sich bringen. Die angebotenen

Möglichkeiten für den Arbeitnehmer, seine Daten zu schützen, können auch für den Arbeitnehmer nach Schutzniveau gruppiert werden und ihm somit eine leichtere Wahl des Schutzgrades ermöglichen.

Bausteine B 2 und B 3:

8. Sammlung der Bausteine