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

Ergebnisbericht D2.1

Bericht über ethische, rechtliche und soziale Implikationen der Projektergebnisse

Version	5.0
Datum	30.11.2024
Verfasser	Simone Salemi

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

Ansprechpersonen

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

Ajla Hajric, B.Sc.
Universität des Saarlandes Campus
Gebäude C 3.1 Raum 1.24
66123 Saarbrücken

Tel: +49 (0) 681 302 -4723
E-Mail: ajla.hajric@zrd-saar.de

Dip.-Jur. Simone Salemi, LL.M.
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

Liste der Abkürzungen ..... **vii**

1 Einleitung und Überblick **1**

2 Anwendungsfall des Projekts **1**

3 Einschlägige Gesetzestexte **1**

3.1 Europäisches Recht 1

3.1.1 Datenschutzgrundverordnung 2

3.1.2 ePrivacy-Richtlinie 5

3.1.3 Data Act 6

3.1.4 European Health Data Space 7

3.2 Nationales Recht 10

3.2.1 Bundesdatenschutzgesetz 10

3.2.2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz 11

3.2.3 Landesdatenschutzgesetze 12

3.3 Anwendbarkeit der Gesetze bei Gewährleistung von Anonymität 13

3.3.1 Formale Anonymität 13

3.3.2 Faktische Anonymität 13

3.3.3 Absolute Anonymität 14

3.3.4 Bedeutung für das Datenschutzrecht 14

3.3.5 Anwendung auf WearPrivate 15

3.3.6 Gefährdung der Anonymität durch die Zusammenführung von Daten 18

3.3.7 Gefährdung der Anonymität durch die Übermittlung von gerätespezifischen Informationen 18

4 Rechtsgrundlagen für die Verarbeitung von Wearable-Daten **20**

4.1 Einwilligung 20

4.1.1 Erforderlichkeit einer Einwilligung aufgrund der ePrivacy-Richtlinie 21

4.1.2 Einwilligung nach der DSGVO und dem BDSG 26

4.1.3 Einwilligung in die Verarbeitung besonders sensibler Daten nach Art. 9 Abs. 2 lit. a DSGVO 30

4.1.4 Einwilligungen in die Verarbeitung besonders sensibler Daten im Beschäftigtenkontext nach § 26 Abs. 3 S. 2, Abs. 2 BDSG 31

4.1.5 Anwendung auf WearPrivate 37

4.2 Verarbeitung sensibler Daten zum Zwecke des Beschäftigungsverhältnisses (§ 26 Abs. 3 S. 1 BDSG) 38

4.2.1 Anwendung auf WearPrivate 39

4.3 Verarbeitung sensibler Daten zum Zwecke der Versorgung im Gesundheitsbereich (Art. 9 Abs. 2 lit. h DSGVO) ... 43
4.4 Weitere Rechtsgrundlagen nach Art. 6 Abs. 1 lit. b-f DSGVO ... 44

5 Informationspflichten und Transparenzgebot ... 44
5.1 Transparenzgebot und Informationspflichten ... 45
5.1.1 Transparenzanforderungen, Art. 12 DSGVO ... 45
5.1.2 Informationspflichten, Art. 13 und Art. 14 DSGVO ... 45
5.2 UI-Design-Anforderungen ... 47
5.2.1 Umfang ... 49
5.2.2 Komplexität ... 49
5.2.3 Visualisierung/Veranschaulichung ... 50
5.2.4 Selbstbestimmungseinstellungen ... 50
5.2.5 Zugang zur Datenschutzerklärung ... 51
5.2.6 Zertifikate ... 51
5.2.7 Fazit ... 51

6 Betroffenenrechte ... 52
6.1 Recht auf Auskunft, Art. 15 DSGVO ... 52
6.2 Recht auf Berichtigung, Art. 16 DSGVO ... 52
6.3 Recht auf Löschung, Art. 17 DSGVO ... 53
6.4 Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO ... 55
6.5 Mitteilungspflicht, Art. 19 DSGVOf ... 56
6.6 Recht auf Datenübertragbarkeit, Art. 20 DSGVO ... 56
6.7 Widerspruchsrecht, Art. 21 DSGVO ... 57
6.8 Automatisierte Entscheidungen im Einzelfall, insbesondere Profiling, Art. 22 DSGVO ... 58
6.9 Rechtliche Besonderheiten im IoT-Bereich ... 59
6.9.1 Sozialer Druck ... 60

7 Datenschutzrechtliche Verantwortlichkeit ... 61
7.1 Pflichten des Verantwortlichen ... 61
7.1.1 Datenschutzerklärung ... 61
7.1.2 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art. 12 DSGVO ... 62
7.1.3 Informationspflicht, Art. 13 DSGVO ... 62
7.1.4 Informationspflicht, Art. 14 DSGVO ... 63
7.1.5 Betroffenenrechte ... 63
7.1.6 Sicherstellung geeigneter technischer und organisatorischer Maßnahmen zum Datenschutz und Sicherheit der Verarbeitung ... 63
7.1.7 Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO ... 63
7.1.8 Meldung von Verletzungen des Schutzes personenbezogener Daten, Art. 33, 34 DSGVO ... 64

7.1.9 Datenschutz-Folgenabschätzung, Art. 35 DSGVO ... 65
7.1.10 Benennung eines Datenschutzbeauftragten, Art. 37 DSGVO ... 66
7.1.11 Drittlandsübermittlung, Art. 44 ff. DSGVO ... 67
7.2 Gemeinsame Verantwortlichkeit ... 67
7.3 Auftragsverarbeitung ... 68
7.3.1 Pflichten des Auftragsverarbeiters ... 70
7.4 Verantwortlichkeit im Projekt WearPrivate ... 70
7.4.1 Arbeitgeber ... 71
7.4.2 Analyseservice ... 71
7.4.3 App-Anbieter ... 72
7.4.4 Cloudservice ... 72

8 Übermittlung von personenbezogenen Daten in Drittländer ... 73
8.1 Anwendung auf WearPrivate ... 77

9 Technische und organisatorische Maßnahmen nach der DSGVO ... 77
9.1 Privacy by Design, Art. 25 Abs. 1 DSGVO ... 78
9.2 Privacy by Default, Art. 25 Abs. 2 DSGVO ... 78
9.3 Sicherheit der Verarbeitung, Art. 32 DSGVO ... 78
9.3.1 Angemessenes Schutzniveau ... 80
9.4 Überblick über die technischen und organisatorischen Maßnahmen ... 81
9.4.1 DSGVO ... 81
9.4.2 TDDDG ... 84
9.5 Anwendung auf WearPrivate ... 84
9.5.1 Analyseservice ... 86
9.5.2 Arbeitgeber ... 87

10 Datenverarbeitung zu wissenschaftlichen Forschungszwecken ... 87
10.1 Anwendung auf WearPrivate ... 90

11 ePrivacy-Aspekte: Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz ... 90
11.1 Anwendbarkeit des TDDDG ... 90
11.1.1 Anbieter von digitalen Diensten ... 91
11.1.2 Pflichten des Anbieters von digitalen Diensten ... 91

12 Auswirkungen des Data Act und des EHDS ... 95
12.1 Data Act ... 96
12.2 EHDS ... 96
12.2.1 Zugangsanspruch nach dem Data Act ... 96

13 Zusammenfassung der rechtlichen Anforderungen ... 97
13.1 Anforderungen bei Erhebung einer Einwilligung ... 97
13.2 Anforderungen bei einer Datenerhebung zum Zwecke des Beschäftigungsverhältnisses ... 97

13.3 Anforderungen an den Verantwortlichen 98
13.4 Anforderungen bei gemeinsamer Verantwortlichkeit 98
13.5 Anforderungen bei Datenübermittlungen in Drittländer 98
13.6 Anforderungen an die Datenerhebung zu Forschungszwecken 98

Anlage – Fragenkatalog zur Ermittlung der datenschutzrechtlichen Verantwortlichkeit des Analysedienstes (WearHealth) und des App-Entwicklers (Neusta) 99
A-1 WearHealth 102
A-2 Neusta 104

Quellenverzeichnis 108

Liste der Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftrage für den Datenschutz und die Informationssicherheit
DSGVO	Datenschutzgrundverordnung
EHDS	European Health Data Space
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
GG	Grundgesetz
GRCH	Grundrechtecharta
GRUR-RS	Gewerblicher Rechtsschutz und Urheberrecht – Rechtsprechung (Zeitschrift)
IoT	Internet of Things
NJW	Neue juristische Wochenschrift
SGB	Sozialgesetzbuch
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
ZD	Zeitschrift für Datenschutz

1 Einleitung und Überblick

Die rechtlichen Fragestellungen, die im Rahmen des Projekts WearPrivate adressiert werden, sind größtenteils im deutschen und europäischen Datenschutzrecht angesiedelt.

Geht es um die Verarbeitung personenbezogener Daten, sind Grundrechte auf unionsrechtlicher sowie auf nationaler Ebene betroffen. Konkret geht es um das allgemeine Persönlichkeitsrecht, welches das Recht auf informationelle Selbstbestimmung beinhaltet (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG), um das Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRCH) und das Recht auf den Schutz personenbezogener Daten (Art. 8 GRCH). Die Datenschutzgrundverordnung und das deutsche Bundesdatenschutzgesetz konkretisieren die Anforderungen an die Datenschutzkonformität und stecken die Rahmenbedingungen für eine grundrechtskonforme Datenverarbeitung ab. Daneben existieren auch noch weitere Gesetze, die im Rahmen des Projekts wichtig werden könnten, wie beispielsweise das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz oder weitere EU-Verordnungen.

2 Anwendungsfall des Projekts

Nachdem sich die Partner während des zweiten Sprints auf einen Anwendungsfall geeinigt haben, kann die rechtliche Beurteilung auf dessen Besonderheiten angepasst werden. Der nun festgelegte Anwendungsfall betrifft die Analyse der kognitiven und physischen Belastung von Arbeitnehmern, die in besonders risikobehafteten Bereichen arbeiten. Bei zu hoher Belastung wird eine Mitteilung an den Arbeitnehmer gesendet, die ihn auf eine mögliche Gesundheitsgefahr aufmerksam macht. Der Arbeitnehmer entscheidet an diesem Punkt selbstbestimmt, wie er nun vorgeht.

Bei der Arbeit an Hochspannungsleitungen sollen Wearables Gesundheitsrisiken minimieren und vor Arbeitsunfällen schützen.

3 Einschlägige Gesetzestexte

Im ersten Schritt ist zu prüfen, welche Gesetze im vorliegenden Fall anwendbar sind.

3.1 Europäisches Recht

Aufgrund des Anwendungsvorrangs des Unionsrechts werden zunächst rechtliche Regelungen auf Ebene des Unionsrechts betrachtet.

3.1.1 Datenschutzgrundverordnung

Die Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung, DSGVO) ist seit dem 25.05.2018 anwendbar. Es handelt sich um eine Verordnung im Sinne des Art. 288 UAbs. 2 AEUV, sie gilt daher unmittelbar in jedem Mitgliedstaat und es bedarf keiner Umsetzung in nationales Recht. Ferner genießt sie als Sekundärrecht der Europäischen Union Anwendungsvorrang vor nationalem Recht.[1]

Der Anwendungsbereich der DSGVO ist in den Art. 2 und 3 DSGVO geregelt.

3.1.1.1 Örtlicher Anwendungsbereich

Der räumliche Anwendungsbereich ist in Art. 3 DSGVO geregelt. Aus Art. 3 DSGVO ergeben sich zwei Prinzipien für die Eröffnung des Anwendungsbereiches der DSGVO. In Art. 3 Abs. 1 DSGVO wird das *Niederlassungsprinzip* normiert. Demnach ist die DSGVO anwendbar, soweit die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Über eine Niederlassung verfügt ein Unternehmen, soweit eine effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung vorliegt.[2] Aus Erwägungsgrund 22 S. 3 zur DSGVO geht hervor, dass die Rechtsform der Einrichtung unerheblich ist.

In Art. 3 Abs. 2 DSGVO ist zudem das *Marktortprinzip* normiert.[3] Demnach kann die DSGVO auch Anwendung auf die Verarbeitung personenbezogener Daten finden, wenn der Verantwortliche bzw. der Auftragsverarbeiter nicht über eine Niederlassung innerhalb der Union verfügt. Voraussetzung hierfür ist jedoch, dass sich die von der Verarbeitung betroffenen Personen innerhalb der Union befinden und die Datenverarbeitung entweder im Zusammenhang damit steht, diesen betroffenen Personen Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist (Art. 3 Abs. 2 lit. a DSGVO) oder damit, das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt (Art. 3 Abs. 2 lit. b DSGVO).

---

[1] W. SCHROEDER in: Streinz AEUV/EUV, Art. 288 AEUV, Rn. 44.

[2] ERNST in: Paal/Pauly, Art. 3 DSGVO Rn. 7.

[3] SCHMIDT in: Taeger/Gabel, Art. 3 DSGVO Rn. 16.

3.1.1.2 Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich der DSGVO ist in Art. 2 DSGVO geregelt. Nach Art. 2 Abs. 1 DSGVO gilt sie für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die Begriffe der „personenbezogenen Daten“ sowie der „Verarbeitung“ sind jeweils in Art. 4 DSGVO definiert. Nach Art. 4 Nr. 1 DSGVO sind **personenbezogene Daten** solche Informationen, die sich auf identifizierte oder zumindest identifizierbare Personen beziehen. Identifiziert ist eine Person, soweit sich ihre Identität direkt aus der Information ergibt.[4] Identifizierbar ist eine Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Identifizierbarkeit liegt mithin vor, wenn eine Person erst durch die Verknüpfung mehrerer Informationen identifiziert werden kann.[5] Aus Erwägungsgrund 26 zur DSGVO geht hervor, dass bei der Frage, ob eine Person als identifizierbar anzusehen ist, alle Mittel zu berücksichtigen sind, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden (S. 3). Dabei werden alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (S. 4). Mithin ist der Begriff der Identifizierbarkeit weit auszulegen.

Weiterhin muss eine **Verarbeitung** personenbezogener Daten vorliegen. Nach Art. 4 Nr. 2 DSGVO ist eine Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

In Art. 2 Abs. 2 DSGVO sind indes vier Ausnahmen vom Anwendungsbereich der DSGVO normiert. Die DSGVO ist demnach nicht anwendbar, wenn die Datenverarbeitung

---

[4] KLAR/KÜHLING in: Kühling/Buchner, Art. 4 Nr. 1 DSGVO Rn. 18.

[5] HERMANN/MÜHLENBECK/SCHWARTMANN in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 4 DSGVO, Rn. 33.

- im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, stattfindet (lit. a)
- durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV, durchgeführt wird (lit. b)
- durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, durchgeführt wird (lit. c, Haushaltsausnahme)
- durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit durchgeführt wird (lit. d).

3.1.1.3 Anwendung auf WearPrivate

Der Anwendungsbereich der DSGVO müsste auch für das Projekt WearPrivate eröffnet sein.

In örtlicher Hinsicht ist der Anwendungsbereich eröffnet. Die Erhebung der Wearable-Daten erfolgt innerhalb von Deutschland. Damit ist die DSGVO in räumlicher Hinsicht anwendbar.

Fraglich ist, ob vorliegend personenbezogene Daten erhoben werden. Eingesetzt wird ein Wearable, über welches insbesondere die Herzratenvariabilität (HRV) und Beschleunigungsdaten (ACC) erhoben werden und an die auf dem Smartphone installierte App übermittelt, welche ihrerseits eine Reihe an „Stammdaten“ des Nutzers speichert, wozu Größe, Gewicht, Geschlecht und Geburtsjahr gehören. Die Angabe dieser Daten ist essentiell, um den Analyseservice zu nutzen. Um die durch das Wearable generierten Daten (HRV und ACC) richtig interpretieren zu können, ist es erforderlich, über einige Informationen zur betroffenen Person und deren Körperwerten zu verfügen.

Im Folgenden übermittelt die App die Daten an den Analyseservice, welcher die gesammelten Rohdaten verarbeitet und das daraus resultierende Feedback an den Arbeitgeber sendet. Diese Daten sind jedoch nur als personenbezogen zu klassifizieren, wenn sie die Identifikation der betroffenen Person ermöglichen. Die Stammdaten (Größe, Geburtsjahr, Gewicht, Geschlecht), die in der App gesammelt werden, können die Identität des Nutzers preisgeben. Insbesondere wenn in einer Analysegruppe, also einer Arbeitsgruppe, nur eine Frau arbeitet oder nur eine Person mit einer auffälligen Größe, so ist diese schnell und unkompliziert identifiziert. Daher handelt es sich hierbei um personenbezogene Daten im Sinne der DSGVO. Ferner zeigen erste Untersuchungen der Universität des Saarlandes, dass die Identifizierung von Personen aus der Herzratenvariabilität möglich ist. Der Aufwand, der zu betreiben ist, um eine Person zu identifizieren, beschränkt sich auf einen geringen Zeitaufwand. Mit nur wenig Internet-Recherche konnte eine relativ einfach umzusetzende Möglichkeit zur Identifizierung gefunden werden. Ähnliches gilt für die Beschleunigungsdaten. Dies spricht dafür,

dass man auch ohne Verknüpfung mit weiteren Daten aus der App bei der Herzratenvariabilität von personenbezogenen Daten sprechen kann.

3.1.2 ePrivacy-Richtlinie

Neben der Datenschutzgrundverordnung könnte auch die Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ePrivacy-Richtlinie) für das Projekt relevant sein. Es handelt sich um eine Richtlinie im Sinne des Art. 288 UAbs. 3 AEUV, weshalb eine Umsetzung in mitgliedstaatliches Recht erforderlich ist.[6] Die Richtlinie schafft im Gegensatz zur Verordnung kein unmittelbar anwendbares Recht in jedem Mitgliedstaat.[7] Die ePrivacy-Richtlinie soll in absehbarer Zeit durch eine ePrivacy-Verordnung[8] ersetzt werden, diese ist derzeit allerdings noch nicht in Kraft getreten.[9] Die Regelungen der ePrivacy-Richtlinie hat der deutsche Gesetzgeber im Telekommunikationsgesetz sowie im Telekommunikations-Telemedien-Datenschutz-Gesetz (mittlerweile: Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz) umgesetzt.[10]

Ziel der ePrivacy-Richtlinie ist gemäß Art. 1 Abs. 1 ePrivacy-RL die Harmonisierung der Vorschriften der Mitgliedstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten. Da sowohl die DSGVO als auch die ePrivacy-Richtlinie die Verarbeitung personenbezogener Daten betreffen können, stehen beide Regelungen in einem Konkurrenzverhältnis. Das Verhältnis beider EU-Rechtsetzungsakte wird in Art. 95 DSGVO näher spezifiziert. Dieser löst den Konflikt zwischen beiden im Wege gesetzlicher Spezialität.[11] Demnach

---

[6] RUFFERT in: Calliess/Ruffert, Art. 288 AEUV Rn. 24.

[7] NETTESHEIM in: Grabitz/Hilf/Nettesheim, Art. 288 AEUV Rn. 104.

[8] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010.

[9] Stand: 30.11.2024.

[10] https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/ePrivacy_Verordnung.html, zuletzt abgerufen am 30.11.2024.

[11] SYDOW in: Sydow/Marsch, Art. 95 DSGVO Rn. 1.

enthält die ePrivacy-Richtlinie für Fragen des Datenschutzes bei der elektronischen Kommunikation die spezielleren und damit auch vorrangig anwendbaren Vorschriften, soweit die speziellen Regelungen der Richtlinie dieselbe Zielrichtung wie die DSGVO-Regelungen verfolgen.[12] Die DSGVO kann allerdings subsidiär dort zur Anwendung kommen, wo die ePrivacy-Richtlinie keine abschließende Regelung enthält.[13] Zum Verhältnis zum Data Act (DA, siehe hierzu Kapitel 3.1.3) gilt Art. 1 Abs. 5 des DA, der erklärt, dass der Data Act die Regelungen der ePivacy-Richtlinie ebenso wie die der DSGVO unberührt lasse.

3.1.2.1 Anwendung auf WearPrivate

Da die Regelungen der ePrivacy-Richtlinie aufgrund ihrer Rechtsnatur als nicht unmittelbar anwendbare Richtlinie erst umgesetzt werden müssen, sind für das Projekt WearPrivate insbesondere die Regelungen der Gesetze relevant, die die ePrivacy-Richtlinie in deutsches Recht umsetzen. Hierzu gehören das TKG und insbesondere das TDDDG (siehe zum Anwendungsbereich des TDDDG Kapitel 3.2.2).

Aufgrund der Tatsache, dass im Projekt Informationen auf einem Smartphone gespeichert und darüber abgerufen werden können, können die Regelungen der ePrivacy-Richtlinie und deren Umsetzung in nationales Recht, die die Speicherung und den Zugriff von und auf Informationen auf elektronischen Endgeräten regeln, relevant sein (wie etwa Art. 5 Abs. 3 ePrivacy-Richtlinie).

Ab Inkrafttreten der ePrivacy-Verordnung werden die darin enthaltenen Regelungen hingegen direkt anwendbar und relevant für die in WearPrivate beispielhaft analysierten Abläufe sein.

3.1.3 Data Act

Mit der Vorstellung ihrer Datenstrategie[14] reagierte die Europäischen Union im Jahr 2021 auf die wachsende Bedeutung von Daten für die Gesellschaft und die Wirtschaft. Im Rahmen dieser Strategie wurden verschiedene Rechtsakte (Data Governance Act, Data Act) sowie die Schaffung eines Datenbinnenmarktes erlassen.

Die Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act, DA) trat am 11.01.2024 in Kraft und ist nach einer Übergangsfrist ab dem 12.09.2025 unmittelbar anwendbar. Ziel ist es nach Erwägungsgrund 32 zum DA unter anderem „die Entwicklung völlig neuartiger Dienste unter Nutzung der betreffenden Daten anzuregen,

---

[12] SYDOW in: Sydow/Marsch, Art. 95 DSGVO Rn. 2, 4.

[13] EBD.

[14] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

auch auf der Grundlage von Daten aus einer Vielzahl von vernetzten Produkten oder verbundenen Diensten.“ Der Data Act gilt sowohl für personenbezogene als auch für nichtpersonenbezogene Daten, Art. 1 Abs. 2 DA. Er gilt nach Art. 1 Abs. 5 DA zwar unbeschadet der DSGVO. Bei Widersprüchen geht die DSGVO dem Data Act jedoch vor, Art. 1 Abs. 5 DA.

3.1.3.1 Anwendung auf WearPrivate

Im Rahmen von WearPrivate werden Daten mittels eines Wearables (Fitnessgurt) generiert. Dabei handelt es sich um ein sogenanntes IoT-Gerät. Die Daten, die mittels Fitnessgurt erhoben werden, fallen mithin unter den DA. Durch den DA wird insbesondere das Recht auf Datenübertragbarkeit sowie der Zugang zu den generierten Daten gestärkt. Da der DA nicht zwischen personenbezogenen Daten und nichtpersonenbezogenen Daten unterscheidet, gilt dieses Recht auch für anonyme Daten, die keinen Personenbezug mehr aufweisen.

Arbeitnehmer im Anwendungsfall von WearPrivate könnten als Nutzer im Sinne des Art. 2 Nr. 12 DA klassifiziert werden. Dies würde mit sich bringen, dass ihnen ein erleichterter Zugang zu den Daten zu gewähren ist, Art. 3 und 4 DA. Dabei sind grundsätzlich bereits die Produkte so zu gestalten, dass der Zugang direkt über das Produkt selbst möglich ist, Art. 3 DA. Funktioniert dies nicht, so muss der Dateninhaber dem Nutzer den Zugang gewähren, Art. 4 Abs. 1 DA. Dateninhaber ist nach Art. 2 Nr. 13 DA eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat. Dateninhaber könnten im Falle von WearPrivate sowohl App-Hersteller als auch Analysedienst sein. Beide Anwendungspartner sind in der Lage, die mit dem Fitnessgurt erhobenen Rohdaten zu nutzen und bereitzustellen. Anders verhält es sich mit dem Arbeitgeber: Dieser erhält nämlich nur die vom Analysedienst bereits verarbeiteten Daten und keine Rohdaten. Er ist damit nicht in der Lage, den Arbeitnehmern Daten bereitzustellen. App-Hersteller und Analysedienst könnten allerdings aufgrund von Art. 4 Abs. 1 DA verpflichtet sein, Rohdaten herauszugeben.

3.1.4 European Health Data Space

Eine weitere Gesetzgebungsinitiative, die im Rahmen der Europäischen Datenstrategie entstanden ist, ist der European Health Data Space (Europäischer Raum für Gesundheitsdaten, EHDS)[15]. Entstehen soll durch die geplante Verordnung ein Datenraum für Gesundheitsdaten (u.a. ein echter Binnenmarkt für

[15] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten 2022/0140 (COD) vom 03.05.2022.

elektronische Patientendatensysteme und relevante Medizinprodukte), der (1) Einzelpersonen dabei unterstützt, die Kontrolle über ihre Gesundheitsdaten zu bewahren; der (2) die Nutzung von Gesundheitsdaten für eine bessere medizinische Versorgung, für Forschung, Innovation und Politikgestaltung fördert und der (3) es der EU ermöglicht, das Potenzial von Austausch, Nutzung und Weiterverwendung von Gesundheitsdaten unter gesicherten Bedingungen voll auszuschöpfen.[16] Dabei werden im EHDS sowohl die Primärnutzung von Gesundheitsdaten durch Einzelpersonen (bspw. hinsichtlich des digitalen Zugangs) als auch die Sekundärnutzung für Forschung, Innovation, Politikgestaltung usw. adressiert.[17]

Die Verordnung zum EHDS gilt neben den anderen bei der Verarbeitung von Gesundheitsdaten möglicherweise relevanten Rechtsvorschriften, wie der DSGVO, dem Daten-Governance-Rechtsakt und dem DA, und lässt diese unberührt, Art. 1 Abs. 4 EHDS.

Art. 1 Abs. 2 EHDS beinhaltet den Regelungsinhalt der Verordnung. Insbesondere regelt die Verordnung die Rechte der natürlichen Personen in Bezug auf die Verfügbarkeit elektronischer Gesundheitsdaten und die Kontrolle über diese Daten, Art. 1 Abs. 2 lit. a EHDS. Es handelt sich beim EHDS um eine sektorspezifische Regelung, die abweichend vom Data Act Regelungen für elektronische Gesundheitsdaten aufstellt.[18] Den persönlichen Anwendungsbereich legt die Verordnung in Art. 1 Abs. 3 EHDS fest. In Art. 2 Abs. 2 EHDS sind zahlreiche Begriffsbestimmungen zu finden.

3.1.4.1 Persönlicher Anwendungsbereich

Der Art. 1 Abs. 3 EHDS listet numerisch die Akteure auf, für die die Regelungen der Verordnung gelten. Demnach ist der Anwendungsbereich in persönlicher Hinsicht für folgende Akteure eröffnet:

- Hersteller und Anbieter von Electronic-Health-Record-Systemen und Wellness-Anwendungen, die in der Union in Verkehr gebracht und in Betrieb genommen werden, und Nutzer solcher Produkte (lit. a)
- in der Union niedergelassene Verantwortliche und Auftragsverarbeiter, die elektronische Gesundheitsdaten von Unionsbürgern und Drittstaatsangehörigen mit rechtmäßigem Wohnsitz im Hoheitsgebiet der Mitgliedstaaten verarbeiten (lit. b)

---

[16] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de, letzter Abruf am 10.10.2023.

[17] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de.

[18] SALEMI/WIEDEMANN/STEFFES, Data Sharing im Kontext digitaler Selbstvermessung in: Data Sharing: Datenkapitalismus bei Default, Posterproceedings Forum Privatheit 2023, S. 28.

- in einem Drittland niedergelassene Verantwortliche und Auftragsverarbeiter, die sich gemäß Artikel 12 Absatz 5 MyHealth@EU angeschlossen haben oder damit interoperabel sind (lit. c)
- Datennutzer, denen elektronische Gesundheitsdaten von Dateninhabern in der Union zur Verfügung gestellt werden (lit. d)

3.1.4.2 Anwendung auf WearPrivate

Die Regelungen zum EHDS können Relevanz für das Forschungsvorhaben entwickeln. So könnten sowohl Art. 1 Abs. 2 lit. b EHDS als auch Art. 1 Abs. 2 lit. d EHDS Anwendung finden. Im Rahmen von WearPrivate werden mittels eines Wearables gesammelte Daten der Arbeitnehmer über die App zum Analysedienst und später zum Arbeitgeber transferiert. Bei diesen Daten könnte es sich um personenbezogene elektronische Gesundheitsdaten im Sinne des Art. 2 Abs. 2 lit. a EHDS handeln. Personenbezogene elektronische Gesundheitsdaten sind Gesundheit und genetische Daten im Sinne der DSGVO sowie Daten über Gesundheitsfaktoren oder Daten, die im Zusammenhang mit der Erbringung von Gesundheitsdiensten verarbeitet werden, sofern sie in elektronischer Form verarbeitet werden. Ferner erfasst der EHDS auch nicht personenbezogene elektronische Gesundheitsdaten, wie sich aus Art. 2 Abs. 2 lit. b EHDS ergibt. Nicht personenbezogene elektronische Gesundheitsdaten sind Daten über die Gesundheit und genetische Daten in elektronischem Format, die nicht unter die Begriffsbestimmung für personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO fallen. Damit ist es für die Anwendbarkeit des EHDS im Projekt WearPrivate lediglich entscheidend, ob elektronische Gesundheitsdaten vorliegen. Hinsichtlich des Begriffs der Gesundheitsdaten ist die durch die DSGVO eingeführte Definition entscheidend, die sich in Art. 4 Nr. 15 DSGVO findet. Zu den Gesundheitsdaten zählen demnach alle *personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen*. Nach Erwägungsgrund 35 S. 1 zur DSGVO zählen alle Informationen, die sich auf den vergangenen, zukünftigen oder gegenwärtigen körperlichen oder geistigen Gesundheitszustand beziehen, zu personenbezogenen Gesundheitsdaten. Der Begriff ist im Sinne eines möglichst umfassenden Schutzes für die betroffenen Personen weit auszulegen.[19] Die Herzratenvariabilität fällt unter den Begriff der Gesundheitsdaten. Durch die Erfassung dieses Datums ist eine Aussage über den Gesundheitszustand der betroffenen Person möglich. In der Literatur ist ferner bereits grundsätzlich anerkannt, dass solche Daten, die von Fitness-Apps oder Health-Apps mittels Wearables erhoben werden, zu Gesundheitsdaten im Sinne des Art. 4

[19] SCHILD in: BeckOK DatenschutzR, Art. 4 DSGVO Rn. 143 mit Verweis auf ERNST in: Paal/Pauly, Art. 4 DSGVO Rn. 109.

Nr. 15 DSGVO gehören.[20] Mithin liegen Gesundheitsdaten vor, die auch elektronisch verarbeitet werden müssten. Auch diese Voraussetzung ist im WearPrivate-Szenario unzweifelhaft erfüllt. Diese elektronischen Gesundheitsdaten werden mindestens durch den Analysedienst mit Sitz im Unionsgebiet und wohl auch durch den Arbeitgeber verarbeitet im Sinne des Art. 4 Nr. 2 DSGVO (zur Verantwortlichkeit der Beteiligten im Einzelnen siehe Kapitel 7). Mithin ist Art. 1 Abs. 3 lit. a EHDS erfüllt.

Ferner könnte Art. 1 Abs. 3 lit. d EHDS einschlägig sein. Demnach gilt der EHDS auch für Datennutzer, denen elektronische Gesundheitsdaten von Dateninhabern in der Union zur Verfügung gestellt werden. Die Begriffe „Datennutzer“ und „Dateninhaber“ werden im EHDS definiert. Ein Datennutzer ist nach Art. 2 Abs. 2 lit. z EHDS „eine natürliche oder juristische Person, die rechtmäßig Zugang zu personenbezogenen oder nicht personenbezogenen elektronischen Gesundheitsdaten für die Sekundärnutzung hat“ und ein Dateninhaber ist nach Art. 2 Abs. 2 lit. y EHDS „jede natürliche oder juristische Person, bei der es sich um eine Organisation oder Einrichtung im Gesundheits- oder Pflegesektor handelt oder die Forschungstätigkeiten hinsichtlich dieser Sektoren durchführt, sowie Organe, Einrichtungen und sonstige Stellen der Union, die gemäß dieser Verordnung, dem geltenden Unionsrecht oder den nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts dazu berechtigt oder verpflichtet sind – oder im Falle nicht personenbezogener Daten durch Kontrolle der technischen Konzeption eines Produkts und der damit zusammenhängenden Dienste dazu befähigt sind –, bestimmte Daten zur Verfügung zu stellen und sie auch zu registrieren, bereitzustellen, den Zugang zu ihnen einzuschränken oder sie auszutauschen.“ Dateninhaber könnten im Rahmen von WearPrivate sowohl der Arbeitgeber als auch der Analysedienst oder der Hersteller des Wearables sein (s.o.), während die Arbeitnehmer Datennutzer sein könnte.

Es lässt sich daher festhalten, dass die Regelungen des EHDS, soweit die Definition des Anwendungsbereichs in der endgültigen Fassung der Verordnung in dieser Form bestehen bleibt, im WerPrivate-Szenario Anwendung finden.

3.2 Nationales Recht

3.2.1 Bundesdatenschutzgesetz

In § 1 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) ist dessen Anwendungsbereich geregelt. Es handelt sich um eine umfassende Regelung sowohl des sachlichen als auch des örtlichen

[20] ERNST in: Paal/Pauly, Art. 4 DSGVO Rn. 110; SCHILD in: BeckOK DatenschutzR, Art. 4 DSGVO Rn. 144.

Anwendungsbereiches. Differenziert wird in diesem Rahmen zwischen öffentlichen Stellen des Bundes, öffentlichen Stellen der Länder sowie nichtöffentlichen Stellen (S. 2).

Gemäß § 1 Abs. 1 BDSG für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes (S. 1 Nr. 1) sowie öffentliche Stellen der Länder (S. 1 Nr. 2), soweit keine landesrechtliche Regelung vorliegt und die Stellen entweder Bundesrecht ausführen (Abs. 1 S. 1 Nr. 2 lit. a) oder die öffentlichen Stellen als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt (Abs. 1 S. 1 Nr. 2 lit. b). Was unter einer öffentlichen Stelle des Bundes zu verstehen ist, ist in § 2 Abs. 1 BDSG geregelt, während sich die Legaldefinition des Begriffs „öffentliche Stellen der Länder“ in § 2 Abs. 2 BDSG befindet.

Ferner ist das BDSG auch auf nichtöffentliche Stellen anwendbar, soweit eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten oder eine nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, vorliegt, § 1 Abs. 1 S. 2 BDSG. Die Formulierung von § 1 Abs. 1 S. 2 BDSG ist identisch mit dem Wortlaut des Art. 2 Abs. 1 DSGVO. Die Definitionen aus Art. 4 Nr. 1 und 2 DSGVO der Begriffe „personenbezogene Daten“ und „Verarbeitung“ sind auch im Rahmen des BDSG anzuwenden.

Nach § 1 Abs. 1 S. 2 BDSG gilt auch beim BDSG die sogenannte „Haushaltsausnahme“ und demnach ist das BDSG nicht anwendbar, soweit die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt.

Zu beachten ist, dass das BDSG nur dort Anwendung findet, wo die DSGVO keine Regelung trifft beziehungsweise mittels einer Öffnungsklausel die Regelung einer bestimmten Materie den Mitgliedstaaten zuweist.

3.2.1.1 Anwendung auf WearPrivate

Im Rahmen des Projekts werden von nichtöffentlichen Stellen (Arbeitgebern) personenbezogene Daten in Deutschland erhoben und verwendet. Das BDSG ist mithin wie auch die DSGVO anwendbar.

3.2.2 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz

Am 01.12.2021 trat das „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (Telekommunikations-Telemedien-Datenschutzgesetz, TTDSG) in Kraft und wurde am 14.05.2024 in „Telekommunikation-Digitale-Dienste-Datenschutz-

Gesetz“ (TDDDG) umbenannt.[21] Der Inhalt des TDDDG blieb dabei im Wesentlichen identisch zu dem des TTDSG, sodass die Literatur zum TTDSG auf das TDDDG übertragbar ist.

3.2.2.1 Sachlicher Anwendungsbereich

In § 1 Abs. 1 TDDDG findet sich eine enumerative Aufzählung der Sachverhalte, die vom TDDDG erfasst werden sollen. Eine klassische Festlegung des sachlichen/personellen Anwendungsbereichs wird hier jedoch nicht vorgenommen. Der personelle Anwendungsbereich wird vielmehr in den jeweiligen Einzelvorschriften festgelegt und die Aufzählung in § 1 Abs. 1 TDDDG wird bei der Auslegung anderer Vorschriften relevant.[22]

3.2.2.2 Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich des Gesetzes ergibt sich aus § 1 Abs. 3 S. 1 TDDDG. Dort heißt es: *Diesem Gesetz unterliegen alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen.*

Der Begriff der Niederlassung entspricht dem der DSGVO und es gilt das oben Gesagte.[23] Der räumliche Anwendungsbereich ist jedoch auch dann eröffnet, wenn zwar keine Niederlassung in Deutschland vorliegt, jedoch Dienstleistungen auf dem Markt erbracht werden/an der Erbringung mitgewirkt wird oder Waren auf dem Markt bereitgestellt werden. Auch im TDDDG gelten damit sowohl das Niederlassungs- als auch das Marktortprinzip.[24]

3.2.3 Landesdatenschutzgesetze

Auch auf Ebene der Länder gibt es relevante datenschutzrechtliche Regelungen. Auch hier gilt es zu beachten, dass die DSGVO als EU-Verordnung grundsätzlich vorrangig anwendbar ist. Finden sich jedoch Öffnungsklauseln in der DSGVO, die den Mitgliedstaaten eigene Regelungen erlauben, sind auch die Gesetze der Mitgliedstaaten zu beachten. Je nachdem, in welchem Bundesland relevante

---

[21] Artikel 8 Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze.

[22] ETTIG in: Taeger/Gabel, § 1 TTDSG Rn. 5.

[23] S. unter 3.1.1 Örtlicher Anwendungsbereich der DSGVO.

[24] ECKHARDT/MÜHLENBECK/SCHWARTMANN in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 1 Rn. 54.

Datenverarbeitungen stattfinden, ist das jeweilige Landesdatenschutzgesetz zu betrachten und die Eröffnung des Anwendungsbereichs zu prüfen.

3.3 Anwendbarkeit der Gesetze bei Gewährleistung von Anonymität

Eines der zentralen technischen Ziele des Projekts WearPrivate ist die Gewährleistung von Anonymität bei der Sammlung der Wearable-Daten. Aufgabe der UdS ist es, verschiedene Anonymisierungskonzepte auszuarbeiten und die technische Umsetzung zu untersuchen. Werden jedoch nur Daten in anonymisierter Form erhoben, hat dies Auswirkungen auf die anwendbaren Gesetze. Der Begriff der Anonymisierung wird in der DSGVO nicht definiert. Es existieren jedoch drei verschiedene Formen der Anonymität. Unterschieden wird zwischen der formalen, der faktischen und der absoluten Anonymität.

3.3.1 Formale Anonymität

Von formaler Anonymität spricht man, wenn unmittelbar identifizierende Merkmale (wie der Name) entfernt werden.[25] Es handelt sich hierbei um die schwächste Form der Anonymität. Teilweise wird die Entfernung unmittelbar identifizierender Merkmale nur als Form der Pseudonymisierung gesehen.[26] Die Pseudonymisierung ist in Art. 4 Nr. 5 DSGVO definiert und bezeichnet demnach die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Soweit eine Re-Identifizierung mit verhältnismäßig geringem Aufwand möglich ist, liegt nur eine Pseudonymisierung und keine Anonymisierung vor.[27]

3.3.2 Faktische Anonymität

Die zweite Form der Anonymität ist die sogenannte faktische Anonymität. Bei der faktischen Anonymität werden so viele identifizierende Merkmale entfernt, dass der Aufwand der Re-Identifizierung so hoch ist, dass nicht mehr vernünftigerweise mit der Identifizierung gerechnet werden kann.[28] Um zu bestimmen, wann der Aufwand der Identifizierung unverhältnismäßig hoch ist,

---

[25] OVG Berlin, NVwZ-RR 2015, 126 (128); ZIEBARTH in: Sydow/Marsch, Art. 4 DSGVO Rn. 31.

[26] ERNST in: Paal/Pauly, Art. 4 DSGVO Rn. 49.

[27] ERNST in: Paal/Pauly, Art. 4 DSGVO Rn. 49.

[28] ZIEBARTH in: Sydow/Marsch, Art. 4 DSGVO Rn. 30.

kann Erwägungsgrund 26 S. 3 zur DSGVO herangezogen werden. Dieser bestimmt eigentlich, wann Identifizierbarkeit im Sinne des Art. 4 Nr. 1 DSGVO vorliegt, also wie lange Daten als personenbezogen zu klassifizieren sind. Bei der Frage nach der Identifizierbarkeit sind indes „alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren". Nach Satz 4 des Erwägungsgrundes sind dabei alle objektiven Faktoren wie beispielsweise Kosten und Zeitaufwand zu berücksichtigen. Diese Maßstäbe lassen sich auch auf die Abgrenzung von Anonymisierung und Pseudonymisierung übertragen: So kann man von Anonymität sprechen, soweit keine Mittel, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, mehr vorliegen. Dies schließt mithin nicht aus, dass faktische Anonymität trotz einer theoretischen Möglichkeit zur Identifizierung vorliegt. Wann Mittel nicht mehr „nach allgemeinem Ermessen wahrscheinlich genutzt werden", ist anhand einer Verhältnismäßigkeitsprüfung festzustellen, wobei der jeweilige Einzelfall zu betrachten ist.[29]

3.3.3 Absolute Anonymität

Die dritte und stärkste Form der Anonymität ist die absolute Anonymität. Diese liegt vor, wenn faktisch niemand mehr dazu in der Lage ist, einen Personenbezug herzustellen.[30]

3.3.4 Bedeutung für das Datenschutzrecht

Anonyme Daten sind das Gegenteil von personenbezogenen Daten.[31] Wie gesehen zeichnen sie sich gerade durch fehlenden Personenbezug aus. Als *anonym* im engeren Sinne sind solche Daten zu bezeichnen, die von Beginn an keinen Personenbezug aufweisen, es kann jedoch auch bei personenbezogenen Daten nachträglich der Personenbezug entfernt werden und ursprünglich personenbezogene Daten auf diese Weise nachträglich anonymisiert werden.[32] Fraglich ist, welche Auswirkungen die Anonymisierung personenbezogener Daten auf die anwendbaren Gesetze hat.

Art. 2 Abs. 1 DSGVO schreibt vor, dass der sachliche Anwendungsbereich der DSGVO bei der Verarbeitung personenbezogener Daten eröffnet ist. Diese Formulierung legt es nahe, dass der Anwendungsbereich für anonyme Daten mangels Personenbezug nicht eröffnet ist. Mit dieser Überlegung im Einklang steht Erwägungsgrund 26 S. 5 zur DSGVO. Aus diesem geht eindeutig hervor,

---

[29] HERMANN/MÜHLENBECK/SCHWARTMANN in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 4 DSGVO Rn. 94.

[30] ZIEBARTH in: Sydow/Marsch, Art. 4 DSGVO Rn. 29.

[31] MANTZ/MAROSI in: Specht/Mantz, DatenschutzR-Hdb, § 3 Rn. 15.

[32] MANTZ/MAROSI in: Specht/Mantz, DatenschutzR-Hdb, § 3 Rn. 15.

dass die Grundsätze des Datenschutzes nicht auf anonyme Daten anzuwenden sind *(„Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“*). Selbiges gilt für das BDSG und das LDSG.

Die Anonymisierung ist (wie auch die Pseudonymisierung) eine technische Maßnahme zum Schutz personenbezogener Daten. So wird in Art. 32 DSGVO, der die Sicherheit der Datenverarbeitung adressiert, die Pseudonymisierung ausdrücklich als geeignete Maßnahme aufgeführt, Art. 32 Abs. 1 lit. a DSGVO.

Anders ist jedoch die Anwendbarkeit des Data Acts, des EHDS und auch der ePrivacy-Richtlinie und damit auch des TDDDG zu bewerten, diese beziehen sich auch auf nicht-personenbezogene Daten.

3.3.5 Anwendung auf WearPrivate

Geplant ist, die Wearable-Daten möglichst nur in anonymer Form zu erheben beziehungsweise sie zu anonymisieren. Durch die verschiedenen Anonymisierungskonzepte, die von der UdS entwickelt wurden, sollen unterschiedliche Möglichkeiten aufgezeigt und dann festgelegt werden, welches Konzept sich am besten mit den Zielen von WearPrivate vereinen lässt.

Je nachdem, welche Form der Anonymisierung verwendet wird, kann dies dazu führen, dass die DSGVO, das BDSG und die LDSG keine Anwendung mehr finden. Zu beachten ist jedoch, dass auch die Anonymisierung selbst ein datenschutzrechtlich relevantes Verhalten und damit eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO darstellen kann. In einem Positionspapier aus dem Jahr 2020 ordnete der Bundesbeauftrage für den Datenschutz und die Informationssicherheit (BfDI) die Anonymisierung als datenschutzrechtlich relevantes Verhalten im Sinne der DSGVO ein. So handele es sich entweder um die Veränderung von Daten oder gegebenenfalls um die Verwendung von Daten.[33] Jedenfalls bedürfe es aber einer Rechtsgrundlage.[34] Diese Ansicht vertrat der BfDI jedoch nicht immer. Im 26. Tätigkeitsbericht aus dem Jahr 2015/2016 wurde die Anonymisierung von Daten

[33] Bundesbeauftragter für Datenschutz und Informationssicherheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand 29.06.2020, S. 5, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 30.11.2024.

[34] Bundesbeauftragter für Datenschutz und Informationssicherheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand 29.06.2020, S. 5, m.w.N., https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 30.11.2024.

ausdrücklich nicht als Verarbeitung eingestuft.[35] Die geänderte Sichtweise des BfDI führte in der rechtswissenschaftlichen Literatur zu gemischten Reaktionen.[36]

Die Anonymisierung könnte entweder eine Veränderung nach Art. 4 Nr. 2 Alt. 7 DSGVO oder eine Verwendung nach Art. 4 Nr. 2 Var. 10 DSGVO darstellen. Unter der Veränderung versteht man die Umgestaltung des Informationsgehalts eines personenbezogenen Datums, wobei die Reduktion des Informationsgehalts nicht ausreichend ist.[37] Der BfDI geht davon aus, dass in der Anonymisierung eine Veränderung zu sehen ist, weil die entsprechenden Daten in ihrer Personenbezogenheit verändert werden.[38] Dies erscheint jedoch nicht plausibel: Eine Änderung des Informations**inhaltes** des Datums wird gerade nicht vorgenommen.[39] Eine Änderung ist nur dann zu bejahen, wenn die Daten insgesamt einen neuen Informationswert erhalten.[40]

Allerdings könnte die Anonymisierung eine Verwendung im Sinne des Art. 4 Nr. 2 Var. 10 DSGVO darstellen. Bei der Verwendung handelt es sich um einen Auffangtatbestand und es wird jede Form der Datenverarbeitung erfasst.[41] Dies verdeutlicht sich auch in Erwägungsgrund 50 zur DSGVO: Dort

---

[35] Bundesbeauftragter für Datenschutz und Informationssicherheit, Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016, S. 170, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/26TB_15_16.pdf;jsessionid=9B7E9C9B786BAF64133B617E536D3596.intranet241?__blob=publicationFile&v=7, zuletzt abgerufen am 30.11.2024.

[36] Zustimmung erhielt der BfDI unter anderem von: GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT E.V. (GDD), Stellungnahme zur Konsultation des BfDI zum Thema „Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 1; VERBRAUCHERZENTRALE BUNDESVERBAND, ANONYMISIERUNG UNTER DER DSGVO, Stellungnahme des vzbv zur Konsultation des BfDI, S. 2; HORNUNG/WAGNER, ZD 2020, 223 (224 f.); STÜRMER, ZD 2020, 626 (629); ROßNAGEL, ZD 2021, 188 (189); ablehnend hingegen u.a.: BITKOM E.V., BfDI Konsultation – Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, S. 1; DEUTSCHE TELEKOM AG, Stellungnahme der Deutschen Telekom anlässlich des öffentlichen Konsultationsverfahrens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK- Branche, S. 2; GESAMTVERBANDES DER DEUTSCHEN VERSICHERUNGSWIRTSCHAFT (GDV), Stellungnahme des Gesamtverbandes der Deutschen Versicherungswirtschaft zum Öffentlichen Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 4; THÜSING/ROMBEY, ZD 2021, 548 (550 ff.).

[37] ARNING/ROTHKEGEL in: Taeger/Gabel, Art. 4 DSGVO Rn. 78.

[38] Bundesbeauftragter für Datenschutz und Informationssicherheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand 29.06.2020, S. 5, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 30.11.2024.

[39] ARNING/ROTHKEGEL in: Taeger/Gabel, Art. 4 DSGVO Rn. 78; THÜSING/ROMBEY, ZD 2021, 548 (550); SCHILD in: BeckOK DatenschutzR, Art. 4 Rn. 45.

[40] SCHILD in: BeckOK DatenschutzR, Art. 4 Rn. 45.

[41] SCHILD in: BeckOK DatenschutzR, Art. 4 Rn. 48.

wird „Verwendung“ als Sammelbegriff für alle Arten der Verarbeitung verwendet.[42] Soweit die Anonymisierung also mit personenbezogenen Daten im Zusammenhang steht, kann es sich um eine Verwendung von Daten handeln.[43] Durch die weite Auslegung des Begriffs liegt diese Annahme auch nahe. Trotzdem gibt es auch hier Stimmen in der Literatur, die die Einordnung der Anonymisierung als Verwendung ablehnen oder zumindest anzweifeln.[44] So sei die Anonymisierung lediglich eine vorbereitende Handlung und weder Nutzung noch Gebrauch von Daten.[45] Andere wiederum stellen die Frage, ob die Anonymisierung überhaupt als datenschutzrechtlich relevantes Verhalten anzusehen ist. Dabei wird mit dem Schutzzweck der DSGVO argumentiert: Dieser liege nämlich gerade im Schutz von Grundrechten sowie Grundfreiheiten betroffener Personen.[46] Regelmäßig handelt es sich bei der Anonymisierung um eine Schutzmaßnahme und weniger um eine Maßnahme, bei der in Grundrechte oder Grundfreiheiten eingegriffen wird.[47] Dies könnte für eine teleologische Reduktion des Anwendungsbereiches der DSGVO sprechen.[48] Allerdings wäre eine Reduktion nur dann sinnvoll, wenn man davon ausgehen könnte, dass durch die Anonymisierung nie die Rechte betroffener Personen beeinträchtigt werden, was allerdings nicht immer der Fall ist.[49]

Dementsprechend ist die Anonymisierung als Verwendung personenbezogener Daten als Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO einzuordnen. Beim Vorgang der Anonymisierung sind daher die Regelungen der DSGVO zu beachten und es bedarf insbesondere auch einer Rechtsgrundlage. Diese Rechtsgrundlage kann, soweit der Zweck der Anonymisierung mit dem ursprünglichen Zweck der Erhebung der personenbezogenen Daten vereinbar ist, dieselbe sein wie bei der Erhebung der Daten.[50]

---

[42] SCHILD in: BeckOK DatenschutzR, Art. 4 Rn. 48; ARNING/ROTHKEGEL in: Taeger/Gabel, Art. 4 DSGVO Rn. 81.

[43] ARNING/ROTHKEGEL in: Taeger/Gabel, Art. 4 DSGVO Rn. 82.

[44] THÜSING/ROMBEY, ZD 2021, 548 (550); mit Vorschlag einer teleologischen Reduktion: HORNUNG/WAGNER, ZD 2020, 223 (225).

[45] THÜSING/ROMBEY, ZD 2021, 548 (550).

[46] HORNUNG/WAGNER, ZD 2020, 223 (225).

[47] HORNUNG/WAGNER, ZD 2020, 223 (225).

[48] HORNUNG/WAGNER, ZD 2020, 223 (225).

[49] HORNUNG/WAGNER, ZD 2020, 223 (225).

[50] Bundesbeauftragter für Datenschutz und Informationssicherheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand 29.06.2020, S. 6, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 30.11.2024.

Nach erfolgter Anonymisierung können die Daten weiterverarbeitet werden, wobei es nun mangels Personenbezug keiner eigenen Rechtsgrundlage mehr bedarf.

3.3.6 Gefährdung der Anonymität durch die Zusammenführung von Daten

Die Zusammenführung verschiedener Daten stellt regelmäßig eine Gefährdung der Anonymität dar. Hierdurch entstehen neue Möglichkeiten, um eine bestehende Anonymisierung oder Pseudonymisierung aufzubrechen.

Die Etablierung des faktischen Anonymitätsbegriff bringt es auch mit sich, dass sich der Aufwand der De-Anonymisierung auch durch eine Veränderung der Umstände so reduzieren kann, dass ein ursprünglich als anonym im Sinne der DSGVO geltendes Datum doch wieder als personenbezogen zu charakterisieren ist.

Diese Gefahr besteht insbesondere bei der Verknüpfung und Zusammenführung von Daten. Werden verschiedene Daten zu einer betroffenen Person an einem einzelnen Ort gespeichert, erleichtert dies erheblich die Identifizierung, selbst wenn einzelne Daten als anonym anzusehen sind. Ebenso ist eine Pseudonymisierung unter diesen Umständen einfacher aufzubrechen.

Auch diese Gefahr gilt es im Kontext von WearPrivate zu betrachten und darauf zu achten, dass eine Zusammenführung von Daten nicht zu einfach möglich ist.

3.3.7 Gefährdung der Anonymität durch die Übermittlung von gerätespezifischen Informationen

Im WearPrivate-Szenario werden Daten vom Smartphone, die in einer App gesammelt werden, an den Analyseservice übermittelt, welcher die Daten alleine oder mithilfe eines Auftragsverarbeiters weiterverarbeitet. Das Resultat der Verarbeitung wird im Folgenden an die App zurückübermittelt. Grundsätzlich übermittelt die App im ersten Schritt insbesondere die Herzratenvariabilität sowie die Beschleunigungsdaten, mithilfe derer die Belastung der Mitarbeiter gemessen werden kann. Darüber hinaus werden allerdings auch weitere gerätespezifische Informationen übermittelt. Hierzu zählen die Firmware des verwendeten Wearables, der Herstellername des Wearables, der Gerätename, die Appversion und die Betriebssystemversion des Smartphones.

Diese Informationen könnten eine Aussage über den Nutzer beinhalten und hierdurch die Identifizierung des Nutzers ermöglichen. Ist die Identifizierung des Nutzers unter vertretbarem Aufwand möglich, so handelt es sich um eine Verarbeitung personenbezogener Daten, wodurch der Anwendungsbereich der DSGVO in sachlicher Hinsicht eröffnet ist und somit die strengen Vorgaben der Verordnung zu beachten sind. Daher stellt sich die Frage, ob die Identifizierung einzelner Nutzer möglich ist. In den meisten Fällen dürfte es sich bei den genannten Daten eher um Sachdaten ohne

Personenbezug handeln, da sich insbesondere die Identität der betroffenen Person nicht direkt aus dem Datum ergibt. Vielmehr kann höchstens eine Identifizierbarkeit angenommen werden. Diese kann allerdings ausreichen, um einen Personenbezug zu begründen. Aus Erwägungsgrund 26 S. 2 zur DSGVO ergibt sich, dass bei der Frage, ob eine Person identifizierbar ist, alle Mittel berücksichtigt werden sollten, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Heranzuziehen sind bei der Feststellung alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, Erwägungsgrund 26 S. 3 zur DSGVO. Abgestellt wird hinsichtlich der Identifizierbarkeit grundsätzlich auf den Verantwortlichen, wobei nach Ansicht des EuGHs auch Wissen und Mittel Dritter miteinbezogen werden kann, soweit für den Verantwortlichen eine rechtliche Handhabe besteht, um auf dieses Wissen zuzugreifen.[51] Fraglich ist, ob die betrachteten gerätespezifischen Daten eine Identifizierung mit entsprechendem Aufwand ermöglichen. Die gerätespezifischen Daten sind indes für sich genommen nicht sehr aussagekräftig und ermöglichen nur unter besonderen Umständen eine Identifizierung. Denkbar wäre die Identifizierung nur, wenn nur eine einzelne Person in einer Gruppe über einen bestimmten Gerätetyp, der beispielsweise aufgrund seines Alters nicht mehr über das neueste Betriebssystem verfügen würde. Diese Information könnte der Arbeitgeber dann recht unproblematisch erhalten, wenn die von den Arbeitnehmern verwendeten Smartphones vom Arbeitgeber ausgegeben würden. Anders ist dies zu beurteilen, wenn die Arbeitnehmer ihre eigenen Geräte verwenden. Dann könnte der Arbeitgeber diese Information nur bei einem kollusiven Zusammenwirken mit dem Analysedienst erhalten und müsste gleichzeitig darüber informiert sein, welcher seiner Arbeitnehmer privat ein veraltetes Smartphone verwendet. Allerdings ist nicht davon auszugehen, dass hierfür eine rechtliche Handhabe des Arbeitgebers existiert, womit nach der herrschenden Ansicht des EuGHs auch kein Personenbezug gegeben ist. Dies gilt für den Arbeitgeber. Der Analysedienst wird hingegen zwar über die Information verfügen, **dass** eine Person ein veraltetes Smartphone verwendet, **welche** Person dies allerdings ist, kann er wiederum nur bei einem kollusiven Zusammenwirken mit dem Arbeitgeber herausfinden – womit auch in dieser Konstellation kein Personenbezug gegeben ist.

Sollte der Arbeitgeber die Geräte selbst ausgeben, gilt Folgendes: Durch die geplante Anonymisierung der Daten wie Herzratenvariabilität und Beschleunigungsdaten und Stammdaten soll eigentlich die Anwendbarkeit der DSGVO ausgeschlossen werden. Lassen allerdings gerätespezifische Informationen einen Rückschluss auf den jeweiligen Nutzer zu, ist die die DSGVO anwendbar. Aus diesem Grund

[51] Siehe hierzu: EuGH, NJW 2016, 3579 (3581, Rn. 49).

erscheint es zumindest in diesem Szenario sinnvoll, statt der genauen gerätespezifischen Angaben Platzhalter an den Analysedienst zu senden.

4 Rechtsgrundlagen für die Verarbeitung von Wearable-Daten

Zu prüfen, wie die Anonymisierung im Anwendungsszenario von WearPrivate umgesetzt werden kann stellt eine der wesentlichen Aufgaben der UdS dar. Es ist jedoch nicht ohne Weiteres davon auszugehen, dass die Anonymisierung lückenlos umgesetzt werden kann, sodass trotzdem die datenschutzrechtliche Zulässigkeit der einzelnen Abläufe im Anwendungsszenario geprüft werden muss. Die nun folgenden Ausführungen gelten somit für den Fall, dass eine vollständige Anonymisierung nicht möglich ist und somit weiterhin ein Personenbezug gegeben ist. In diesem Fall sind die Vorgaben der DSGVO und innerhalb der Anwendbarkeit auch des BDSG und LDSG zu beachten.

Die Verarbeitung personenbezogener Daten steht unter einem Verbot mit Erlaubnisvorbehalt.[52] Demnach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, es existiert ein Erlaubnistatbestand, der sie rechtfertigt. Im folgenden Kapitel sind die für den Wearable-Einsatz im Arbeitskontext in Betracht kommenden Rechtsgrundlagen zu prüfen.

4.1 Einwilligung

In Betracht käme zunächst eine Einwilligung. Die Einwilligung wird in Art. 4 Nr. 11 DSGVO legaldefiniert: Eine Einwilligung ist 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.

Grundsätzlich ist Art. 6 Abs. 1 lit. a DSGVO heranzuziehen. Im WearPrivate-Szenario werden mit der Herzratenvariabilität personenbezogene Gesundheitsdaten gesammelt, weshalb neben Art. 6 Abs. 1 lit. a DSGVO auch Art. 9 Abs. 2 lit. a DSGVO heranzuziehen sein könnte. Allerdings handelt es sich ferner um eine Datenverarbeitung im Beschäftigtenkontext, weshalb auch § 26 Abs. 2 BDSG und § 26 Abs. 3 S. 2 i.V.m. § 26 Abs. 2 BDSG als lex specialis gegenüber Art. 9 Abs. 2 lit. a einschlägig sind.[53]

Die Einwilligung hat formelle sowie materielle Voraussetzungen, die sich in einer Gesamtschau aus allen einschlägigen Regelungen ergeben (hierzu zählen insbesondere die Art. 4 Nr. 11, 6 Abs. 1 lit. a, 7

---

[52] BUCHNER/PETRI in: Kühling/Buchner, Art. 6 DSGVO Rn. 11.

[53] Zu der teilweisen Europarechtswidrigkeit von § 26 BDSG siehe Kapitel 4.1.2.

DSGVO). Diese grundsätzlichen Voraussetzungen werden durch die speziellen Vorschrift Art. 9 Abs. 2 lit. a DSGVO und § 26 Abs. 2 und 3 BDSG modifiziert.

4.1.1 Erforderlichkeit einer Einwilligung aufgrund der ePrivacy-Richtlinie

Grundsätzlich sind in der DSGVO verschiedene Erlaubnistatbestände für die Verarbeitung personenbezogener Daten angelegt. Zu finden sind diese in den Art. 6 Abs. 1 und 9 Abs. 2 DSGVO. Die Erlaubnistatbestände sind in einem Katalog aufgelistet. Zwischen den Erlaubnistatbeständen besteht indes keine Hierarchie und es muss (gemäß Art. 6 Abs. 1 DSGVO) lediglich einer der möglichen Erlaubnistatbestände vorliegen. Auch im vorliegenden Szenario sind verschiedene Rechtsgrundlagen denkbar, auf die die Verarbeitung gestützt werden kann, bspw. die Einwilligung, die spezifischen Rechtsgrundlagen des Beschäftigtendatenschutzes oder berechtigte Interessen. Vorliegend könnte sich allerdings aufgrund der besonderen Situation, dass Daten über ein Wearable gesammelt und später auch darauf zugegriffen wird, aufgrund von ePrivacy-Aspekten die Erforderlichkeit einer Einwilligung ergeben. So ist grundsätzlich nach Art. 5 Abs. 3 ePRivacy-Richtlinie, umgesetzt in § 25 TDDDG[54], eine Einwilligung erforderlich, wenn auf Informationen zugegriffen wird, die auf dem Endgerät eines Nutzers gespeichert sind. Diese Einwilligung ist nur unter den Umständen rechtmäßig, dass der Nutzer klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern, Art. 5 Abs. 3 ePrivacy-Richtlinie. Gemäß § 25 Abs. 1 S. 2 TDDDG muss die Einwilligung in den Zugriff auf Daten, die auf einem Endgerät gespeichert sind, den Vorgaben der DSGVO entsprechen. Ausnahmen von der grundsätzlich erforderlichen Einwilligung finden sich in § 25 Abs. 2 TDDDG. Diese Regelungen sind **nur** für den Zugriff (bzw. auch die Speicherung) von Informationen auf einer Endeinrichtung einschlägig, weitere Verarbeitungen bedürfen vielmehr einer datenschutzrechtlichen Erlaubnis, die regelmäßig aus der DSGVO oder dem BDSG hervorgehen dürfte.[55]

Zunächst bedarf es der Auseinandersetzung mit der Frage, ob im vorliegenden Fall der Zugriff auf Informationen von einer Endeinrichtung vorliegt. Eine Endeinrichtung ist nach § 2 Abs. 2 Nr. 6 TDDDG „jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung

---

[54] SCHNEIDER in: Assion TTDSG, § 25 Rn. 13.

[55] SCHMITZ in: Beck`scher TKG-Kommentar, § 25 Rn. 35.

und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet". Gemeint sind damit alle Geräte, die Nachrichten senden, empfangen oder verarbeiten können.[56] Auch, wenn diese Definition ursprünglich auf Computer, Telefone und ähnliche Geräte ausgelegt war, fallen nach heutigem Verständnis auch sämtliche Geräte, die zum IoT gehören, darunter.[57] IoT-Geräte sind smarte Geräte, die über einen Zugang zum Internet verfügen oder über andere Netzwerke auch untereinander kommunizieren, wie eben beispielsweise Wearables.[58] In persönlicher Hinsicht wird der Endnutzer der Endeinrichtung geschützt.[59] Der Begriff des Endnutzers ist in § 3 Nr. 13 TKG definiert. Der Endnutzer ist ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt, wobei ein Nutzer nach § 3 Nr. 41 TKG eine natürliche oder juristische Person ist, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt.

Sowohl in Art. 5 Abs. 3 ePrivacy-Richtlinie als auch in § 25 Abs. 2 TDDDG sind Ausnahmen von der grundsätzlichen Pflicht zur Einholung von Einwilligungen normiert. So ist die Einwilligung nach § 25 Abs. 2 Nr. 1 TDDDG einerseits entbehrlich, wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist. Andererseits ist die Einwilligung nicht erforderlich, wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann.

Darauf, dass der Zugriff auf Daten, die auf entsprechenden Endgeräten gespeichert werden, eine Einwilligung des Nutzers erfordert, weist auch Erwägungsgrund 36 zum Data Act hin – diese ausdrückliche Erwähnung zeigt, dass auch die Vorschriften des Data Acts, die teilweise den Zugriff auf Daten von IoT-Geräten erleichtern, durch das Einwilligungserfordernis der ePrivacy-Richtlinie flankiert werden.

---

[56] ASSION in: Assion TTDSG, § 2 Rn. 34.

[57] SCHNEIDER in: Assion TTDSG, § 25 Rn. 22.

[58] HAGAR, JON DUNCAN, IoT System Testing: An IoT Journey from Devices to Analytics and the Edge, 1. Ausgabe 2022, S. 3.

[59] SCHNEIDER in: Assion TTDSG, § 25 Rn. 18.

4.1.1.1 Anwendung auf WearPrivate

Im WearPrivate-Szenario werden nach der Registrierung in einer App, in der verschiedene Stammdaten (Größe, Geburtsjahr, Gewicht, Geschlecht), über ein Wearable (vorzüglich einen Fitnessgurt) Daten wie die Herzratenvariabilität sowie Beschleunigungsdaten gesammelt. Diese Daten werden im Anschluss über die App weiter zum Analysedienst transferiert, der die Daten in der Cloud verarbeitet. Erst im Anschluss erhält der Arbeitgeber die verarbeiteten und anonymisierten Daten.

Für die Verarbeitungen, die Analysedienst und Arbeitgeber durchführen, bedarf es jeweils einer Rechtsgrundlage. Fraglich ist, ob Art. 5 Abs. 3 der ePrivacy-Richtlinie bzw. § 25 Abs. 1 TDDDG hier einschlägig sind. Hierfür bedürfte es grundsätzlich eines Zugriffs auf Daten, die auf einem Endgerät gespeichert werden, wobei es jeweils eines drittveranlassten Zugriffs bedarf (mithin nicht vom berechtigten Endnutzer veranlasst).[60] Als Endeinrichtung kämen hier sowohl das Wearable wie etwa ein Fitnessgurt als auch das Smartphone der Arbeitnehmer in Betracht.[61] In beiden Fällen müsste auf Daten zugegriffen werden, die auf dem Gerät bereits gespeichert sind. Erfasst von der Regelung ist der Fernzugriff auf gespeichert Daten.[62] Hierbei gilt es zu beachten, dass bereits die zielgerichtete sowie erfolgreiche **Beschaffung der Zugriffsmöglichkeit** ausreicht; nicht erforderlich ist nach unionskonformer Auslegung der tatsächliche Zugriff auf die gespeicherten Daten.[63] § 25 TDDDG regelt weder den weiteren Umgang mit den Daten, auf die zugegriffen wurde (wie bspw. das Auslesen oder die Kenntnisnahme), noch die Übermittlung von Daten an einen Dritten, der selbst nicht mit der Endeinrichtung kommuniziert.[64]

4.1.1.1.1 App-Betreiber

In der Kette am Anfang steht der App-Betreiber. Dieser erhält die Daten, die auf dem Wearable, zwar mangels großen Speicherplatzes nur für kurze Zeit, allerdings trotzdem zwischengespeichert werden und leitet diese, ohne sie auf seinen eigenen Servern zwischenzuspeichern, an den Analysedienst weiter. Fraglich ist, ob hierdurch auf die auf dem Wearable gespeicherten Daten zugegriffen wird. Ausreichend ist, wie oben gesehen, die Beschaffung der Zugriffsmöglichkeit. Auch, wenn der Begriff des „Zugriffs“ scheinbar ein aktives Handeln beschreibt, ist auch ein automatischer Download von

---

[60] HANLOSER in: Gierschmann/Baumgartner TTDSG, § 25 Rn. 57 f.

[61] Siehe zum Begriff der Endeinrichtung: HANLOSER in: Gierschmann/Baumgartner TTDSG, § 25 Rn. 44.

[62] HANLOSER in: Gierschmann/Baumgartner TTDSG, § 25 Rn. 60.

[63] EBD.

[64] HANLOSER in: Gierschmann/Baumgartner TTDSG, § 25 Rn. 60, 61.

Daten hiervon erfasst.[65] Dies gilt allerdings nicht für „automatische Sendevorgänge“, die bei IoT-Geräten versendet werden, um beispielsweise anzuzeigen, dass das Gerät empfangsbereit ist.[66] Der Zugriff auf darüber hinausgehende Informationen ist anhand von § 25 TDDDG zu beurteilen.[67] Für das WearPrivate-Szenario ergibt sich aus diesen Ausführungen, dass auch die automatische Sendung der Daten, die auf dem Wearable gespeichert werden, an das Smartphone als Zugriff im Sinne des § 25 TDDDG einzuordnen sind. Demnach müsste der App-Betreiber eine Einwilligung des Arbeitnehmers einholen. Da § 25 TDDDG jede natürliche oder juristische Person adressiert, die tatsächlich Daten speichert oder auf diese zugreift und weder an die Eigenschaft als Anbieters von digitalen Diensten noch als Verantwortlicher im Sinne der DSGVO anknüpft, ist auch der App-Betreiber Verpflichteter.[68] Grundsätzlich bedarf es mithin einer Einwilligung des Arbeitnehmers gegenüber dem App-Betreiber. Jedoch könnte hier die Ausnahme aus § 25 Abs. 2 Nr. 2 TDDDG einschlägig sein. Demnach ist die Einwilligung nicht erforderlich, wenn der Zugriff auf die gespeicherten Daten erforderlich ist, damit der Anbieter eines digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann. **Ausdrücklich erwünscht** ist ein digitaler Dienst, wenn eine spezifische Ausrichtung auf den bestimmten digitalen Dienst unternommen wird, beispielsweise durch das bewusste Aufrufen einer bestimmten Webseite.[69] Es bedarf einer initiativen Handlung des Endnutzers, um einen bestimmten Dienst in einem klar definierten Umfang anzufordern.[70] **Unbedingt erforderlich** ist der Zugriff auf den gewünschte digitalen Dienst dann, wenn er oder die konkret angeforderte Funktion des Dienstes nicht funktionieren würde.[71] Der Dienst der App ist im vorliegenden Fall ausdrücklich erwünscht. Der Nutzer des Wearables lädt sich die App bewusst und initiativ in dem Wissen herunter, dass hierüber Daten weitergegeben werden, um an der Analyse, die im WearPrivate-Szenario durchgeführt wird, teilzunehmen. Ferner ist auch davon auszugehen, dass die Dienstleistung der App nicht erbracht werden kann, ohne dass ein Zugriff auf die Daten des Wearables stattfindet. Mithin ist an dieser Stelle keine Einwilligung nach dem TDDDG bzw. der ePrivacy-Richtlinie erforderlich.

---

[65] SCHNEIDER in: Assion TTDSG, § 25 Rn. 23.

[66] BURKHARDT/REIF/SCHWARTMANN in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 25 Rn. 27.

[67] EBD.

[68] BURKHARDT/REIF/SCHWARTMANN in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 25 Rn. 30, 31.

[69] HANLOSER in: Gierschmann/Baumgartner TTDSG, § 25 Rn. 101.

[70] WERKMEISTER in: Säcker/Körber, § 25 TTDSG Rn. 35 mit Verweis auf: Artikel-29-Datenschutzgruppe, 00879/12/DE WP 194, S. 4.

[71] EBD.

4.1.1.1.2 Analysedienst

In der Kette der Verarbeitung steht nach dem App-Betreiber der Analysedienst. Der Analysedienst greift indes nicht auf das Wearable zu, sondern die Daten werden vom Smartphone zum Analysedienst weitergeleitet. Das Smartphone stellt ebenfalls eine Endeinrichtung im Sinne des TDDDG/der ePrivacy-Richtlinie dar. Ferner reicht wie bereits ausgeführt auch der automatische Download von Daten aus, um einen Zugriff in diesem Sinne zu beschreiben. Fraglich ist, ob die Daten, die das Wearable generiert, auch auf dem Smartphone gespeichert werden. Hinsichtlich der Beschleunigungs- und der Herzratenvariabilitätsdaten gilt, dass diese gespeichert werden. Dies ist allerdings unerheblich, da Stammdaten wie Geschlecht, Gewicht, Geburtsjahr und Größe, welche auf der Endeinrichtung gespeichert sind, an den Analysedienst weitergegeben werden. Somit hat der Analysedienst Zugriff auf Informationen, die in der Endeinrichtung gespeichert sind, was für die Erforderlichkeit einer Einwilligung spricht. Allerdings stellt sich auch hier die Frage, ob nicht ein ausdrücklich erwünschter digitaler Dienst vorliegt, für den der Datenzugriff unbedingt erforderlich ist. Die unbedingte Erforderlichkeit dürfte indes zu bejahen sein, da der Analysedienst seine Leistung nicht erbringen kann, wenn er keinen Zugriff auf die Daten erhält. Fraglich ist, ob es sich um einen ausdrücklich erwünschten Dienst handelt. Erforderlich wäre, dass der Endnutzer initiativ eine Handlung vorgenommen hat, um einen bestimmten Dienst in einem klar definierten Umfang anzufordern. Im vorliegenden Szenario lädt der Endnutzer die Smartphone-App herunter, ohne dass konkret der Analysedienst angefordert wird. Jedoch wird der Endnutzer transparent über alle Verarbeitungsvorgänge aufgeklärt und die Tatsache, dass der Analysedienst die Daten von der App erhält, ist klar ersichtlich. Lädt sich der Nutzer die App in diesem Wissen bewusst herunter, kann auch hier von der Inanspruchnahme eines ausdrücklich erwünschten digitalen Dienstes ausgegangen werden. Mithin greift auch hier die Ausnahme des § 25 Abs. 2 Nr. 2 TDDDG und das Einwilligungserfordernis entfällt. Jedoch ist zu beachten, dass alle weiteren Handlungen des Analysedienstes (auch die Kenntnisnahme und Übermittlung an den Clouddienst der Daten) unter dem Vorbehalt der DSGVO stehen.

4.1.1.1.3 Clouddienst

Hinter dem Analysedienst steht indes der Clouddienst. Der Clouddienst erhält die Daten vom Analysedienst, § 25 TDDDG ist für diese Datenübermittlung nicht mehr einschlägig.

4.1.1.1.4 Arbeitgeber

Fraglich ist zuletzt, ob gegenüber dem Arbeitgeber eine Einwilligung erklärt werden kann. Da es sich um eine Nutzung der Endeinrichtung im Beschäftigtenkontext handelt, bedarf es an dieser Stelle des Hinweises, dass der Arbeitgeber je nach Konstellation auch ohne Einwilligung des Arbeitnehmers zugriffsberechtigt sein könnte. Dies wäre insbesondere dann der Fall, wenn die jeweilige

Endeinrichtung dem Arbeitnehmer durch den Arbeitgeber erst zur Verfügung gestellt worden wäre und es sich um eine fremdadministrierte Endeinrichtung handelte.[72] Im WearPrivate-Szenario ist an dieser Stelle zwischen dem Wearable und dem Smartphone zu unterscheiden. Das Wearable wird vom Arbeitgeber, voraussichtlich im Rahmen einer „Grabbelkiste“ ausgegeben; für das Smartphones sollen die Arbeitnehmer hingegen regelmäßig ihr eigenes Mobilgerät verwenden. Hinsichtlich des Smartphones scheidet mithin meist die Zugriffsberechtigung des Arbeitgebers aus. Bei dem Wearable könnte es sich hingegen um eine fremdadministrative Endeinrichtung, die durch den Arbeitgeber erst zur Verfügung gestellt worden ist, handeln. Der Arbeitgeber bleibt in diesem Verhältnis zugriffsberechtigt.

Jedoch bleibt darauf zu verweisen, dass der Arbeitgeber nicht auf Daten, die auf dem Wearable oder auf dem Smartphone gespeichert sind, zugreift. Vielmehr erhält er erst die durch den Clouddienst fertig verarbeiteten Daten; für diese Übermittlung ist das TDDDG nicht mehr einschlägig. Diese Übermittlung richtet sich nach der DSGVO.

4.1.1.1.5 Ergebnis

Im WearPrivate-Szenario ist der **Zugriff** auf die Daten, die auf dem Wearable bzw. dem Smartphone gespeichert sind, durch den App-Anbieter bzw. den Analysedienst ohne Einwilligung des Arbeitnehmers möglich. Weitere Verarbeitungen richten sich nach der DSGVO bzw. nach dem BDSG.

4.1.2 Einwilligung nach der DSGVO und dem BDSG

Weitere Datenverarbeitungen im WearPrivate-Szenario richten sich nach den datenschutzrechtlichen Vorschriften, die der DSGVO bzw. dem BDSG entspringen. Grundsätzlich genießt die DSGVO als unionsrechtliche Regelung Anwendungsvorrang gegenüber dem BDSG. Dies gilt jedoch nicht für solche Regelungen im BDSG, die im Rahmen der Ausfüllung einer Öffnungsklausel der DSGVO erlassen wurden.[73] Für den Beschäftigtenkontext existiert mit Art. 88 Abs. 1 DSGVO eine solche Klausel.[74] Diese Klausel wurde in Deutschland mit § 26 BDSG ausgefüllt.[75] § 26 BDSG enthält indes verschiedene Regelungen. In § 26 Abs. 1 S. 1 BDSG sind Verarbeitungen personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen

---

[72] HANLOSER in: Gierschmann/Baumgartner TTDSG, § 25 Rn. 54.

[73] Siehe hierzu: PÖTTERS in: Gola/Heckmann, Art. 88 DSGVO Rn. 3.

[74] RIESENHUBER in: BeckOK DarenschutzR, Art. 88 DSGVO Rn. 1.

[75] RIESENHUBER in: BeckOK DarenschutzR, Art. 88 DSGVO Rn. 100.

Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist, geregelt. § 26 Abs. 1 S. 2 BDSG betrifft die Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten. § 26 Abs. 2 BDSG regelt die Datenverarbeitung im Beschäftigtenverhältnis auf Grundlage einer Einwilligung der Arbeitnehmer – hier werden auch die Besonderheiten einer Einwilligung im Beschäftigtenverhältnis angesprochen. § 26 Abs. 3 BDSG enthält wiederum besondere Regelungen, da diese sich auf die Verarbeitung besonders sensibler Daten im Sinne des Art. 9 DSGVO im Arbeitsverhältnis bezieht. § 26 Abs. 3 BDSG beruht indes nicht auf Art. 88 Abs. 1 DSGVO, sondern auf Art. 9 Abs. 4 DSGVO.[76] § 26 Abs. 4 BDSG bezieht sich auf die Datenverarbeitung auf Grundlage einer Kollektivvereinbarung, Abs. 5 verweist auf die Pflicht zur Einhaltung der allgemeinen Grundsätze der Datenverarbeitung in Art. 5 DSGVO und Abs. 8 regelt den Begriff des Beschäftigten.

Dort, wo der Anwendungsbereich des § 26 BDSG eröffnet ist und die Vorgaben des § 26 BDSG spezieller sind als die der DSGVO, verdrängt er als lex specialis die Regelungen der DSGVO.[77] Dies könnte insbesondere hinsichtlich § 26 Abs. 1 S. 1 BDSG und Art. 6 Abs. 1 lit. b DSGVO gelten.[78] Allerdings bestehen insbesondere hinsichtlich § 26 Abs. 1 S. 1 BDSG seit einem Urteil des EuGH vom 30.03.2023[79] Bedenken hinsichtlich der Vereinbarkeit mit Art. 88 DSGVO mangels speziellerer Regelungen. Der EuGH äußert sich in der Entscheidung zur beinahe wortgleichen Vorschrift im hessischen Datenschutzgesetz (§ 23 Abs. 1 S. 1 HDSIG). Der Gerichtshof erkennt im Urteil zwar an, dass Mitgliedstaaten grundsätzlich zusätzliche, strengere oder einschränkende, nationale Vorschriften vorsehen dürfen und ihnen die Entscheidung hinsichtlich der Art und Weise der Durchführung dieser Bestimmungen obliegt.[80] Hinsichtlich des § 23 Abs. 1 S. 1 HDSG moniert der EuGH jedoch das Fehlen geeigneter und besonderer Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, weshalb die Vereinbarkeit mit Art. 88 Abs. 1 und 2 DSGVO zu bezweifeln ist.[81] Aufgrund des in großen Teilen übereinstimmenden Wortlauts von § 23 Abs. 1 S. 1 HDSG und § 26 Abs. 1 S. 1 BDSG sind beide Vorschriften in der derzeitigen Form nicht

---

[76] FRANZEN in: ErfK ArbeitsR, § 26 BDSG Rn. 46.

[77] MALORNY, JuS 2022, 289 (293).

[78] FRANZEN in: ErfK ArbeitsR, § 26 BDSG Rn. 4, 5.

[79] EuGH, Urt. v. 30.3.2023 - C-34/21, NZA 2023, 487.

[80] EuGH, Urt. v. 30.3.2023 – C-34/21, NZA 2023, 487, (489 Rn. 51).

[81] EuGH, Urt. v. 30.3.2023 – C-34/21, NZA 2023, 487 (490 Rn. 64 f.; 491 Rn. 74).

mehr anzuwenden.[82] Es ist auf die allgemeinen Erlaubnistatbestände der DSGVO zurückzugreifen. Allerdings ist darauf hinzuweisen, dass der Mehrwert des § 26 Abs. 1 S. 1 BDSG ohnehin nur begrenzt war; so bietet die Vorschrift keinen stärkeren Schutz als die allgemeinen Erlaubnistatbestände der DSGVO ohne besonderen Bezug zum Beschäftigtendatenschutz.[83]

Diese Ausführungen gelten indes nur für § 26 Abs. 1 S. 1 BDSG, § 26 Abs. 2 BDSG sowie § 26 Abs. 3 BDSG bleiben hingegen anwendbar. § 26 Abs. 2 BDSG wiederholt bzw. modifiziert die Regelungen der DSGVO im Hinblick auf die Einwilligung im Beschäftigtenkontext nur leicht. In dem Fall verdrängt die Regelung die allgemeinen Erlaubnistatbestände der DSGVO nicht.[84]

Da im WearPrivate-Szenario mehrere verschiedene Rechtsgrundlagen herangezogen werden könnten, sind beide Vorschriften zu überprüfen. Zunächst stellt sich die Frage, ob eine Einwilligung der Arbeitnehmer eingeholt werden könnte. Wie bereits erläutert, modifiziert § 26 Abs. 2 BDSG die allgemeinen Vorgaben zur Einwilligung der DSGVO, weshalb es sowohl einer Betrachtung der allgemeinen formellen sowie materiellen Wirksamkeitsvoraussetzungen der Einwilligung bedarf als auch der Betrachtung der modifizierenden besonderen Voraussetzungen aus § 26 Abs. 2 BDSG und Art. 9 Abs. 2 lit. a DSGVO.

4.1.2.1 Formelle Voraussetzungen einer wirksamen Einwilligung

Zunächst sind die formellen Anforderungen an eine wirksame Einwilligung einzuhalten. Diese beschränken sich auf das Vorliegen der Einwilligungsfähigkeit der einwilligenden Person und auf deren ordnungsgemäße Einwilligungserklärung. Die Einwilligungsfähigkeit beschreibt die Fähigkeit der Person, die Tragweite und Konsequenzen, die die Einwilligung als eine rechtserhebliche Erklärung mit sich bringt, einsehen zu können.[85] Daneben muss eine wirksame Einwilligungserklärung vorliegen. Diese erfolgt grundsätzlich formfrei.[86] Es bedarf jedoch der Nachweisbarkeit der erfolgten Einwilligung (Art. 7 Abs. 1 DSGVO). Diesen Nachweis muss der Verantwortliche der Datenverarbeitung führen, weshalb sich die Dokumentation der abgegebenen Einwilligungserklärungen empfiehlt.[87]

---

[82] GRIMM, DETLEF, Beschäftigtendatenschutz: § 26 Abs. 1 S. 1 BDSG nicht DSGVO-konform, ArbRB 2023, 131 (131).

[83] MEINECKE, DOMINIK, Anmerkung zu EuGH (Erste Kammer) Urt. v. 30.3.2023 – C-34/21, NZA 2023, 487 (493).

[84] FRANZEN in: ErfK ArbeitsR, § 26 BDSG Rn. 5.

[85] HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 7 Rn. 32; BUCHNER/KÜHLING in: Kühling/Buchner, DSGVO Art. 7 Rn. 56.

[86] HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 7 Rn. 35.

[87] STEMMER in: BeckOK Datenschutz, DSGVO Art. 7 Rn. 80, 86.

Zusätzlich ist der Verantwortliche aufgrund der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO dazu verpflichtet, die sich aus Art. 5 Abs. 1 DSGVO ergebenden Grundsätze der Datenverarbeitung einzuhalten. Geregelt in Art. 5 Abs. 1 DSGVO ist unter anderem auch die Pflicht zur rechtmäßigen Verarbeitung der Daten (lit. a). Die Einhaltung dieser Grundsätze muss der Verantwortliche nachweisen können.[88] Auch aus diesem Grund bedarf es der Dokumentation der Einwilligung. Zur Wirksamkeit der Einwilligung bedarf es allerdings lediglich einer unmissverständlichen Handlung, was auch die konkludente Einwilligungserklärung mittels eines eindeutigen Handelns nicht ausschließt.[89] Trotzdem muss ein eindeutig bejahendes Verhalten vorliegen. Durch diese Voraussetzung wird eine Einwilligung durch Schweigen oder vorangekreuzte Kästchen von vornherein ausgeschlossen.[90] Die Einwilligung muss bereits *vor* der Datenverarbeitung vorliegen und darf nicht erst im Nachhinein erklärt werden.[91]

4.1.2.2 Materielle Voraussetzungen einer wirksamen Einwilligung

In materieller Hinsicht sind weitere Anforderungen an die wirksame Einwilligung zu stellen. So stehen vor allem die notwendige Informiertheit und die Freiwilligkeit im Vordergrund. Daneben sind aber auch der Bestimmtheits- und der Zweckbindungsgrundsatz einzuhalten. Zudem ist die Einwilligung jederzeit widerrufbar, Art. 7 Abs. 3 S. 1 DSGVO.

Informiertheit liegt vor, wenn die einwilligende Person die Tragweite ihrer Einwilligungserklärung abschätzen kann und ihr bewusst ist, welche Daten zu welchem Zweck erhoben werden, wer diese verarbeitet und gegebenenfalls an welche Dritten sie weitergegeben werden.[92] Daher braucht es vor Abgabe der Einwilligung eine umfassende Aufklärung hinsichtlich der Folgen der Erklärung.[93] Dies ergibt sich schon aus dem Transparenzgebot des Art. 7 Abs. 2 DSGVO. Aus diesem folgt, dass die Einwilligung inhaltlich in leicht zugänglicher Form und in klarer, einfacher Sprache erfolgen muss. Es muss also einem juristischen Laien, etwa einem durchschnittlichen Verbraucher, möglich sein, den Inhalt der Einwilligung nachvollziehen zu können.[94] Hierbei sollten verschiedene Empfehlungen beachtet werden. Beispielsweise ist es sinnvoll, die Einwilligung auch als solche zu bezeichnen, da die

---

[88] PÖTTERS in: Gola DSGVO, Art. 5 Rn. 30.

[89] INGOLD in: Sydow/Marsch, Art. 4 DSGVO Rn. 170, Art. 7 DSGVO Rn. 23.

[90] Erwägungsgrund 32 DSGVO; HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 7 Rn. 36.

[91] INGOLD in: Sydow/Marsch, Art. 7 DSGVO Rn. 17.

[92] BUCHNER/KÜHLING in: Kühling/Buchner, DSGVO Art. 7 Rn. 59.

[93] HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 7 Rn. 40.

[94] WOLFF in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 523.

ausdrückliche Benennung dem juristischen Laien verdeutlicht, dass es sich um eine freiwillige Einwilligung seinerseits handelt und nicht um eine verpflichtende Erklärung.[95] Gleichzeitig muss sich der zeitliche Aufwand, um den Inhalt der Einwilligung zu erfassen, in Grenzen halten.[96]

Freiwilligkeit erfordert, wie sich aus Erwägungsgrund 42 zur DSGVO ergibt, echte Wahlfreiheit. Diese besteht nur dann, wenn sich an die Ablehnung der Einwilligung keine Nachteile anschließen. Allerdings kann nicht jeder kleine Nachteil zum Fehlen der Freiwilligkeit führen.[97] Die Einwilligung muss frei von jeglichem Zwang erfolgen, wobei auch ein innerer Zwang (beispielsweise bei einem Machtungleichgewicht, Erwägungsgrund 43 zur DSGVO) zu beachten ist.[98] Zudem besteht ein Kopplungsverbot, Art. 7 Abs. 4 DSGVO.

Weitere Anforderungen ergeben sich aus dem Bestimmtheitsgrundsatz und dem Zweckbindungsgrundsatz. Demnach muss die Einwilligung inhaltlich und hinsichtlich ihrer Modalitäten hinreichend bestimmt sein.[99] Die eindeutig festgelegten und legitimen Zwecke der Einwilligung sind für den Datenverarbeiter bindend und schließen es aus, dass dieser ohne Einholung einer erneuten Einwilligung zu anderen Zwecken Daten verarbeitet (Art. 6 Abs. 4 DSGVO).[100]

4.1.3 Einwilligung in die Verarbeitung besonders sensibler Daten nach Art. 9 Abs. 2 lit. a DSGVO

Der Analysedienst benötigt für seine Auswertungen insbesondere die Herzratenvariabilität. Die Herzratenvariabilität bezeichnet die Veränderungen des Abstands zwischen einzelnen Herzschlägen über einen bestimmten Zeitraum.[101] Die Herzratenvariabilität gehört zu den in Art. 4 Nr. 15 DSGVO definierten Gesundheitsdaten (s.o.).

Die Verarbeitung von Gesundheitsdaten unterliegt erhöhten Anforderungen. Gesundheitsdaten gehören zu den besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO.

---

[95] WOLFF in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 522; LG Berlin, ZD 2013, 451 (453).

[96] WOLFF in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 524.

[97] KLEMENT in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 7 DSGVO Rn. 48.

[98] HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 7 Rn. 50 f.

[99] INGOLD in: Sydow/Marsch, Art. 7 DSGVO Rn. 37.

[100] HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 7 Rn. 65.

[101] https://www.apotheken-umschau.de/gesund-bleiben/psyche/herzratenvariabilitaet-stress-messen-gezielt-entspannen-848387.html, zuletzt abgerufen am 30.11.2024.

Die Verarbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich verboten. Jedoch nennt auch Art. 9 DSGVO im zweiten Absatz Ausnahmen von diesem grundsätzlichen Verbot.

Auch für die Verarbeitung von Gesundheitsdaten kann die Einwilligung eine Rechtsgrundlage darstellen, Art. 9 Abs. 2 lit. a DSGVO. Aufgrund der Sensitivität der Gesundheitsdaten gibt es jedoch einige Besonderheiten.

Die Einwilligung muss sich explizit auf die besondere Kategorie von Daten beziehen. Dies geht aus dem Wortlaut des Art. 9 Abs. 2 lit. a DSGVO hervor: Erforderlich ist eine „ausdrückliche Einwilligung". Eine Einwilligung in diesem Sinne kann demnach nicht durch ein schlüssiges oder konkludentes Handeln erklärt werden, welches in sonstigen Fällen für die Erteilung der Einwilligung ausreicht.[102] Vielmehr braucht es eine ausdrückliche Einwilligung der betroffenen Person.[103] Da im WearPrivate-Szenario Gesundheitsdaten im Beschäftigtenkontext verarbeitet werden, ist § 26 Abs. 3 BDSG als speziellere Rechtsgrundlage heranzuziehen.

4.1.4 Einwilligungen in die Verarbeitung besonders sensibler Daten im Beschäftigtenkontext nach § 26 Abs. 3 S. 2, Abs. 2 BDSG

Art. 88 DSGVO ist eine Öffnungsklausel zugunsten der Mitgliedstaaten, die Deutschland mit der Schaffung des § 26 BDSG umgesetzt hat. Art. 9 Abs. 2 lit. b DSGVO enthält indes eine speziellere Öffnungsklausel für die Verarbeitung von besonders sensiblen Daten, welche in § 26 Abs. 3 BDSG für den Beschäftigtenkontext umgesetzt wurde. § 26 Abs. 3 BDSG regelt einen Zulässigkeitstatbestand für die Verarbeitung besonders sensibler Daten einerseits und erklärt andererseits den Absatz 2 des § 26 BDSG auch für Einwilligungen in die Verarbeitung besonders sensibler personenbezogener Daten für anwendbar, § 26 Abs. 3 S. 2 BDSG. § 26 Abs. 2 S. 1, 2 BDSG beschreibt die Besonderheiten, die hinsichtlich der Freiwilligkeit von Einwilligungen im Beschäftigtenkontext gelten. Auch muss die Einwilligung, obwohl sie grundsätzlich formfrei möglich ist, hier schriftlich oder elektronisch eingeholt werden, § 26 Abs. 2 S. 3 BDSG. Ferner hat der Verantwortliche die betroffene Person über den Zweck der Verarbeitung sowie über das Widerrufsrecht nach Art. 7 Abs. 3 DSGVO in **Textform** zu informieren, § 26 Abs. 2 S. 4 BDSG.

4.1.4.1 Freiwilligkeit und sozialer Druck

Im Beschäftigtenkontext liegt ein besonderes Augenmerk auf der Freiwilligkeit der abgegebenen Einwilligung. Es bedarf bei der Abgabe einer Einwilligung stets einer echten Wahlfreiheit. Diese liegt

---

[102] WEICHERT in: Kühling/Buchner, DSGVO, Art. 9 Rn. 47.

[103] KAMPERT in: Sydow/Marsch, Art. 9 DSGVO Rn. 13.

nur dann vor, wenn sich an die Ablehnung der Einwilligung keine Nachteile knüpfen.[104] Da auch ein innerer Zwang die Freiwilligkeit hindert, ist im Beschäftigtenkontext besondere Vorsicht geboten. Erwägungsgrund 43 zur DSGVO legt nahe, dass bei einem Machtgefälle die Einwilligung schon gar keine gültige Rechtsgrundlage darstellen kann. Dies ist jedoch nicht pauschal, sondern im Einzelfall, zu bestimmen. Sicherzustellen ist in jedem Fall, dass keine Nachteile bei Nichtabgabe der Einwilligung entstehen. Da Deutschland im Beschäftigtenkontext Öffnungsklauseln der DSGVO ausgefüllt hat, ist § 26 Abs. 2 BDSG zu beachten. Freiwilligkeit liegt insbesondere dann vor, wenn gleichgelagerte Interessen bestehen oder ein Vorteil an die Weitergabe der betreffenden Daten angeknüpft wird. Bei datenschutzrechtlichen Einwilligungen, die im Verhältnis Arbeitnehmer - Arbeitgeber abgegeben werden, muss daher im jeweiligen Einzelfall bestimmt werden, ob die erforderliche Freiwilligkeit gegeben war oder nicht. Eine faktisch erzwungene Einwilligung ist nicht wirksam. Insbesondere sind auch Verhaltensweisen zu betrachten, die dem sogenannten „Nudging“ zuzuordnen sind, und zwar aus zweierlei Perspektiven.

Einerseits könnte Druck am Arbeitsplatz dazu führen, dass eine faktische Verpflichtung der Arbeitnehmer dahingehend entsteht, dass sie dem Wearable-Einsatz zustimmen, obwohl sie nicht mit der Datenweitergabe einverstanden sind. Dies kann die Freiwilligkeit einer Einwilligung hemmen. Hier stellt sich sogar die Frage, ob überhaupt noch von Nudging gesprochen werden kann.

Nudging ist eine Art der Verhaltensbeeinflussung. Charakteristisch für diese ist, dass sie nicht notwendigerweise negativ für den Beeinflussten ist. Häufig wird er auch in die „richtige“, für ihn vorteilhafte Richtung gestupst. Hierin unterscheidet sich „Nudging“ von „Dark Patterns“. Bei „Dark Patterns“ kann auch eine Beeinflussung in die falsche, ungewollte Richtung eintreten. „Nudging“ ist zudem die deutlich eingeschränktere Beeinflussung. Im Falle einer Art „faktischen Verpflichtung“ ist daher fraglich, ob überhaupt noch von Nudging gesprochen werden kann, da es sich dann nicht mehr um ein „Anstupsen“ in diesem Sinne handelt, sondern um eine stärkere Verhaltensbeeinflussung, eigentlich schon um eine Verpflichtung, auch wenn der Zwang nicht auf einer Anordnung oder rechtlichen Verpflichtung beruht. Beim „Nudging“ wird häufig an das schlechte Gewissen appelliert oder an das Gefühl, etwas richtig machen zu wollen. Wird am Arbeitsplatz Druck auf die Arbeitnehmer ausgeübt, um sie zur Nutzung von Wearables zu drängen, handelt es sich jedoch um mehr als den Appell an das schlechte Gewissen. Vielmehr werden Arbeitnehmer zum Wearable-Einsatz gedrängt, weil sie sich vor Strafe fürchten oder Nachteile am Arbeitsplatz erwarten, wenn sie sich gegen den Einsatz der Wearables entscheiden. Dies geht über die Verhaltensbeeinflussung im Sinne von Nudging

[104] Erwägungsgrund 42 S. 5 zur DSGVO.

hinaus. Es handelt sich nicht mehr um ein bloßes „in die richtige Richtung stupsen“. Insbesondere kann es sein, dass der Wearable-Einsatz gerade nicht im Interesse des Arbeitnehmers liegen. Dies spricht gegen eine solche sehr eingeschränkte Verhaltensbeeinflussung.

„Nudging“ kann hier aber auch noch in einem anderen Kontext eine Rolle spielen. So ist darauf hinzuweisen, dass auch von den Wearables selbst eine Verhaltensbeeinflussung ausgehen kann.[105] Diese können nämlich autonome Entscheidungen beeinflussen. Die Beeinflussung erfolgt häufig im positiven Sinne, also beispielsweise, wenn eine Smartwatch anzeigt, dass man zu müde ist, um der geplanten Tätigkeit weiter nachzugehen. Dies kann dann den positiven Aspekt haben, dass eine Tätigkeit eingestellt wird, bevor aufgrund von Müdigkeit o.ä. Unfälle eintreten. Gleichzeitig sollten solche Beeinflussungen kritisch betrachtet werden, da sie doch die Entscheidungsautonomie des Einzelnen beeinflussen. Insbesondere können auch gerade solche Wearables, die gesundheitliche Daten erheben, einen Einfluss auf Verhaltensweisen haben. Diese Beeinflussung kann einen positiven Aspekt haben, beispielsweise dadurch, dass darauf hingewiesen wird, dass mehr Schlaf oder Bewegung für einen gesundheitsbewussten Lebensstil erforderlich ist. Andererseits könnte auch einem Ziel zuwider beeinflusst werden – z. B., wenn einer Person, die sich aufgrund einer Verletzung schonen muss, aufgezeigt wird, dass sie sich mehr bewegen soll.

Grundsätzlich ist es problematisch, wenn autonome Entscheidungen durch Technologieeinsatz beeinflusst werden. Daher kommen in diesem Bereich ethische Bedenken auf, die im Rahmen des Projekts berücksichtigt werden müssen. Jedoch ist zu beachten, dass in diesem Fall tatsächlich eher ein Anstupsen in die richtige Richtung erfolgt. So wird in der Regel darauf hingewiesen, dass ein bestimmtes Verhalten positiv zum Erhalt des Gesundheitsstatus´ oder zum Schutz vor Unfällen beitragen würde. Zudem kann der Wearable-Einsatz so eingestellt werden, dass jede Person noch selbst über ihr Verhalten entscheiden kann – beispielsweise dadurch, dass nur sie selbst Informationen über die Wearable-Daten erhält und diese Daten erst mit Zustimmung und im Nachgang an den Arbeitgeber übermittelt werden, sodass die Angst vor dessen Reaktion stark eingeschränkt wird. In diesem Fall bleibt es bei einer autonomen Entscheidung des Arbeitnehmers. Dies gilt insbesondere, weil sich Wearables auch an die persönlich gesteckten Ziele anpassen lassen, sodass auch in Sonderfällen die Bedürfnisse angepasst werden können. Trotzdem sollte dieser Punkt im Auge behalten werden.

---

[105] CONRADIE, The moral opportunities and perils of smart wearables for decisional autonomy.

4.1.4.1.1 Gegenmaßnahmen zur Abhilfe von sozialem Druck

Um sozialem Druck zu begegnen, der beim Einsatz von Wearables im Arbeitskontext eine Rolle spielt, können verschiedene Maßnahmen ergriffen werden.

4.1.4.1.2 Einwilligung als Rechtsgrundlage

Schon die grundsätzliche Entscheidung dafür, den Wearable-Einsatz an die Einwilligung von Mitarbeitern zu knüpfen, statt ihn auf andere Rechtsgrundlagen (s.u.) zu stützen, kann sozialem Druck entgegenwirken. So ist zumindest die Möglichkeit gegeben, dass die Arbeitnehmer sich auch gegen den Wearable-Einsatz entscheiden können.

4.1.4.1.3 Schriftliche Zusicherung des Arbeitgebers

Eine zentrale Voraussetzung für den Einsatz von Wearables am Arbeitsplatz ist, dass Arbeitnehmer weder durch die Ablehnung der Nutzung des Wearables noch durch die gesammelten Daten benachteiligt werden. Letzteres kann durch die Nutzung von Methoden der Anonymisierung verhindert werden: Weiß der Arbeitgeber ohnehin nicht, welchem Arbeitnehmer welche Daten zuzuordnen sind, ist es zumindest unmöglich, dass einzelne Arbeitnehmer Nachteile erhalten. Die Benachteiligung von Gruppen ist hingegen nicht ausgeschlossen.

Solche Benachteiligungen von Arbeitnehmern, sei es von einzelnen oder von einer Gruppe von Arbeitnehmern, gilt es zu vermeiden. Hilfreich kann es sein, eine zusätzliche, verbindliche Vereinbarung mit dem Arbeitgeber zu treffen, in der dieser zusagt, dass keine Nachteile aus dem Wearable-Einsatz am Arbeitsplatz erwachsen. Durch die verbindliche Zusicherung des Arbeitgebers haben die Arbeitnehmer zumindest eine rechtliche Handhabe sich zu wehren, sollte der Eindruck entstehen, dass der Arbeitgeber aufgrund der Wearable-Daten einen oder mehrere Arbeitnehmer benachteiligt.

4.1.4.1.4 Wahl des Wearables

Allerdings ist auch mit der Heranziehung einer Einwilligung als Rechtsgrundlage nicht sichergestellt, dass Arbeitnehmer frei von Druck entscheiden können. Das Gefühl von einem Arbeitgeber zur Wearable-Nutzung gezwungen zu sein, kann auch bei der faktischen Möglichkeit, eine Einwilligung zu verweigern, gegeben sein. Dies hängt damit zusammen, dass der Arbeitgeber regelmäßig überlegen scheint und der Arbeitnehmer in einem Abhängigkeitsverhältnis zum Arbeitgeber steht. Insbesondere dann, wenn das betreffende Wearable sichtbar am Körper getragen werden muss, ist es stets für alle ersichtlich, ob der jeweilige Arbeitnehmer der Wearable-Nutzung zugestimmt hat oder nicht. Hilfreich könnte es an dieser Stelle bereits sein, wenn solche Wearables genutzt werden, die am Körper getragen werden können, ohne von außen sichtbar zu sein, wie beispielsweise ein Brustgurt, der unter

der Kleidung getragen wird. In diesem Szenario könnte ein Arbeitnehmer zumindest nach außen verbergen, dass er sich gegen die Wearable-Nutzung entschieden hat.

4.1.4.1.5 Transparenz gegenüber Arbeitnehmern

Grundlegend wichtig und auch schon zur Einhaltung datenschutzrechtlicher Pflichten erforderlich ist die Transparenz gegenüber Arbeitnehmern. Die Aufklärung, wie genau die Wearable-Nutzung ablaufen wird, welche Daten erhoben werden und was mit diesen passiert, ist unerlässlich. Hilfreich ist es, Informationen nicht nur in Textform zur Verfügung zu stellen, sondern beispielsweise Schulungen anzubieten oder visuell aufbereitete Informationen zur Verfügung zu stellen. Die Transparenz gegenüber den Arbeitnehmern ist Grundvoraussetzung für jede rechtskonforme Datenverarbeitung im Kontext von WearPrivate.

4.1.4.1.6 Anonymität und Anonymisierung

Ein weiterer wichtiger Aspekt ist die Anonymisierung. Geplant ist, dass weder der Analyseservice noch der Arbeitgeber weiß, wem welche Daten zuzuordnen sind. Dabei soll spezifischen Bedrohungsszenarien begegnet werden (siehe hierzu D 3.1 Abschnitt Schutzmaßnahmen durch Datenaggregierung und -anonymisierung). Hierzu gehören beispielsweise unbeabsichtigte Datenlecks beim Analysedienstleister, Appanbieter oder Arbeitgeber. Auch soll verhindert werden, dass durch einen böswilligen Akteur oder durch das Zusammenwirken von Analysedienstleister und Arbeitgeber die Anonymität aufgehoben oder durchbrochen wird. Die Anonymität soll durch verschiedene Maßnahmen gesichert werden.

So soll bereits die Verteilung der Wearables (soweit diese tatsächlich vom Arbeitgeber verteilt werden) zufällig ablaufen, sodass nicht ersichtlich ist, welcher Arbeitnehmer über welches Wearable verfügt. Dies kann beispielsweise mithilfe einer Grabbelkiste geschehen. Falls die Arbeitnehmer sich die Wearables selbst anschaffen werden, können diese frei entscheiden, welches Wearable sie wählen, soweit das gewählte Wearable mit dem Service und der App kompatibel ist.

Auch nach der Verteilung der Wearables sollen weitere Maßnahmen ergriffen werden, um die Anonymität der Arbeitnehmer zu schützen. Beispielsweise sollen auch die Daten, die die Arbeitnehmer in der App angeben müssen (Stammdaten), leicht verrauscht werden. Daneben sind Altersklassen oder Gewichts- und Größenspannen denkbar. Gemeint ist damit eine Generalisierung. Zur Generalisierung fällt sowohl die Bildung von Prädikaten als auch die Vorverarbeitung von Daten. (siehe hierzu D 3.1 Abschnitt Schutzmaßnahmen durch Datenaggregierung und -anonymisierung).

Werden Daten nur anonym verarbeitet und ist eine Identifizierung für den Arbeitgeber faktisch nicht möglich, so ist ein besonders starker Schutz für den Arbeitnehmer gegeben. Durch diese

Schutzmaßnahme sind auch Benachteiligungen einzelner Arbeitnehmer ausgeschlossen. Möglich wäre höchstens eine Benachteiligung einer ganzen Gruppe, wenn der Arbeitgeber mit dem anonymisierten Gruppenbericht nicht einverstanden sein sollte. Dieser Gefahr ist mit anderen Mitteln wie beispielsweise einer verbindlichen Zusicherung des Arbeitgebers zu begegnen (s.o.)

4.1.4.1.7 Selbstbestimmung und Einstellungsmöglichkeiten für die Arbeitnehmer

Von besonderer Bedeutung ist ebenfalls die Sicherstellung der (informationellen) Selbstbestimmung der Arbeitnehmer. Das Recht auf informationelle Selbstbestimmung beschreibt das Recht, selbst über die Verwendung und Preisgabe personenbezogener Daten zu entscheiden. Den Arbeitnehmern ist ein möglichst großer Spielraum hinsichtlich des Umgangs mit ihren personenbezogenen Daten einzuräumen. Erreicht werden soll dies im Projekt WearPrivate unter anderem mit verschiedenen Einstellungsmöglichkeiten in der App: So soll der Arbeitnehmer wählen können, ob seine Rohdaten wenig, moderat oder viel verrauscht werden sollen. Da das Verrauschen möglicherweise Auswirkungen auf die Genauigkeit der Analysedaten haben kann, sollten die Nutzer vor ihrer Entscheidung hinreichend über die Konsequenzen aufgeklärt werden. Darüber hinaus sollen auch Opt-In/Opt-Out Möglichkeiten eingeräumt werden, durch die Arbeitnehmer darüber entscheiden können, ob sie an einem Gruppenreport teilnehmen möchten. Somit bleibt die Letztentscheidung darüber, ob den Arbeitgeber verarbeitete Daten der Arbeitnehmer erreichen, beim Arbeitnehmer. Fürchtet der Arbeitnehmer also beispielsweise, dass aufgrund der gesammelten Daten ein schlechter Eindruck entstehen könnte, kann er die Aufnahme in den Gruppenreport ablehnen.

4.1.4.1.8 Vorteile und Belohnungen für Arbeitnehmer

Aus § 26 Abs. 2 S. 2 BDSG ergibt sich, dass Einwilligungen im Beschäftigtenkontext insbesondere dann freiwillig sein können, wenn beschäftigten Personen ein rechtlicher oder wirtschaftlicher Vorteil eingeräumt wird oder die Interessen der Arbeitgeber und der beschäftigten Personen gleichgelagert sind. Denkbar wäre es daher auch, den betroffenen Personen (bzw. Arbeitnehmern) einen Vorteil oder eine Belohnung in Aussicht zu stellen, wenn sie die Wearables nutzen und damit einen wesentlichen Teil zur Verbesserung der Arbeitssicherheit bzw. des Arbeitsschutzes beitragen.

4.1.4.1.9 Fazit

Es gibt eine Reihe an Maßnahmen, die ergriffen werden könnten, um sozialen Druck entgegenzuwirken. Sinnvoll ist die Kombination der oben genannten Maßnahmen. So wird erst die Kombination aus der Implementierung von Selbstbestimmungseinstellungen, Anonymität und gleichzeitiger schriftlicher Zusicherung des Arbeitgebers, dass keine Nachteile für die Arbeitnehmer aus den Wearable-Daten entstehen, effektiv sozialen Druck lindern können.

4.1.5 Anwendung auf WearPrivate

Der Einsatz von Wearables kann im Beschäftigtenkontext auf eine Einwilligung gestützt werden. Im Anwendungsfall von WearPrivate wäre es denkbar, dass der Arbeitgeber seinen Mitarbeitern zunächst die Möglichkeit der Wearable-Nutzung aufzeigt und dann denjenigen Arbeitnehmern, die sich einverstanden erklären, den Fitnessgurt zur Nutzung überlässt.

Entscheidet sich der Arbeitgeber in diesem Fall für eine Einwilligung als Rechtsgrundlage für die Datenverarbeitung, sind eine Reihe an Voraussetzungen zu beachten.

1. Die Informiertheit der Arbeitnehmer ist sicherzustellen. Der Arbeitgeber hat die Arbeitnehmer angemessen zu informieren. Die Arbeitnehmer sind mindestens darüber zu informieren, dass die Herzratenvariabilität gesammelt wird. Des Weiteren muss der Arbeitgeber darlegen, wie mit der Herzratenvariabilität die Arbeitssicherheit erhöht wird. Den Arbeitnehmern ist klar zu kommunizieren, dass die Herzratenvariabilität ein Gesundheitsdatum ist und welche Schlüsse aus den gesammelten Daten gezogen werden können. Ferner ist den Arbeitnehmern aufzuzeigen, wer für die Datenverarbeitung verantwortlich und damit auch Ansprechpartner für die Geltendmachung von Betroffenenrechten ist. Auch über das bestehende Widerrufsrecht nach Art. 7 Abs. 3 S. 1 DSGVO sind die Arbeitnehmer zu informieren. Gemäß § 26 Abs. 2 S. 4 BDSG sind die Informationen in Textform zur Verfügung zu stellen. Über eventuelle Übermittlungen von Daten in ein Drittland sind die Arbeitnehmer ebenso zu informieren.
2. Die Einwilligungen sind im Einklang mit Art. 9 Abs. 2 lit. a DSGVO ausdrücklich einzuholen und nicht auf konkludentes Verhalten zu stützen.
3. Den Arbeitnehmern ist freie Wahl hinsichtlich der Nutzung des Fitnessgurtes zu geben. Dies erfordert vor allem, dass negative Folgen bei Ablehnung der Einwilligung ausgeschlossen werden. Hierfür ist zumindest eine Zusicherung des Arbeitgebers erforderlich. Bestenfalls könnte eine Vertragsklausel diesbezüglich aufgenommen werden, wodurch auch konkrete Ansprüche geltend gemacht werden können.

   Ferner sollte jede Form von Zwang vermieden werden. Dies umfasst auch unterschwelligen Druck oder Kritik, durch den sich Arbeitnehmer genötigt fühlen könnten, den Fitnessgurt entgegen ihrem eigentlichen Willen zu nutzen. Jedoch ist zu beachten, dass es unmöglich ist, sozialen Druck wirksam auszuschließen, auch wenn man sich zuvor darauf verständigt. Wichtig ist es daher, dass Maßnahmen ergriffen werden, um dem entgegenzuwirken. Diese Maßnahmen können unterschiedliche Formen annehmen. Denkbar sind sowohl Aufklärungs- und Informationsgespräche als auch die Einrichtung von Belohnungen oder sonstigen

Vorteilen für die Arbeitnehmer, wenn sie sich dazu entschließen den Fitnessgurt zu tragen. Ferner können zu diesem Ziel auch Anonymisierungsmaßnahmen beitragen. Erhält der Arbeitgeber beispielsweise nur ein anonymes Feedback über eine Gruppe von Arbeitnehmern, ist für ihn nicht offensichtlich, welcher Arbeitnehmer teilnimmt. Da der Fitnessgurt auf der Haut sitzen muss, ist auch nicht von außen erkennbar, wer den Gurt trägt und wer nicht. (s.o.)

4.2 Verarbeitung sensibler Daten zum Zwecke des Beschäftigungsverhältnisses (§ 26 Abs. 3 S. 1 BDSG)

Denkbar wäre es auch, die Datenverarbeitung auf § 26 Abs. 3 S. 1 BDSG zu stützen. Aus § 26 Abs. 3 S. 1 BDSG, der auf der Öffnungsklausel gemäß Art. 9 Abs. 2 lit. b iVm Abs. 4 DSGVO beruht, ergibt sich in Bezug auf sensible personenbezogene Daten Folgendes: Die Verarbeitung im Beschäftigtenverhältnis ist zulässig, soweit sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und keine Hinweise darauf bestehen, dass schutzwürdige Interessen der Arbeitnehmer überwiegen. § 26 Abs. 3 S. 1 BDSG stellt keine eigenständige Rechtsgrundlage dar, sondern ist nur in Verbindung mit einer anderen Vorschrift (aus dem Sozial- oder Arbeitsrecht) anwendbar.[106] Die bloße Heranziehung von legitimen Interessen des Arbeitgebers reicht daher nicht aus, wenn keine rechtliche Verpflichtung existiert (anders als in § 26 Abs. 1 S. 1 BDSG).[107]

Es handelt sich bei § 26 Abs. 3 BDSG um eine Spezifizierung von Art. 9 DSGVO. § 26 Abs. 3 BDSG ist lex specialis (aufgrund Spezialität vorrangig anzuwenden) gegenüber § 26 Abs. 1 und Abs. 2, da er sich spezifisch auf die Verarbeitung von sensiblen Daten nach Art. 9 DSGVO bezieht

Besteht eine Pflicht aus dem Arbeits- oder Sozialrecht, bedarf es ferner einer Verhältnismäßigkeitsprüfung, bei der die widerstreitenden Interessen von Arbeitgeber und Arbeitnehmer in einen angemessenen Ausgleich zu bringen sind.[108] Es stehen sich die Interessen des Arbeitnehmers an dem Schutz seines Allgemeinen Persönlichkeitsrechts (insb. Recht auf informationelle Selbstbestimmung) und des Arbeitgebers gegenüber. Der Arbeitgeber hat Interesse an

---

[106] GOLA/PÖTTERS in: Gola/Heckmann, § 26 BDSG, Rn. 76

[107] GOLA/PÖTTERS in: Gola/Heckmann, § 26 BDSG, Rn. 77. Entsprechende Pflichten können beispielsweise aus § 80 BetrVG für die Unterrichtung des Betriebsrates, MASCHMANN in: Kühling/Buchner, § 26 BDSG, Rn. 24, oder aus dem Informationsschutzgesetz bezüglich einer Corona-Infektion/des Impfstatus eines Arbeitnehmers, FRANZEN in: Erfurter Kommentar zum Arbeitsrecht, 23. Auflage 2023, § 26 BDSG, Rn. 46, folgen.

[108] GOLA/PÖTTERS in: Gola/Heckmann, § 26 BDSG, Rn. 75.

der vereinfachten Koordination des Einsatzes der Arbeitnehmer[109], an einem effektiven Gesundheitsschutz (auch Vorbeugung von Krankheiten/Verletzungen) und der Erhöhung der Arbeitssicherheit.

Zu prüfen ist insbesondere die Erforderlichkeit geplanter Maßnahmen.[110] Sie liegt vor, wenn das mildeste aller gleich geeigneten Mittel zur Anwendung kommt.[111]

4.2.1 Anwendung auf WearPrivate

4.2.1.1 Verpflichtung aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes

§ 26 Abs. 3 S. 1 BDSG ist nur in Kombination mit einer weiteren Rechtsgrundlage, die dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder dem Sozialschutz entstammen, anwendbar. Die für den vorliegenden Fall heranzuziehende Pflicht könnte sich aus dem Arbeitsschutzgesetz (ArbSchG) ergeben. Das Arbeitsschutzgesetz dient der Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes bei der Arbeit.[112] Das ArbSchG regelt unter anderem Pflichten des Arbeitgebers, insbesondere dahingehend, welche Maßnahmen er zu ergreifen hat, um die Arbeitnehmer zu schützen. Nach § 2 Abs. 1 ArbSchG sind „Maßnahmen“ im Sinne des ArbSchG Maßnahmen zur Verhütung von Unfällen bei der Arbeit und arbeitsbedingten Gesundheitsgefahren einschließlich Maßnahmen der menschengerechten Gestaltung der Arbeit. Welche Pflichten den Arbeitgeber treffen ergibt sich aus den §§ 3 ff. ArbSchG. In § 3 ArbSchG findet sich eine Regelung zu den Grundpflichten des Arbeitgebers. Nach § 3 Abs. 1 ArbSchG ist der Arbeitgeber dazu „verpflichtet, die erforderlichen Maßnahmen des Arbeitsschutzes unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen. Er hat die Maßnahmen auf ihre Wirksamkeit zu überprüfen und erforderlichenfalls sich ändernden Gegebenheiten anzupassen. Dabei hat er eine Verbesserung von Sicherheit und Gesundheitsschutz der Beschäftigten anzustreben.“ Die §§ 4 – 14 ArbSchG enthalten spezielle Pflichten des Arbeitgebers, die auf den Grundpflichten nach § 3 ArbSchG beruhen.[113] Die Generalklausel in § 3 Abs. 1 ArbSchG regelt für den Arbeitgeber eine „umfassende und präventive Handlungspflicht, die erforderlichen Maßnahmen des Arbeitsschutzes unter Berücksichtigung der Umstände zu treffen, die

---

[109] RAMMOS in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, § 25 Rn. 88.

[110] GRÄBER/NOLDEN in: Paal/Pauly, § 26 BDSG, Rn. 40.

[111] TIEDEMANN in: Sydow/Marsch, § 26 BDSG, Rn. 22.

[112] ROLOFF in: ErfK Arbeitsrecht, § 1 ArbSchG Rn. 1.

[113] ROLOFF in: ErfK Arbeitsrecht, § 3 ArbSchG Rn. 1.

Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen.“.[114] Die Maßnahmen, die der Arbeitgeber ergreift, sind zu überprüfen und gegebenenfalls zu erneuern.[115] Der in WearPrivate geplante Einsatz von Wearables zur Erhöhung des Gesundheitsschutzes und der Arbeitssicherheit könnte eine erforderliche Maßnahme im Sinne des § 3 ArbSchG darstellen – § 3 Abs. 1 ArbSchG könnte in Verbindung mit § 26 Abs. 3 S. 1 BDSG eine Rechtsgrundlage für die Verarbeitung der sensiblen Daten der Arbeitnehmer dienen. Hierfür müsste allerdings zunächst eine Rechtspflicht des Arbeitgebers aus § 3 ArbSchG erwachsen. Der Arbeitgeber hat nach § 3 Abs. 1 ArbSchG „erforderliche“ Maßnahmen zu ergreifen. Der Hinweis auf die Erforderlichkeit in der Vorschrift schafft eine Verbindung zu § 5 Abs. 1 ArbSchG, der Gefährdungsbeurteilung.[116] Demnach hat der Arbeitgeber auf Grundlage einer Beurteilung der mit der zu verrichtenden Arbeit verbundenen Gefährdung zu beurteilen, welche Maßnahmen erforderlich sind. Die in diesem Zusammenhang ermittelten Gefährdungen sind mit den in § 4 BDSG niedergelegten allgemeinen Anforderungen aus dem Arbeitsschutzrecht sowie weiteren besonderen Anforderungen, die sich aus anderen Vorschriften ergeben, abzugleichen.[117] Neben diesen Anforderungen ist grundsätzlich der Verhältnismäßigkeitsgrundsatz[118], der eine Prüfung des legitimen Interesses des Arbeitgebers, der Geeignetheit und der Erforderlichkeit sowie der Angemessenheit (Verhältnismäßigkeit im engeren Sinne) erfordert, zu beachten.

Fraglich mithin ist, ob der Wearable-Einsatz als erforderliche Maßnahme einzuschätzen ist. Nach § 4 Nr. 1 ArbSchG ist die Arbeit so zu gestalten, „dass eine Gefährdung für das Leben sowie die physische und die psychische Gesundheit möglichst vermieden und die verbleibende Gefährdung möglichst geringgehalten wird“. Bei der Wahl der jeweiligen Maßnahme sind der Stand der Technik, die Arbeitsmedizin und Hygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse zu beachten, § 4 Nr. 3 ArbSchG. Der Einsatz von Wearables, die die HRV sowie Beschleunigungsdaten überwachen, um dadurch schnell besondere Belastung oder auch Stürze zu erkennen, kann dazu beitragen, Gefährdungen für Leib und Leben zu minimieren bzw. zu vermeiden. Dies gilt jedoch nur insoweit, wie die Belastungsmessung tatsächlich dazu beitragen soll, gefährliche Handlungen zu vermeiden – beispielsweise, wenn aufgrund des besonderen Stresslevels keine Arbeit mehr an einem gefährlichen Ort wie einer Hochspannungsleitung mehr vorgenommen werden soll. Anders wäre dies

---

[114] EBD.

[115] EBD.

[116] KOHTE in: Kollmer/Klindt/Schucht, § 3 Rn. 26.

[117] KOHTE in: Kollmer/Klindt/Schucht, § 3 Rn. 27.

[118] EBD.

dann zu beurteilen, wenn das gemessene Stresslevel „nur“ dafür verwendet werden soll, Arbeit effizienter aufzuteilen. Im ersten Fall ließe sich jedoch unter Beachtung der Grundsätze aus § 4 ArbSchG und des Grundsatzes der Verhältnismäßigkeit der Wearable-Einsatz als erforderliche Maßnahme argumentieren. Jedoch sagt § 4 Nr. 2 ArbSchG grundsätzlich aus, dass Gefahren an der Quelle zu bekämpfen sind. Dies könnte gegen die Erforderlichkeit des Wearable-Einsatzes sprechen. Allerdings gilt zu beachten, dass nicht jede Gefahr an der Quelle bekämpft werden kann und es daher auch Sekundärmaßnahmen bedarf. Arbeitet eine Person in einem gefährlichen Umfeld, so kommen häufig nur Sekundärmaßnahmen als Schutzmaßnahmen in Betracht. Die Erforderlichkeit des Wearable-Einsatzes ist daher zu bejahen.

§ 3 Abs. 1 ArbSchG kann mithin als Rechtspflicht für § 26 Abs. 3 S. 1 BDSG herangezogen werden. Auch hinsichtlich der Datenverarbeitung gilt es, die Verhältnismäßigkeit der Verarbeitung zu überprüfen.

4.2.1.2 Legitime Ziele des Arbeitgebers

Zunächst ist die Frage zu stellen, ob der Arbeitgeber mit der Datenverarbeitung legitime Ziele verfolgt. Dabei ist festzustellen, welche Zwecke vom Arbeitgeber mit der Datenverarbeitung verfolgt werden und ob diese legal und nachvollziehbar sind. Im nun festgelegten Anwendungsfall von WearPrivate stehen die Erhöhung der Arbeitssicherheit und des Gesundheitsschutzes im Vordergrund. Hierbei handelt es sich um nachvollziehbare Ziele, deren Verfolgung auch nicht im Widerspruch zu gesetzlichen Regelungen steht.

4.2.1.3 Geeignetheit des Einsatzes des Fitnessgurtes

Des Weiteren müssen die eingesetzten Maßnahmen geeignet sein. Geeignetheit ist anzunehmen, wenn die geplante Maßnahme die legitimen Zwecke fördert und nicht völlig ungeeignet ist. Mit dem Fitnessgurt wird die Herzratenvariabilität aufgezeichnet. Damit besteht die Möglichkeit, Arbeitnehmer zu warnen, wenn ihre Herzrate in einen kritischen Bereich gehen. Insbesondere bei Arbeiten in einem Hochrisiko-Bereich, also beispielsweise an Hochspannungsgeräten, kann die Warnung zur Verhinderung von Unfällen beitragen.

4.2.1.4 Erforderlichkeit des Einsatzes des Fitnessgurtes

Erforderlichkeit ist anzunehmen, wenn es sich bei der geplanten Maßnahme um das mildeste aller gleich geeigneten Mittel handelt. Diese Voraussetzung muss in jedem Einzelfall geprüft werden. Es müssen dann jeweils die milderen Mittel ausgemacht werden, mit denen die Ziele des Arbeitgebers auch erreicht werden könnten. Ob diese dann gleich effektiv, aber weniger einschneidend sind, ist im Einzelfall zu klären. Im Anwendungsfall von WearPrivate ist daher die Frage zu stellen, ob es ein Mittel gibt, mit dem die Arbeitssicherheit und die Gesundheit der Arbeitnehmer ebenso gut geschützt

werden kann wie durch den Einsatz des Fitnessgurtes. Für den Fitnessgurt spricht, dass er sehr genaue Ergebnisse und Daten liefert. Die Qualität der Daten verhindert Fehlalarme und ermöglicht eine genaue Bewertung der Gefährlichkeit der jeweiligen Situation. Gegen den Fitnessgurt könnte hingegen der Tragekomfort sprechen. Es handelt sich dabei um ein Wearable, welches eng anliegend am Körper getragen werden muss, was zumindest manchen Arbeitnehmern unangenehm sein könnte. Gerade für Frauen, die Büstenhalter tragen, könnte der Fitnessgurt unangenehm eng anliegen. Jene Überlegungen sind bei der Analyse der Erforderlichkeit einzubeziehen. Ein milderes Mittel könnte beispielsweise der Einsatz einer SmartWatch sein, die weniger nah am Körper getragen werden muss. Für den Einsatz einer SmartWatch wäre beispielsweise auch keine Angabe betreffend des Gewichts oder Körperumfangs erforderlich. Der Fitnessgurt existiert in verschiedenen Größen[119], weshalb diesbezüglich Angaben der Arbeitnehmer erforderlich wären. Jedoch bleibt darauf zu verweisen, dass der Fitnessgurt wesentlich genauere Ergebnisse liefert als eine SmartWatch. Mithin können die beiden Wearables nicht immer als „gleich wirksam“ eingeordnet werden.

4.2.1.5 Angemessenheit

Angemessenheit liegt vor, wenn die Interessen des Arbeitgebers die widerstreitenden Interessen der Arbeitnehmer überwiegen.

Auf Seiten des Arbeitgebers steht das Ziel der Sicherstellung des Arbeits- und Gesundheitsschutzes. Dieses Ziel soll unter anderem durch die Verhinderung von Arbeitsunfällen sowie die frühzeitige Erkennung gesundheitlicher Probleme erreicht werden. Auch wenn mit dem Fitnessgurt keine medizinischen Diagnosen gestellt werden können, kann die Feststellung eines hohen Stresslevels trotzdem Überlastung vorbeugen. Darüber hinaus können auch Auffälligkeiten bei der Herzratenvariabilität zumindest erste Anzeichen für Herzprobleme und hilfreich bei der Erkennung ebendieser sein.

Dem stehen jedoch auch Interessen der Arbeitnehmer entgegen. Der einzelne Arbeitnehmer kann sich auf sein Recht auf informationelle Selbstbestimmung berufen und hat grundsätzlich das Recht, selbst darüber zur entscheiden, welche seiner personenbezogenen Daten er herausgeben will. Dies gilt insbesondere im Bereich besonders sensibler Gesundheitsdaten. Bei Gesundheitsdaten gilt zudem auch noch ein sogenanntes Recht auf „Nichtwissen“. Demnach steht jedem Menschen grundsätzlich frei, selbst zu entscheiden, ob er über körperliche Defizite Bescheid wissen möchte oder nicht.

---

[119] https://www.polar.com/de/sensors/h10-heart-rate-sensor, zuletzt abgerufen am 30.11.2024.

Zudem kann das Gefühl des ständigen Überwachtwerdens entstehen, wenn Wearables am Körper getragen werden sollen. Eine Totalüberwachung ist grundsätzlich nicht zulässig.[120] Der Fitnessgurt muss eng am Körper getragen werden, damit er seine volle Funktionalität entfalten kann und auch die Fehlerquote niedrig gehalten wird. Das beschriebene Problem haben die Partner jedoch erkannt und verschiedene Maßnahmen ergriffen, um dem entgegenzuwirken. Unter anderem sollen dem Arbeitnehmer Mechanismen an die Hand gegeben werden, um bereits im Vorhinein durch Einstellungen den Datenfluss zu kontrollieren. Den Arbeitnehmern werden mithin weitreichende Möglichkeiten gegeben, um ihr Recht auf informationelle Selbstbestimmung effektiv auszuüben. Aufgrund der ergriffenen Gegenmaßnahmen wiegen die Interessen der Arbeitnehmer weniger schwer und das Interesse des Arbeitgebers an einem sicheren Arbeitsplatz überwiegt. Darüber hinaus gilt es auch zu beachten, dass die Sicherheit des Arbeitsplatzes, die Verhinderung von Unfällen sowie der Gesundheitsschutz Ziele sind, die auch im Interesse der Arbeitnehmer liegen und ihnen bei entsprechenden Schutzmaßnahmen zugutekommen.

Allerdings sollen unter Umständen auch private Bereiche überwacht werden, etwa zur Kalibrierung der Messung anhand einer persönlichen Baseline. Beispielsweise kann eine Datenverarbeitung mit dem Ziel, herauszufinden, wie sich zu wenig Schlaf auf die Arbeitsleistung auswirkt, nicht durch § 26 Abs. 3 S. 1 BDSG gerechtfertigt werden. Empfehlungen für einen gesünderen Lebensstil erlauben keinen Zugriff des Arbeitgebers auf die Daten der Arbeitnehmer. Die Daten, die durch die Wearables erhoben werden, müssen der Arbeitssicherheit und dem Gesundheitsschutz dienen. Nur dann kann § 26 Abs. 3 S. 1 BDSG als Rechtsgrundlage dienen.

Grundsätzlich ist es denkbar, den Einsatz von Wearables auf § 26 Abs. 3 S. 1 BDSG zu stützen. Es dürfen jedoch ausschließlich Daten erhoben werden, die einen Bezug zur Arbeitssicherheit aufweisen und erforderlich sind, um diese zu erhöhen. Gleichzeitig ist die Erstellung eines lückenlosen Ortungsprofils nicht mit § 26 Abs. 3 S. 1 BDSG vereinbar. Die Abwägung muss jeweils für die Anwendungsfälle einzeln vorgenommen werden und es müssen die besonderen Umstände jeder Situation betrachtet werden.

4.3 Verarbeitung sensibler Daten zum Zwecke der Versorgung im Gesundheitsbereich (Art. 9 Abs. 2 lit. h DSGVO)

Mit Art. 9 Abs. 2 lit. h DSGVO gibt es noch eine dritte mögliche Rechtsgrundlage, auf die sich die Datenverarbeitung mittels Wearables im Beschäftigtenkontext stützen lässt. Die Arbeitsmedizin befasst sich mit der Wechselbeziehung von Anforderungen und Organisation der Arbeit einerseits und

[120] KORT, RdA, 2018, 24 (28).

der gesundheitlichen Verfassung des Beschäftigten andererseits. Art. 9 Abs. 2 lit. h DSGVO ist in Verbindung mit Art. 9 Abs. 3 DSGVO zu sehen (es bedarf des medizinischen Fachpersonals, welches einer beruflichen Schweigepflicht unterliegt). Es ist in jedem Fall strikt zu unterscheiden, ob die Daten für die arbeitsplatzspezifische Sicherheit wichtig sind oder nicht. Helfen sie nur dabei, sich einen gesünderen Lebensstil anzueignen, so ist der Zugriff des Arbeitgebers nicht möglich.[121]

4.4 Weitere Rechtsgrundlagen nach Art. 6 Abs. 1 lit. b-f DSGVO

Wie oben beschrieben findet § 26 Abs. 1 S. 1 BDSG in seiner derzeitigen Form keine Anwendung. Für Szenarien des Workloggings werden, bevor § 26 Abs. 1 S. 1 BDSG überarbeitet wird, die Art. 6 Abs. 1 lit. b, lit. c oder lit. f DSGVO heranzuziehen sein.[122] Zu prüfen ist dann, ob das Worklogging für die Erfüllung eines Vertrages, bspw. eben des Arbeitsvertrages[123], oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Erforderlich für die Erfüllung eines Vertrages ist die Verarbeitung personenbezogener Daten dann, wenn sie notwendig ist, um *vorvertragliche Anfragen* zu bearbeiten, einen Vertragsschluss vorzunehmen, eingegangene Vertragspflichten zu erfüllen oder eigene Rechte geltend zu machen.[124] Für Art. 6 Abs. 1 lit. c bedarf es einer Pflicht kraft objektiven Rechts, keiner lediglich vertraglich entstandenen Pflicht.[125] Eine solche kann sich beispielsweise aus Tarif- und Betriebsvereinbarungen ergeben.[126] Art. 6 Abs. 1 lit. f DSGVO hingegen erfordert eine Interessenabwägung, ist allerdings nicht einschlägig für Verarbeitungen, die im Rahmen der Erfüllung der Aufgaben von Behörden durchgeführt werden, Art. 6 Abs. 1 UAbs. 2 DSGVO.

5 Informationspflichten und Transparenzgebot

Die Datenschutzgrundverordnung normiert verschiedene Rechte betroffener Personen, die diese gegenüber dem datenschutzrechtlich Verantwortlichen geltend machen können. Sie finden sich in den Art. 15 ff. DSGVO.

---

[121] WEICHERT, NZA 2017, 565.

[122] MEINECKE, DOMINIK, Anmerkung zu EuGH (Erste Kammer) Urt. v. 30.3.2023 – C-34/21, NZA 2023, 487 (493).

[123] TAEGER in: Taeger/Gabel, Art. 6 DSGVO, Rn. 56.

[124] A.a.O. Rn. 59.

[125] SCHULZ in: Gola/Heckmann, Art. 6 DSGVO, Rn. 44.

[126] SCHULZ in: Gola/Heckmann, Art. 6 DSGVO, Rn. 44 m.w.N.

5.1 Transparenzgebot und Informationspflichten

Die DSGVO regelt vor den spezifischen Betroffenenrechten in den Art. 15 - 22 DSGVO auch noch allgemeine Pflichten des Verantwortlichen, die er insbesondere in Bezug auf die Rechte betroffener Personen einhalten muss.

5.1.1 Transparenzanforderungen, Art. 12 DSGVO

In Art. 12 DSGVO werden Transparenzanforderungen geregelt. Der Verantwortliche hat nach Art. 12 Abs. 1 DSGVO sicherzustellen, dass den Betroffenen Informationen zu den Betroffenenrechten in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden. Darüber hinaus trifft ihn auch eine aktive Unterstützungspflicht hinsichtlich der Geltendmachung von Betroffenenrechten: So ist er dazu verpflichtet, Betroffenen die Ausübung ihrer Rechte zu erleichtern, Art. 12 Abs. 2 S. 1 DSGVO. Die Vorschrift besitzt Appellcharakter.[127] Nach Erwägungsgrund 59 S. 1 zur DSGVO „sollten Modalitäten festgelegt werden, die einer betroffenen Person die Ausübung der Rechte, die ihr nach dieser Verordnung zustehen, erleichtern, darunter auch Mechanismen, die dafür sorgen, dass sie unentgeltlich insbesondere Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung beantragen und gegebenenfalls erhalten oder von ihrem Widerspruchsrecht Gebrauch machen kann“. So sollen insbesondere nach Erwägungsgrund 59 S. 2 zur DSGVO Anträge elektronisch gestellt werden können. Dies kann beispielsweise durch die Implementierung von Online-Formularen umgesetzt werden. Der Verantwortliche darf dem Betroffenen ferner den Zugang zu Informationen und die Geltendmachung von Betroffenenrechten nicht erschweren. Insbesondere dürfen keine Schranken implementiert werden, wodurch es dem Betroffenen erschwert wird, an notwendige Informationen zu kommen.

5.1.2 Informationspflichten, Art. 13 und Art. 14 DSGVO

Die DSGVO normiert Informationspflichten. In den Art. 13 und 14 DSGVO sind in Katalogen die Informationen aufgeführt, die der Verantwortliche Betroffenen im Zeitpunkt der Datenerhebung mitteilen muss.

Laut Art. 13 Abs. 1 DSGVO teilt der Verantwortliche dem Betroffenen mindestens folgende Informationen mit:

- **Name und Kontaktdaten des Verantwortlichen** sowie gegebenenfalls dessen Vertreters;

[127] HECKMANN/PASCHKE in: Ehmann/Selmayr DSGVO, Art. 12 Rn. 24.

- gegebenenfalls die Kontaktdaten des **Datenschutzbeauftragten**;
- die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung;
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland oder eine internationale Organisation zu übermitteln**, sowie die zugrundeliegende Rechtsgrundlage nach den Art. 45 ff. DSGVO

Nach Art. 13 Abs. 2 DSGVO stellt der Verantwortliche noch weitere Informationen zur Verfügung. Hierzu gehören:

- Speicherdauer
- Betroffenenrechte;
- wenn eine Einwilligung als Rechtsgrundlage herangezogen wird: das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DSGVO.

Art. 14 Abs. 1 DSGVO normiert Informationspflichten des Verantwortlichen, wenn die personenbezogenen Daten nicht bei dem Betroffenen selbst erhoben werden. Folgende Informationen sind dem Betroffenen in diesem Fall zur Verfügung zu stellen:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke und die Rechtsgrundlage der Verarbeitung;
- die Kategorien personenbezogener Daten, die verarbeitet werden;

- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- gegebenenfalls die Absicht des Verantwortlichen, eine Drittlandsübermittlung vorzunehmen und die jeweilige Rechtsgrundlage

Aus Art. 14 Abs. 2 DSGVO geht hervor, dass der Verantwortliche darüber hinaus noch weitere Informationen zur Verfügung stellen muss:

- Speicherdauer
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- Betroffenenrechte;
- Wenn eine Einwilligung als Rechtsgrundlage herangezogen wird: das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DSGVO.

Die genannten Informationen werden dem Betroffenen regelmäßig in einer Datenschutzerklärung zur Verfügung gestellt. Die grundlegenden Anforderungen an die Ausgestaltung von Datenschutzerklärungen gehen aus den oben genannten Vorschriften hervor. An die Datenschutzerklärung ist grundsätzlich der Anspruch zu stellen, dass der technisch und juristisch unbedarfte, durchschnittlich informierte Internetnutzer einen auf das Wesentliche komprimierten und inhaltlich nachvollziehbaren Überblick über Umfang und Reichweite der Datenerhebung und -verwendung auf der Webseite, Rechtsgrundlagen für die Verarbeitung und die Betroffenenrechte erhält.[128]

5.2 UI-Design-Anforderungen

Aus den Informationspflichten erwachsen Anforderungen an das Design der App, die in WearPrivate geplant ist.

[128] CONRAD/DOVAS IN: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Rn. 55.

Bei der Information betroffener Personen besteht meist ein Spannungsfeld zwischen einerseits juristischer Präzision und andererseits intuitiver Verständlichkeit für Nutzer. Die DSGVO normiert in den Art. 13 und 14 DSGVO weitreichende Informationspflichten (s.o.). Diese weitreichende Verpflichtung führt in Kombination mit der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht des Verantwortlichen dazu, dass Datenschutzerklärungen häufig sehr umfangreich und kompliziert sind. Datenschutzerklärungen enthalten regelmäßig lange und schwierige Sätze sowie juristische Fachbegriffe[129] und sind aus diesem Grund nicht nur für juristische Laien schwer verständlich[130]. Überlange, komplizierte Datenschutzerklärungen führen bei betroffenen Personen regelmäßig nicht zu dem erhofften Effekt der besseren Informiertheit, sondern vielmehr zu Überforderung und Ermüdung. So hat sich inzwischen eine Art „clicking-without-reading"-Kultur[131] eingestellt, die in mit der im Bereich der Cookie-Einwilligungen (Einwilligungen nach § 25 TDDDG bzw. Art. 5 Abs. 3 ePrivacy-Richtlinie) relevanten „Cookie-Fatigue" (Cookie-Müdigkeit)[132] verglichen werde kann. Gemeint ist mit der Cookie-Fatigue die Frustration und Überforderung, die sich bei Nutzern durch sich ständig wiederholende Aufforderungen zur Einwilligung, einstellt.[133] Diese Frustration und Überforderung führt regelmäßig dazu, dass Nutzer gedankenlos die „Alle akzeptieren"-Schaltfläche aktivieren, statt sich dezidiert mit den Folgen dieser Wahl auseinanderzusetzen und im Anschluss eine informierte Entscheidung zu treffen. Ähnlich verhält es sich auch beim „clicking-without-reading": Dieses zeichnet sich regelmäßig dadurch aus, dass Personen Einwilligungen erteilen, ohne sich vorher ausführlich mit den Konsequenzen dieser rechtserheblichen Erklärung auseinandergesetzt zu haben.[134] „Bestätigen" lässt sich dieses Phänomen beispielsweise durch die Betrachtung der durchschnittlichen Zeit, die Nutzer auf den Privacy Policy Webseiten großer Unternehmen verbringen: So verbrachten Nutzer nur knapp 47 Sekunden mit dem „Studieren" der Privacy Policy von Google UK.[135] Es ist nur schwer vorstellbar, dass in dieser kurzen Zeit ein echtes Verständnis für die teils komplizierten Regelungen aufgebaut wird.

---

[129] GERPOTT, MMR 2020, 739 (740).

[130] ARNOLD/HILLEBRAND/WALDBURGER, Personal Data and Privacy - Final Report, S. 2; Linden *et. Al.*, Proceedings on Privacy Enhancing Technologies 2020, S. 47.

[131] ARNOLD/HILLEBRAND/WALDBURGER, Personal Data and Privacy - Final Report, S. 1.

[132] RAUER/ETTIG, ZD 2021, 18 (19); SESING, MMR 2021, 544 (544); HANSEN/BRECHTEL, GRUR-Prax 2020, 385.

[133] WERKMEISTER in: Säcker/Körber, § 25 TTDSG, Rn. 25.

[134] ARNOLD/HILLEBRAND/WALDBURGER, Personal Data and Privacy - Final Report, S. 1.

[135] Competition and Markets Authority, Online platforms and digital advertising, 2019, p. 129 f.

Diesem Phänomen gilt es entgegenzuwirken. *Gerpott* nennt in seinem Aufsatz zum Thema rechtskonforme Datenschutzerklärungen eine Reihe an typischen Problemen, die das clicking-without-reading begünstigen.[136] Hierzu gehören[137]:

- großer Textumfang und daraus resultierender Zeitaufwand für die Lektüre;
- niedrige Textverständlichkeit;
- fehlende Erkennbarkeit praktischer Folgen der Datenverarbeitung für die eigene Person;
- hoher Zustimmungsdruck zur Öffnung von Interaktionsmöglichkeiten mit dem Anbieter;
- hohes Vertrauen in Datenschutz-Fairness des Anbieters oder das Schutzniveau durch staatliche Regulierung;
- geringe Wahrscheinlichkeit und Nachvollziehbarkeit von Sanktionen gegenüber Anbietern bei DS-GVO-Verletzungen;
- starke Unterbrechung des eigentlich gewünschten Ablaufs beim Bewegen auf Anbieterseiten (flow interruption);
- geringe Lesbarkeit auf kleinen Bildschirmen mobiler Endgeräte.

Diesen Punkten kann mit einigen Gegenmaßnahmen begegnet werden.

5.2.1 Umfang

Die Datenschutzerklärung sollte, wie sich an den obigen Ausführungen zeigt, nicht zu umfangreich sein, um die Zeitdauer, diese zu lesen und zu verstehen, zu reduzieren. Allerdings steht diese Anforderung in gewisser Weise im Widerspruch zu den Art. 13 und 14 DSGVO. Die Informationspflichten der DSGVO sind sehr umfangreich; es sind eine Reihe an Informationen zur Verfügung zu stellen, um die Verpflichtungen der DSGVO einzuhalten. Da der Verantwortliche auch nachweisen können muss, dass er die Verpflichtungen der DSGVO eingehalten hat, ist es aus Gründen der Rechtssicherheit auch sinnvoll alle Informationen explizit zu nennen und auszuführen. Gänzlich verkürzt kann eine Datenschutzerklärung mithin nicht dargestellt werden. Allerdings ist es als sinnvoll anzusehen, einfache kurze Sätze zu verwenden und Sachverhalte möglichst kurz und knapp darzustellen.

5.2.2 Komplexität

Vermieden werden sollten neben der Überlänge von Datenschutzerklärungen auch komplizierte Fachbegriffe. Juristische Fachsprache ist, soweit es nicht zwingend erforderlich ist, um die Präzision

---

[136] GERPOTT, MMR 2020, 739 (741).

[137] EBD.

einer Aussage beizubehalten, möglichst zu vermeiden und durch Alltagssprache zu ersetzen. Diese Anforderung könnte allerdings wiederum dazu führen, dass Datenschutzerklärungen an Umfang gewinnen, soweit einzelne Begriffe durch längere Erklärungen ersetzt werden müssen. An dieser Stelle ist abzuwägen, welchem Bedürfnis der betroffenen Personen abgeholfen werden soll. Generell sollte darauf geachtet werden, dass auch wenn zu Alltagssprache gegriffen wird, diese Erklärung den Text nicht unnötig verlängert.

Darüber hinaus ist auch darauf zu achten, dass aus den sprachlichen Veränderungen keine juristischen Ungenauigkeiten oder sonstiger Informationsverlust resultieren: So sollten keine Worte verwendet werden, die zwar in der Alltagssprache eine ähnliche bis synonyme Bedeutung haben, im juristischen Kontext allerdings einen anderen Sinngehalt besitzen (bspw. Abgrenzung der Begriffe „Einwilligung“ und „Genehmigung“ im juristischen Kontext). Ferner erfordern manche Vorgaben der DSGVO auch juristisch korrekte Angaben, die nicht unerwähnt bleiben dürfen (wie beispielsweise die genaue Angabe der Rechtsgrundlage). Trotzdem ist es möglich, andere Punkte in weniger komplizierter Sprache zu umschreiben.

Insbesondere die konkrete Ausformulierung von bestimmten Konsequenzen und Gefahren für betroffene Personen können für ein besseres Verständnis und mehr Sichtbarkeit konkreter Folgen von Datenverarbeitungen folgen.

5.2.3 Visualisierung/Veranschaulichung

Eine weitere sinnvolle Maßnahme ist die Nutzung von Bildern und Symbolen, um die Datenverarbeitungen bildhaft darzustellen. Hierfür könnten beispielsweise Privacy Icons[138] verwendet werden. Hierdurch können auch die Konsequenzen von bestimmten Einstellungen verständlich dargestellt werden. Die Visualisierung wie auch die Nutzung von Alltagssprache können dazu beitragen, dass die praktischen Konsequenzen für die betroffenen Personen greifbarer erscheinen.

5.2.4 Selbstbestimmungseinstellungen

Für betroffene Personen ist auch der hohe Zustimmungsdruck zur Öffnung von Interaktionsmöglichkeiten mit dem Anbieter ein Problem. Daraus lässt sich schlussfolgern, dass es betroffenen Personen regelmäßig so erscheint, als blieben ihnen keine wirklichen Auswahlmöglichkeiten, da zur Interaktion mit dem gewünschten Dienst die Annahme der Datenschutzerklärung erforderlich ist.

---

[138] Wie sie beispielsweise der Bitkom e.V. vorgestellt hat: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Privacy-Icons, letzter Abruf am 27.06.2023.

Das Gefühl, eine Wahlmöglichkeit zu besitzen, könnte für die betroffenen Personen entstehen, wenn verschiedene Selbstbestimmungsmechanismen implementiert werden und bei einigen Punkten somit eine Auswahlmöglichkeit bleibt. Sinnvoll wäre es beispielsweise, wenn betroffene Personen bei einigen Punkten wählen können, welche Sicherheitsstufe sie bevorzugen. Hinsichtlich der Selbstbestimmungsmechanismen sind in WearPrivate unterschiedliche Ansätze geplant; unter anderem sollen Betroffene selbst einstellen können, wie stark ihre Rohdaten vorm Weitertransport an den Analysedienst verrauscht werden sollen. Solche Wahlmöglichkeiten können die Datenschutzerklärung für betroffene Personen verständlicher und intuitiver machen.

5.2.5 Zugang zur Datenschutzerklärung

Da auch die Erreichbarkeit der Datenschutzerklärung für betroffene Personen ein Problem zu sein scheint, ist es auch sinnvoll und erforderlich, dass die Datenschutzerklärung für betroffene Personen unproblematisch erreichbar ist. Der Verantwortliche darf, wie sich auch aus Art. 12 DSGVO ergibt, keine Hindernisse und Barrieren aufbauen, durch die die Zugänglichkeit zu den erforderlichen Informationen für betroffene Personen erschwert wird. Vielmehr muss er aktiv dabei unterstützen, dass Betroffene alle Informationen erhalten.

Dazu gehört auch, dass keine den Lesefluss beeinträchtigenden Maßnahmen ergriffen werden sollten. Ebenso ist es sinnvoll, dass die Datenschutzerklärung an einem Ort auffindbar ist und keine weiteren Webseiten besucht werden müssen, um alle Informationen zu erhalten. Ebenso ist es gerade für eine Smartphone-App erforderlich, dass eine Version der Datenschutzerklärung vorliegt, die auf einem mobilen Endgerät gut lesbar ist.

5.2.6 Zertifikate

Auch die Nutzung von Zertifikaten[139] im Sinne von Art. 42 DSGVO könnten zumindest das Vertrauen in die Korrektheit der Datenschutzerklärung stützen.[140]

5.2.7 Fazit

Es gibt einige Maßnahmen, die ergriffen werden können, um Datenschutzerklärungen intuitiver und verständlicher zu machen. Eine Kombination dieser Maßnahmen kann schlussendlich zu einer rechtskonformen und für Betroffene angenehm verständlichen Datenschutzerklärung führen.

---

[139] Wie beispielsweise: https://www.tuvit.de/de/leistungen/datenschutz/datenschutz-zertifizierung/trusted-site-privacy/ oder https://www.euprivacyseal.com/de/.

[140] GERPOTT, MMR 2020, 739 (743 f.).

6 Betroffenenrechte

6.1 Recht auf Auskunft, Art. 15 DSGVO

Gemäß Art. 15 DSGVO steht einer betroffenen Person ein Recht auf Auskunft zu. Demnach kann die betroffene Person einen Antrag stellen und eine Auskunft des Verantwortlichen über die Verarbeitung ihrer personenbezogenen Daten verlangen.[141] Es handelt sich um eine wichtige Ergänzung zu den proaktiven Informationspflichten aus Art. 13 und Art. 14 DSGVO.[142] Für die Geltendmachung eines Auskunftsanspruchs gemäß Art. 15 DSGVO bedarf es eines Antrags der die Auskunft begehrenden Person. Dieser sollte möglichst präzise dahingehend sein, über welche Informationen und Verarbeitungsvorgänge Auskunft verlangt wird.[143] Hierbei ist jedoch weder die Einhaltung einer Form noch eine Begründung notwendig.[144] Der Anspruch auf Auskunft ist **voraussetzungslos** gewährleistet.[145] Daher ist die tatsächliche Betroffenheit der Person **nicht** Voraussetzung für den Anspruch auf Auskunft gemäß Art. 15 DSGVO.

Neben dem Recht auf Auskunft steht noch ein Recht auf Kopie gemäß Art. 15 Abs. 3 DSGVO zur Verfügung. Aus Art. 15 Abs. 3 S. 1 und 2 DSGVO geht hervor, dass die erste Kopie ohne Zahlung zur Verfügung gestellt werden muss; für weitere Kopien kann eine Zahlung zur Deckung der Verwaltungskosten verlangt werden.[146]

6.2 Recht auf Berichtigung, Art. 16 DSGVO

Gemäß Art. 16 S. 1 DSGVO kann eine betroffene Person verlangen, dass unrichtige personenbezogene Daten über sie berichtigt werden. Zudem kann sie gemäß Satz 2 des Art. 16 DSGVO auch die Vervollständigung der sie betreffenden personenbezogenen Daten verlangen. Das Recht auf Berichtigung und Vervollständigung zählt zum sogenannten „Selbstdatenschutz“.[147] Art. 16 DSGVO verfolgt indes verschiedene Ziele: Hierzu gehört einerseits die objektive Richtigkeit der

---

141 BÄCKER in: Kühling/Buchner, DSGVO Art. 15 Rn. 1.

142 BÄCKER in: Kühling/Buchner, DSGVO Art. 15 Rn. 1; MESTER in: Taeger/Gabel, DSGVO Art. 15 Rn. 1.

143 KAMLAH in: Plath DSGVO/BDSG, DSGVO Art. 15 Rn. 4.

144 FRANCK in: Gola DSGVO, Art. 15 Rn. 25.

145 BÄCKER in: Kühling/Buchner, DSGVO Art. 15 Rn. 6; MESTER in: Taeger/Gabel, DSGVO Art. 15 Rn. 2; FRANCK in: Gola DSGVO Art. 15 Rn. 5.

146 NINK in: Spindler/Schuster, DSGVO Art. 15 Rn. 11.

147 REIF in: Gola DSGVO, Art. 16 Rn. 1.

personenbezogenen Daten, andererseits auch die „Dateninhaltswahrheit und -klarheit“. [148] Art. 16 DSGVO dient mithin der Umsetzung der Schutzprinzipien der DSGVO (Art. 5 Abs. 1 DSGVO).[149] Art. 5 Abs. 1 lit. d der DSGVO verlangt schließlich die sachliche Richtigkeit der personenbezogenen Daten, die verarbeitet werden.

Unrichtigkeit liegt vor, wenn die Daten von der Realität abweichen.[150] Nicht von Bedeutung ist indes die Wesentlichkeit der Daten oder die Gründe für die Unrichtigkeit.[151] Es gibt keine Bagatellgrenze bei Art. 16 DSGVO.[152] Zudem ist auch kein Verschulden des Verantwortlichen erforderlich.[153]

Der Anspruch auf Vervollständigung ist lex specialis gegenüber dem Berichtigungsanspruch.[154] Wichtig ist, dass es hierbei *nicht* um falsche Daten geht; vielmehr steht die Ergänzung von richtigen Daten hier im Mittelpunkt.[155] Unvollständigkeit liegt also vor, wenn grundsätzlich richtige Daten vorliegen, diese aber in der Gesamtschau einen falschen Eindruck erwecken oder aufgrund ihrer Lückenhaftigkeit missverständlich sind.[156]

In beiden Fällen folgt ein unionsrechtlicher und unmittelbar geltender Anspruch gegen den Verantwortlichen.[157]

6.3 Recht auf Löschung, Art. 17 DSGVO

Art. 17 DSGVO regelt das sogenannte „Recht auf Vergessenwerden“. Dieses Recht erlangte größere Bekanntheit durch die Entscheidungen des Europäischen Gerichtshofes hinsichtlich des Rechts auf

---

[148] KAMANN/BRAUN in: Ehmann/Selmayr DSGVO, Art. 16 Rn. 3.

[149] EuGH, ZD 2014, 350 (356 Rn. 67).

[150] WORMS in: BeckOk DatenschutzR, DSGVO Art. 16 Rn. 49; REIF in: Gola DSGVO, Art. 16 Rn. 11; PEUKER in: Sydow/Marsch, Art. 16 DSGVO Rn. 7; BVerwG, NVwZ 2004, 626 (627); DIX in: Simitis/Hornung/Spiecker, DSGVO Art. 16 Rn. 11; HERBST in: Kühling/Buchner, DSGVO Art. 16 Rn. 8.

[151] DIX in: Simitis/Hornung/Spiecker, DSGVO Art. 16 Rn. 11; HERBST in: Kühling/Buchner, DSGVO Art. 16 Rn. 11; PEUKER in: Sydow/Marsch, Art. 16 DSGVO Rn. 8; WORMS in: BeckOk DatenschutzR, DSGVO Art. 16 Rn. 52;

[152] DIX in: Simitis/Hornung/Spiecker, DSGVO Art. 16 Rn. 11.

[153] MEENTS/HINZPETER in: Taeger/Gabel DSGVO, Art. 16 Rn. 8; HERBST in: Kühling/Buchner, DSGVO Art. 16 Rn. 14.

[154] KEPER/KEPPELER in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO Art. 16 Rn. 14; HERBST in: Kühling/Buchner, DSGVO Art. 16 Rn. 4.

[155] HERBST in: Kühling/Buchner, DSGVO Art. 16 Rn. 18; KREMER in Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 4 Rn. 45.

[156] KREMER in Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 4 Rn. 45; KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 16 Rn. 36; BVerwGE 120, 188 Rn.11.

[157] KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 16 Rn. 30, 40.

Löschung gegenüber dem Suchmaschinenbetreiber Google.[158] Art. 17 DSGVO stellt ein ergänzendes Recht für betroffene Personen dar, da aus Art. 5 Abs. 1 lit. c–e DSGVO bereits die proaktive Verpflichtung folgt, unrichtige und nicht mehr erforderliche Daten zu löschen.[159]

Begrifflich müssen das Recht auf Löschung und das Recht auf Vergessenwerden voneinander abgegrenzt werden. Das Recht auf Vergessenwerden beinhaltet das Recht auf Löschung und geht über dieses noch hinaus.[160] Das Recht auf Löschung ist ein klassisches Löschrecht, während das Recht auf Vergessenwerden das Recht aus Art. 17 Abs. 2 DSGVO beschreibt.[161] Das Recht auf Vergessenwerden im engeren Sinne stellt also eine Informationspflicht des Verantwortlichen dar.[162]

Der Verantwortliche kann demnach auch ohne Antrag auf Löschung verpflichtet sein.[163] Die Verpflichtung des Verantwortlichen zur unverzüglichen Löschung der personenbezogenen Daten ist gemäß Art. 17 Abs. 1 DSGVO bereits dann anzunehmen, wenn einer der Löschungsgründe gemäß der Buchstaben a bis f vorliegt. Der Verantwortliche muss stets prüfen, ob die Kontaktaufnahme zu der betroffenen Person erforderlich ist – dies zumindest in den Fällen, in denen diese ein Wahlrecht hat oder andere schutzwürdige Interessen gegen eine Löschung sprechen könnten.[164] Folgende Gründe führen zu einer Löschungsverpflichtung:

- lit. a: Fortfall des Verarbeitungszwecks
- lit. b: Widerruf einer erteilten Einwilligung
- lit. c: Widerspruch gegen die Verarbeitung
- lit. d: Unrechtmäßige Verarbeitung der personenbezogenen Daten
- lit. e: Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich
- lit. f: Daten von Kindern wurden erhoben gemäß Art. 8 DSGVO

---

158 EuGH, NJW 2014, 2257.

159 DIX in: Simitis/Hornung/Spiecker, DSGVO Art. 17 Rn. 1.

160 KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 17 Rn. 2.

161 KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 17 Rn. 3.

162 KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 17 Rn. 41.

163 LEUTHEUSSER-SCHNARRENBERGER/KEPPELER in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO Art. 17 Rn. 16.

164 DIX in: Simitis/Hornung/Spiecker, DSGVO Art. 17 Rn. 6; PAAL in: Paal/Pauly DSGVO, Art. 17 Rn. 20; HERBST in: Kühling/Buchner, DSGVO Art. 17 Rn. 8 ff.

Ist einer dieser Gründe einschlägig, folgt die Verpflichtung zur unverzüglichen Löschung, also zur physischen Vernichtung beziehungsweise Unbrauchbarmachung der Daten.[165] Es muss nach dem Löschungsvorgang unmöglich sein, die zuvor verarbeiteten Informationen wahrzunehmen.[166] „Unverzüglich" bedeutet in diesem Zusammenhang ohne schuldhafte Verzögerung – die Löschung darf nicht weiter als notwendig herausgezögert werden.[167] Konkret wird in diesem Zusammenhang vorgeschlagen, im Einklang mit Art. 12 Abs. 3 S. 1 DSGVO eine einmonatige Frist als die äußerste Grenze anzusehen.[168]

Bei Vorliegen der Voraussetzungen des Art. 17 Abs. 1 DSGVO folgt für den Verantwortlichen neben der Pflicht auf unverzügliche Löschung auch eine Informationspflicht gemäß Art. 17 Abs. 2 DSGVO. Hat der Verantwortliche die betroffenen Daten öffentlich gemacht, so ist er, nachdem ihn ein Löschungsbegehren erreicht hat, dazu verpflichtet, dies auch anderen Verantwortlichen mitzuteilen, die die veröffentlichten Daten verarbeiten.

Aus Art. 17 Abs. 3 DSGVO ergibt sich derweil, wann kein Anspruch auf Löschung besteht.

6.4 Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO

Art. 18 DSGVO gewährt dem Betroffenen ein Recht auf Einschränkung der Verarbeitung, soweit einer der in den Buchstaben a bis d geregelten Katalogtatbestände gegeben ist. Aus dem Wortlaut der Buchstaben a bis d geht hervor, dass jeweils ein bestimmtes Verhalten der betroffenen Person erforderlich ist. So muss sie gemäß Buchstabe a beispielsweise die Richtigkeit der Daten bestreiten oder nach Buchstabe b die Einschränkung statt der Löschung bei unrechtmäßiger Datenverarbeitung verlangen.

Der zweite Absatz von Art. 18 DSGVO schreibt indes vor, wie die eingeschränkte Verarbeitung abläuft. Die Verarbeitung der personenbezogenen Daten ist demgemäß nur noch mit der **Einwilligung** der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** oder zum **Schutz der Rechte anderer natürlicher oder juristischer Personen** oder aus Gründen **öffentlichen Interesses** der Union oder eines Mitgliedstaates möglich.

---

165 PAAL in: Paal/Pauly DSGVO, Art. 17 Rn. 30; EuGH, NJW 2018, 767 (769 Rn. 55).

166 HERBST in: Kühling/Buchner, DSGVO Art. 17 Rn. 37.

167 HERBST in: Kühling/Buchner, DSGVO Art. 17 Rn. 37.

168 PAAL in: Paal/Pauly DSGVO, Art. 17 Rn. 31; DIX in: Simitis/Hornung/Spiecker, DSGVO Art. 17 Rn. 8; HERBST in: Kühling/Buchner, DSGVO Art. 17 Rn. 46; KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 16 Rn. 33.

Hat der Verantwortliche auf Antrag des Betroffenen eine Einschränkung der Verarbeitung vorgenommen, so trifft ihn eine Unterrichtungspflicht gemäß Abs. 3, sobald die Einschränkung wieder aufgehoben wird.[169]

6.5 Mitteilungspflicht, Art. 19 DSGVOf

Art. 19 der DSGVO enthält kein direktes Betroffenenrecht, sondern eher eine ergänzende Vorschrift zu den anderen Betroffenenrechten.[170] Er verdient jedoch trotzdem eine Erwähnung, da hier Mitteilungspflichten des Verantwortlichen im Zusammenhang mit den anderen Betroffenenrechten gemäß der Art. 16, 17 und 18 DSGVO. Es handelt sich um eine Folgemitteilungspflicht gegenüber den Empfängern der betroffenen personenbezogenen Daten.[171]

6.6 Recht auf Datenübertragbarkeit, Art. 20 DSGVO

Art. 20 DSGVO stützt das Recht auf informationelle Selbstbestimmung, indem dem Betroffenen das Recht auf Datenübertragbarkeit gewährt wird.[172] Der Betroffene kann verlangen, dass ihm die bereitgestellten Daten vom Verantwortlichen in einem anpassbaren Format übermittelt werden oder dass der Verantwortliche die Daten direkt an einen Dritten weiterübermittelt.[173] Voraussetzung für den Anspruch ist, dass die Verarbeitung entweder auf einer Einwilligung des Betroffenen oder auf einem Vertrag beruht **und** die Verarbeitung automatisiert durchgeführt werden soll. Das Recht auf Datenübertragbarkeit dient binnenmarkt- und wettbewerbspolitischen Zielen.[174] Insbesondere soll der Wechsel von einem Diensteanbieter im Internet, wie etwa einem sozialen Netzwerk oder einem E-Mail-Provider, zum anderen ermöglicht werden, indem Daten aus einem Profil übertragen werden können.[175] Dies dient auch und insbesondere der Erhaltung des Wettbewerbs zwischen verschiedenen Anbietern.[176]

---

[169] KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 18 Rn. 36.

[170] KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 19 Rn. 2.

[171] KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 19 Rn. 2.

[172] SPINDLER/DALBY in: Spindler/Schuster, DSGVO Art. 20 Rn. 1.

[173] MUNZ in Taeger/Gabel, DSGVO Art. 20 Rn. 1.

[174] KAMANN/BRAUN in Ehmann/Selmayr DSGVO, Art. 20 Rn. 3.

[175] HERBST in: Kühling/Buchner, DSGVO Art. 20 Rn. 2; SCHANTZ, NJW 2016, 1841 (1845).

[176] SCHANTZ, NJW 2016, 1841 (1845).

6.7 Widerspruchsrecht, Art. 21 DSGVO

Art. 21 DSGVO enthält das Widerspruchsrecht betroffener Personen. Geregelt wird das Recht der Betroffenen, **jederzeit** Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen. Gemäß Absatz 1 Satz 2 muss der Verantwortliche die Verarbeitung der personenbezogenen Daten daraufhin einstellen, es sei denn, er kann gegenläufige schutzwürdige Interessen nachweisen. Das Widerspruchsrecht besteht gegen die rechtmäßige Ausübung der Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. e (öffentliches Interesse) oder lit. f (berechtigtes Interesse) DSGVO.[177] Erfolgt die Datenverarbeitung hingegen unrechtmäßig, so liegt gemäß Art. 17 DSGVO (s.o.) eine unmittelbare Löschungsverpflichtung vor und es bedarf keines Widerspruchs der betroffenen Person.[178]

Art. 21 DSGVO beinhaltet neben dem allgemeinen Widerspruchsrecht für Verarbeitungen, die auf Grundlage von Art. 6 DSGVO ergehen, noch weitere, spezielle Widerspruchsrechte. Absatz 2 bezieht sich auf Datenverarbeitungen zum Zwecke der Direktwerbung. Die Verarbeitung zur Direktwerbung kann mittels der Einlegung eines Widerspruchs beendet werden, ohne dass weitere Voraussetzungen erfüllt sein müssen.[179] Anders ist dies im Falle des Widerspruchs gegen die Verarbeitung aus Forschungs- oder Statistikzwecken. In diesem Fall muss die Verarbeitung nicht eingestellt werden, soweit die Verarbeitung einer im öffentlichen Interesse liegenden Aufgabe dient (Absatz 6).

Sowohl im Falle des Widerspruchs nach Absatz 1 als auch nach Absatz 6 müssen Gründe vorliegen, die sich aus der „besonderen persönlichen Situation“ ergeben. Hierbei reicht es nicht aus, sich auf die Unrechtmäßigkeit der Verarbeitung zu berufen, hiergegen kann man sich nur mit der Geltendmachung von Betroffenenrechten wehren.[180]

Dies folgt daraus, dass die Verarbeitung gemäß Art. 6 Abs. 1 lit. f DSGVO bereits auf einer Interessenabwägung beruht, die zugunsten des Verantwortlichen ausgefallen ist.[181] Daher muss im Einzelfall aufgrund einer Analyse der Situation entschieden werden, ob besondere persönliche Gründe anzunehmen sind.[182]

---

[177] SCHULZ in: Gola DSGVO, Art. 21 Rn. 1.

[178] SCHULZ in: Gola DSGVO, Art. 21 Rn. 1.

[179] SCHULZ in: Gola DSGVO, Art. 21 Rn. 1.

[180] HERBST in: Kühling/Buchner, DSGVO Art. 21 Rn. 5.

[181] SCHULZ in: Gola DSGVO, Art. 21 Rn. 9.

[182] SCHULZ in: Gola DSGVO, Art. 21 Rn. 9.

Der Widerspruch kann vor oder auch während der Verarbeitung der personenbezogenen Daten eingelegt werden.[183]

6.8 Automatisierte Entscheidungen im Einzelfall, insbesondere Profiling, Art. 22 DSGVO

Art. 22 DSGVO enthält eine Vorschrift zum Schutz von Individuen vor vollständig automatisierten Entscheidungen. Demnach muss sich kein Mensch einer Entscheidung unterwerfen, die nur durch eine Maschine getroffen wurde, **ohne** dass diese von einem Menschen nachgeprüft wurde.[184] Es geht hier mithin um die Automatisierung von Lebenssachverhalten.[185] Dies kann zu Bedenken hinsichtlich der Verletzung der Menschenwürde führen, da es hier zu verhindern gilt, den Menschen zu einem „bloßen Objekt zu degradieren".[186]

Art. 22 DSGVO stellt ein Verbot dar, welches unabhängig von einer individuellen Geltendmachung ist.[187] Weitgehende Ausnahmen von diesem Verbot finden sich in Art. 22 Abs. 2 DSGVO.

Wichtig ist, dass der Anwendungsbereich von Art. 22 DSGVO nur dann eröffnet ist, wenn eine **vollständig automatisierte Entscheidung** vorliegt, die **Rechtswirkung** hat oder sie in ähnlicher Weise erheblich beeinträchtigend ist. Es bedarf mithin eines „gestaltenden Aktes mit Außenwirkung, bei dem mindestens zwei Alternativen vorliegen"[188]. Zudem muss die Entscheidung ausschließlich maschinell erfolgen, also ohne Zutun eines Menschen – dies ist dann nicht der Fall, wenn die maschinelle Verarbeitung eher als Vorbereitung einer menschlichen Entscheidung dient.[189] Rechtswirkung ist dann anzunehmen, wenn durch die Entscheidung der rechtliche Status einer Person verändert wird.[190] Mittelbar rechtliche Auswirkungen genügen indes nicht.[191] Eine „in ähnlicher Weise erhebliche

---

[183] HERBST in: Kühling/Buchner, DSGVO Art. 21 Rn. 16.

[184] VON LEWINSKI in: BeckOK DatenschutzR, DSGVO Art. 22 Rn. 2.

[185] ATZERT in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO Art. 22 Rn. 4.

[186] ATZERT in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO Art. 22 Rn. 4; MARTINI in: Paal/Pauly DSGVO, Art. 22 Rn. 1.

[187] MARTINI in: Paal/Pauly DSGVO, Art. 22 Rn. 29b; ATZERT in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO Art. 22 Rn. 2; BUCHNER in: Kühling/Buchner, DSGVO Art. 22 Rn. 12.

[188] MARTINI in: Paal/Pauly DSGVO, Art. 22 Rn. 15a.

[189] HLADJK in: Ehmann/Selmayr DSGVO, Art. 22 Rn. 6.

[190] MARTINI in: Paal/Pauly DSGVO, Art. 22 Rn. 26.

[191] VON LEWINSKI in: BeckOK DatenschutzR, DSGVO Art. 22 Rn. 28.

Beeinträchtigung“ liegt vor, wenn die Wirkung einer Entscheidung einer Rechtswirkung gleichkommt.[192]

6.9 Rechtliche Besonderheiten im IoT-Bereich

Die Geltendmachung von Betroffenenrechten stellt sich für viele Personen als schwieriges Unterfangen dar. So fällt es den Personen häufig schwer, ihr Anliegen zu formulieren und den richtigen Ansprechpartner zu finden. Im Bereich des IoT stellen sich noch weitere Probleme und Herausforderungen für betroffene Personen.

Betroffenenrechte sind beim Verantwortlichen geltend zu machen. Gemäß Art. 26 Abs. 3 DSGVO ist die Geltendmachung von Betroffenenrechten bei allen Verantwortlichen möglich.

Im Szenario des Projekts WearPrivate ist regelmäßig eine gemeinsame Verantwortlichkeit von Arbeitgeber und Analysedienstleister anzunehmen (s.u.): Es handelt sich also bei beiden Akteuren um Ansprechpartner für betroffene Personen, soweit diese ihre Betroffenenrechte geltend machen möchten. Beiden stehen indes unterschiedliche Möglichkeiten zur Verfügung, um den Bedürfnissen der Betroffenen nachzukommen. Gegebenenfalls kann daher ein Zusammenwirken beider Parteien (u.U. auch noch mit dem App-Entwickler sowie dem Cloudanbieter) erforderlich sein. Den Verantwortlichen obliegt die Pflicht, die Betroffenen bei der Geltendmachung ihrer Rechte aktiv zu unterstützen, Art. 12 Abs. 2 S. 1 DSGVO.[193] Die Pflicht bezieht sich insbesondere auf die Mitteilung der Informationen, die notwendig sind, um die Betroffenenrechte auszuüben.[194] Hierzu gehört sowohl die genaue Definition der Zuständigkeiten (insbesondere der zuständigen Stelle des Verantwortlichen) als auch die Einräumung des Zugangs zu den erforderlichen Informationen.[195] Besonders hilfreich sind Kontaktformulare. Ferner sind auch intern Maßnahmen zu ergreifen: Die konsistente Aufgaben- und Zuständigkeitsaufteilung ist hilfreich und erforderlich.[196]

Im IoT-Bereich liegt die Besonderheit darin, dass Informationen zur Geltendmachung von Betroffenenrechten und auch mögliche Kontaktformulare regelmäßig nicht auf dem Gerät selbst implementiert werden können. Diese Informationen finden sich in der Regel in der App auf dem

---

[192] MARTINI in: Paal/Pauly DSGVO, Art. 22 Rn. 27.

[193] QUAAS in: BeckOK DatenschutzR, Art. 12 DSGVO Rn. 32.

[194] S. Fn. 142.

[195] PAAL/HENNEMANN in: Paal/Pauly Art. 12 DS-GVO Rn. 44.

[196] FRANCK in: Gola/Heckmann, Art. 12 DSGVO Rn. 13.

Smartphone, über die das Gerät gesteuert wird. Dies wird auch im Rahmen von WearPrivate der Fall sein. Darüber hinaus besteht auch die Besonderheit, dass die datenschutzrechtliche Verantwortlichkeit in WearPrivate weder beim Hersteller des Wearables noch beim Programmierer der App liegt. Vielmehr sind der Analysedienst sowie der Arbeitgeber verantwortlich. Diese Aufteilung der datenschutzrechtlichen Verantwortlichkeit ist transparent offenzulegen.

Um den Arbeitnehmern im Kontext von WearPrivate die Geltendmachung von Betroffenenrechten zu erleichtern, ist die Implementierung eines Formulars zum Ausfüllen in der zugehörigen App sinnvoll. Die App ist aufgrund der Tatsache, dass dort auch die relevante Datenschutzerklärung verankert ist, intuitiv der erste Ort, an dem nach Hilfe für die Geltendmachung von Betroffenenrechten gesucht wird. Festgehalten werden sollte allerdings, dass die Übermittlung von Betroffenenanfragen auch tatsächlich stattfindet. Ist der App-Betreiber als Auftragsverarbeiter einzuordnen (siehe hierzu unter Kapitel 7) trifft sie nach Art. 28 Abs. 3 lit. e DSGVO auch die Pflicht, geeignete technische und organisatorische Maßnahmen zu ergreifen, um Verantwortliche bei der Pflicht zur Beantwortung von Anfragen der Betroffenen zu unterstützen. Hierzu könnte auch die automatische Weiterleitung von Betroffenenanfragen gehören.

Ist der App-Betreiber nicht als Auftragsverarbeiter einzuordnen, müsste auf andere Weise geregelt werden, dass Betroffenenanfragen weitergegeben werden.

6.9.1 Sozialer Druck

Liegt eine gemeinsame Verantwortlichkeit vor, steht es betroffenen Personen grundsätzlich frei zu entscheiden, bei welchem der Verantwortlichen sie ihre Betroffenenrechte geltend machen möchten, Art. 26 Abs. 3 DSGVO. So wäre im Kontext von WearPrivate die Geltendmachung sowohl beim Analyseservice als auch beim Arbeitgeber denkbar. Allerdings stellen sich auch hier wieder Herausforderungen hinsichtlich des bereits mehrfach angesprochenen sozialen Drucks. Zwar erscheint die Geltendmachung beim Arbeitgeber auf den ersten Blick niedrigschwelliger und einfacher möglich als beim Analyseservice. So könnte sich für die Arbeitnehmer die Möglichkeit ergeben, den Arbeitgeber direkt anzusprechen.

Allerdings besteht zwischen Arbeitnehmer und Arbeitgeber wie bereits erläutert ein Abhängigkeitsverhältnis sowie ein Machtungleichgewicht, welches Auswirkungen auf die Geltendmachung von Betroffenenrechten haben könnte. So ist es zumindest vorstellbar, dass die Arbeitnehmer sich nicht trauen, gegenüber ihrem Arbeitgeber Ansprüche zu stellen und beispielsweise Auskunft über die verarbeiteten Daten zu verlangen oder einer Datenverarbeitung nach Art. 21 DSGVO aktiv zu widersprechen. Dabei ist zwischen den verschiedenen Betroffenenrechten zu unterscheiden.

Das Auskunftsrecht nach Art. 15 DSGVO und das Recht auf Berichtigung nach Art. 16 DSGVO weisen im Gegensatz zu dem Recht auf Löschung sowie dem Recht auf Widerspruch nach Art. 21 DSGVO wenig Diskussionspotential. Müsste der Arbeitnehmer beispielsweise darlegen, dass er eine Verarbeitung für unrechtmäßig hält, könnte die Überlegenheit des Arbeitgebers den Arbeitnehmer in der Geltendmachung seiner Rechte hemmen. Daher ist es denkbar, dass eher der Analyseservice als Ansprechpartner in Anspruch genommen wird. Dies ist vor dem Hintergrund, dass der Analyseservice auch über alle relevanten Informationen verfügt und der Arbeitgeber keine darüberhinausgehenden Daten kennt, praktisch sinnvoll. Ferner verfügt der Analyseservice über die Möglichkeit, die Betroffenenrechte schnell und unkompliziert umzusetzen. So ist das Löschen oder Korrigieren von Daten für den Analyseservice einfacher umzusetzen als für den Arbeitgeber, der den Analyseservice bei einem entsprechenden Anliegen erst kontaktieren müsste, um auch beispielsweise Historie und Rohdaten zu löschen. Allerdings kann nicht verhindert werden, dass bei beispielsweise einem Löschungsbegehren auch der Arbeitgeber informiert werden muss.

7 Datenschutzrechtliche Verantwortlichkeit

Verantwortlicher ist, wer über Zweck und Mittel der Datenverarbeitung entscheidet. Dies ergibt sich aus Art. 4 Nr. 7 DSGVO. Der Verantwortliche ist strikt vom sogenannten Auftragsverarbeiter zu unterscheiden, der gemäß Art. 4 Nr. 8 DSGVO auf Weisung und im Auftrag des Verantwortlichen tätig wird.

7.1 Pflichten des Verantwortlichen

Es ist wichtig, grundlegend zu klären, wer die datenschutzrechtliche Verantwortlichkeit trägt. Der Verantwortliche ist nicht nur zuständig dafür, die Informationspflichten im Sinne der Art. 13 und 14 DSGVO zu erfüllen, er ist auch Ansprechpartner für die Ausübung von Betroffenenrechten. Zusätzlich existiert gemäß Art. 5 Abs. 2 DSGVO die Rechenschaftspflicht, wonach der Verantwortliche die Einhaltung der Grundsätze der Datenverarbeitung nachweisen muss (s.o.). Zudem treffen ihn auch andere Haftungsrisiken als den Auftragsverarbeiter. Im Folgenden werden die Pflichten des Verantwortlichen aufgeführt.

7.1.1 Datenschutzerklärung

Der Verantwortliche muss gem. Art. 12 Abs. 1 S. 1 Hs. 1 DSGVO geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen gemäß den Art. 13 und 14 DSGVO und alle Mitteilungen gem. Art. 15-22 DSGVO und Art. 34 DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache

übermitteln. Die Übermittlung der Informationen kann dabei schriftlich oder ggfs. in elektronischer Form erfolgen.

7.1.2 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art. 12 DSGVO

Der Verantwortliche ist dazu verpflichtet, die Betroffenenrechte der Art. 15 ff. DSGVO umzusetzen. Die Informationen aus Art. 13 und Art. 14 DSGVO sowie alle Mitteilungen und Maßnahmen gem. den Art. 15 bis 22 und Art. 34 DSGVO sind der betroffenen Person unentgeltlich zur Verfügung zu stellen, Art. 12 Abs. 5 S. 1 DSGVO.

Bei offenkundig unbegründeten exzessiven Anträgen einer betroffenen Person oder im Falle einer häufigen Wiederholung kann der Verantwortliche ein angemessenes Entgelt verlangen oder sich weigern, aufgrund eines Antrags tätig zu werden, Art. 12 Abs. 5 S. 2 lit. a und b DSGVO. Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen, Art. 12 Abs. 5 S. 3 DSGVO.

Der Verantwortliche muss gem. Art. 12 Abs. 2 DSGVO der betroffenen Person die Ausübung ihrer Rechte aus Art. 15 bis 22 DSGVO erleichtern. Dies könnte in Form einer elektronischen Antragsstellung erfolgen, siehe Erwägungsgrund 59 zur DSGVO.

Des Weiteren muss der Verantwortliche der betroffenen Person Informationen über die auf Antrag gem. den Art. 15 bis 22 ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen, Art. 12 Abs. 3 S. 1 DSGVO.

Die Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist, Art. 12 Abs. 3 S. 2 DSGVO. In diesem Fall muss die betroffene Person über die Fristverlängerung und deren Gründe informiert werden, Art. 12 Abs. 3 S. 3 DSGVO. Sofern der Verantwortliche auf den Antrag der betroffenen Person nicht tätig wird, muss er die betroffene Person ohne Verzögerung, spätestens innerhalb eines Monats nach Eingang des Antrags, über die Gründe informieren, Art. 12 Abs. 4 DSGVO.

7.1.3 Informationspflicht, Art. 13 DSGVO

Art. 13 DSGVO betrifft Informationspflichten, welche der Verantwortliche bei der Erhebung von personenbezogenen Daten bei der betroffenen Person zu beachten hat.

Zusätzlich zu den o.g. Informationen stellt der Verantwortliche weitere in Art. 13 Abs. 2 DSGVO aufgeführten Informationen der betroffenen Person zur Verfügung.

Sofern der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, stellt er der betroffenen Person vor der Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung, Art. 13 Abs. 3 DSGVO.

7.1.4 Informationspflicht, Art. 14 DSGVO

Sofern die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, muss der Verantwortliche der betroffenen Person dies mitteilen.

Des Weiteren muss der Verantwortliche der betroffenen Person, die in Art. 14 Abs. 2 DSGVO aufgeführten Informationen zur Verfügung stellen.

7.1.5 Betroffenenrechte

Zu den Betroffenenrechten gehören das Auskunftsrecht nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO und ein Recht auf Löschung nach Art. 17 DSGVO. Des Weiteren hat der Betroffene ein Recht auf Datenübertragbarkeit nach Art. 20 DSGVO und ein Widerspruchsrecht nach Art. 21 DSGVO.

7.1.6 Sicherstellung geeigneter technischer und organisatorischer Maßnahmen zum Datenschutz und Sicherheit der Verarbeitung

Nach Art. 24 Abs. 1 DSGVO setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis bringen zu können, dass die Datenverarbeitung im Einklang mit der DSGVO steht. Die technischen und organisatorischen Maßnahmen werden in Kapitel 9 genauer beleuchtet.

7.1.7 Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO

Der Verantwortliche muss ein Verzeichnis aller Verarbeitungstätigkeiten führen. Die konkreten Anforderungen an ein solches Verzeichnis unterscheiden sich dahingehend, ob ein Verantwortlicher (Art. 30 Abs. 1 DSGVO) oder ein Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO) handelt. Eine Ausnahme gilt gem. Art. 30 Abs. 5 DSGVO für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigten, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen in sich, die Verarbeitung erfolgt nur gelegentlich oder es findet keine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DSGVO bzw. Art. 10 DSGVO statt.

In dem Verzeichnis sind vom Verantwortlichen folgende Angaben aufzulisten, Art. 30 Abs. 1 Satz 2 DSGVO:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

Das Verzeichnis ist schriftlich oder in einem elektronischen Format zu führen, da es als Nachweis zur Einhaltung der DSGVO dient. Ferner ist das Verzeichnis der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

7.1.8 Meldung von Verletzungen des Schutzes personenbezogener Daten, Art. 33, 34 DSGVO

Sofern eine Verletzung des Schutzes personenbezogener Daten vorliegt, muss der Verantwortliche unverzüglich und möglichst innerhalb von 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gem. Art. 55 DSGVO zuständigen Aufsichtsbehörde melden. Eine Ausnahme besteht dabei nur, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Sollte die Meldung nicht innerhalb von 72 Stunden an die Aufsichtsbehörde erfolgen, muss der Verantwortliche der Aufsichtsbehörde eine entsprechende Begründung für die Verzögerung beifügen, Art. 33 Abs. 1 DSGVO.

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, Art. 4 Nr. 12 DSGVO.

Der Verantwortliche ist verpflichtet, die Verletzungen des Schutzes personenbezogener Daten zu dokumentieren einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen, Art. 33 Abs. 5 DSGVO. Die möglichen Folgen als auch die Abhilfemaßnahmen müssen dann der zuständigen Aufsichtsbehörde gemeldet werden.

Sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, muss auch die betroffene Person unverzüglich über die Verletzung benachrichtigt werden, Art. 34 Abs. 1 DSGVO. Dabei muss die Benachrichtigung der betroffenen Person in klarer und einfacherer Sprache die Art der Verletzung des Schutzes personenbezogener Daten und die in Art. 33 Abs. 3 DSGVO genannten Informationen und Maßnahmen darlegen.

Eine Benachrichtigung gegenüber der betroffenen Person ist nicht erforderlich, sofern eine in Art. 34 Abs. 3 DSGVO aufgelisteten Bedingungen erfüllt sind.

Des Weiteren kann auch die zuständige Aufsichtsbehörde dem Verantwortlichen gegenüber die Benachrichtigung der betroffenen Person anordnen, Art. 34 Abs. 4 DSGVO.

7.1.9 Datenschutz-Folgenabschätzung, Art. 35 DSGVO

Sofern eine Verarbeitung von Daten, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt, muss vom Verantwortlichen vorab eine Folgenabschätzung durchgeführt werden, Art. 35 Abs. 1 DSGVO.

Der Verantwortliche muss bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, einholen, Art. 35 Abs. 2 DSGVO.

Art. 35 Abs. 3 DSGVO führt Fälle auf, bei denen eine Folgenabschätzung erforderlich ist.

Eine Folgenabschätzung muss mindestens Folgendes enthalten, Art. 35 Abs. 7 DSGVO:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Des Weiteren hat der Verantwortliche bei der Beurteilung der Auswirkungen der durchgeführten Verarbeitungsvorgängen die Einhaltung der genehmigten Verhaltensregeln gem. Art. 40 DSGVO zu berücksichtigen, Art. 35 Abs. 8 DSGVO.

Sofern sich in der Folgenabschätzung herausstellt, dass ein hohes Risiko bei der Verarbeitung für die betroffene Person besteht, muss der Verantwortliche nach Art. 36 DSGVO die zuständige Aufsichtsbehörde vor der Verarbeitung konsultieren. Ebenso ist der zuständige Datenschutzbeauftragte einzubinden. Möglicherweise ist auch der Standpunkt der betroffenen Person oder ihrer Vertreter zu der beabsichtigten Verarbeitung einzuholen, Art. 35 Abs. 9 DSGVO.

Falls erforderlich führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gem. der Datenschutz-Folgenabschätzung durchgeführt wird, Art. 35 Abs. 11 DSGVO.

7.1.10 Benennung eines Datenschutzbeauftragten, Art. 37 DSGVO

Des Weiteren ist vom Verantwortlichen ein Datenschutzbeauftragter zu benennen, sofern:

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO besteht.

Der Verantwortliche muss dabei gem. Art. 38 Abs. 1 DSGVO sicherstellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Die Aufgaben des Datenschutzbeauftragten werden in Art. 39 DSGVO näher geregelt. Besonders bei der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO steht er dem Verantwortlichen zur Verfügung.

7.1.11 Drittlandsübermittlung, Art. 44 ff. DSGVO

Sofern personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt werden, muss der Verantwortliche die Bestimmungen der Art. 44 ff. DSGVO beachten (siehe Kapitel 8).

7.2 Gemeinsame Verantwortlichkeit

Im Projekt WearPrivate könnte eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO vorliegen. Hierfür bedarf es einer gemeinsamen Entscheidung über Zwecke und Mittel der Datenverarbeitung, Art. 26 Abs. 1 S. 1 DSGVO. Diese Rechtsfigur wird indes sehr weit ausgelegt. So kann eine stillschweigende Einflussnahme auf die Datenverarbeitung aus reinem Eigeninteresse bereits eine gemeinsame Verantwortlichkeit begründen. Zudem ist es weder erforderlich, dass beide Verantwortliche im selben Stadium der Datenverarbeitung tätig werden, noch bedarf es überhaupt eines Zugriffs beider Parteien auf die verarbeiteten Daten.

Folgende Punkte sind bei der Bewertung der gemeinsamen Verantwortlichkeit zu beachten[197]:

- Zugang zu den personenbezogenen Daten: Es müssen nicht alle Parteien Zugang zu den personenbezogenen Daten haben.
- Gemeinsamer Zweck: Gemeinsamer Zweck muss nicht der Verarbeitungszweck sein (Allgemeiner übergeordneter Zweck oder übergeordnetes Ziel genügt).
- Gemeinsame Entscheidung: Eine gemeinsame Entscheidung ist durch Einflussnahme auf die Verarbeitung (auch stillschweigend) möglich.
- Phasenweise Betrachtung: Ein unterschiedliches Ausmaß an Verantwortlichkeit in verschiedenen Phasen ist möglich.

An die **gemeinsame** Entscheidung über Zweck und Mittel der Datenverarbeitung sind geringe Anforderungen zu stellen, es reichen schon rudimentäre Absprachen aus.[198] Auch die weitestgehend

---

[197] KREMER in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO, Art. 26 Rn. 44 ff.

[198] TRISTAN RADKTE, Gemeinsame Verantwortlichkeit unter der DSGVO, S. 158 f.

unabhängige Tätigkeit einer jeden Partei widerspricht einer gemeinsamen Verantwortlichkeit nicht.[199] Wie gesehen, wird der Begriff der gemeinsamen Verantwortlichkeit sehr weit ausgelegt.

Die Annahme einer gemeinsamen Verantwortlichkeit bringt Verpflichtungen mit sich. Jeden Verantwortlichen treffen eine Reihe von Verpflichtungen, die er erfüllen muss (s.o.).

Die gemeinsame Verantwortlichkeit bringt die Verpflichtung mit sich, in einer Vereinbarung (einem Joint-Controller-Vertrag) festzulegen, wer welche Verpflichtungen wahrnimmt und wie die jeweiligen Funktionen und Beziehungen ausgestaltet sind.[200] Fehlt es an einem entsprechenden Vertrag, kann dies zu Bußgeldern führen. Der Mindestinhalt des Vertrages ist in Art. 26 DSGVO geregelt.

7.3 Auftragsverarbeitung

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen erhebt, verarbeitet oder nutzt und rechtlich außerhalb des Verantwortlichen steht.[201]

Der Auftragsverarbeiter ist als „verlängerter Arm“ des „Herrn der Daten“ (= der Verantwortliche) zu qualifizieren. Der Verantwortliche als auch der Auftragsverarbeiter bilden eine „Verarbeitungseinheit“.[202]

Charakteristisch für das Vorliegen einer Auftragsverarbeitung ist die Weisungsgebundenheit des Auftragsverarbeiters. Der Auftragsverarbeiter verarbeitet personenbezogene Daten der Betroffenen im Auftrag des Verantwortlichen.[203]

Der Auftragsverarbeiter ist zur Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen verpflichtet.

Die DSGVO gibt nicht vor, dass eine Beschränkung lediglich auf die Erbringung von technischen Hilfeleistungen besteht.[204]

---

199 TRISTAN RADKTE, Gemeinsame Verantwortlichkeit unter der DSGVO, S. 159.

200 KÜHLING/KLAR/SACKMANN, Datenschutzrecht, Rn. 536.

201 ARNING/ROTHKEGEL in: Taeger/Gabel, DS-GVO Art. 4, Rn. 246.

202 SCHMIDT/SCHMIDT in: Hamm, Beck’sches Rechtsanwalts-Handbuch, § 50 Rn. 42

203 ARNING/ROTHKEGE in: Taeger/Gabel, DS-GVO Art. 4, Rn. 254.

204 ARNING/ROTHKEGEL in: Taeger/Gabel, DS-GVO Art. 4, Rn 248.

Durch die Hinzuziehung eines Auftragsverarbeiters ist der Betroffene weiteren Risiken ausgesetzt. Denn auch der Auftragsverarbeiter hat erweiterte Zugriffsmöglichkeiten auf die personenbezogenen Daten des Betroffenen, wobei es bei Vorliegen der Voraussetzungen des Art. 28 DSGVO keiner weiteren Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten bedarf.[205] Folglich muss auch keine Einwilligung des Betroffenen eingeholt werden.[206]

Die Risiken werden durch strenge Voraussetzungen der Auftragsverarbeitung kompensiert.[207] Der Auftragsverarbeiter darf keine eigene Entscheidung treffen. Dies ist dem Verantwortlichen vorbehalten.[208] Sofern der Auftragsverarbeiter jedoch über Zwecke und Mittel der Datenverarbeitung entscheidet, gilt er gemäß Art. 28 Abs. 10 DSGVO selbst als Verantwortlicher. Eine mögliche weitere davon zu trennende Konstellation ist die der gemeinsamen Verantwortung nach Art. 26 DSGVO.

Um die Risiken des Betroffenen weiter einzudämmen, erfolgt die Datenverarbeitung des Auftragsverarbeiters gemäß Art. 28 Abs. 3 S. 1 DSGVO auf der Grundlage eines schriftlichen oder in elektronischer Form vorliegenden Vertrages oder eines anderen Rechtsinstruments. In einem solchen Vertrag müssen der Gegenstand und die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt werden.

Sofern sich diese Angaben aus dem zugrundeliegenden Hauptvertrag des Verantwortlichen ergeben, kann darauf verwiesen werden.[209]

Nach Art. 30 Abs. 2 DSGVO muss der Auftragsverarbeiter ein schriftliches Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führen.

Die Haftung des Auftragsverarbeiters ist nach Art. 82 Abs. 2 DSGVO auf Verstöße gegen die ihm auferlegten Pflichten aus der DSGVO und der Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisung beschränkt.

---

[205] SCHMIDT/SCHMIDT in: Hamm, Beck'sches Rechtsanwalts-Handbuch, § 50 Rn. 42.

[206] SCHEJA/REIBACH in: Leupold, Wiebe/Glossner, Teil 6.6, Rn. 202.

[207] SCHMIDT/SCHMIDT in: Hamm, Beck'sches Rechtsanwalts-Handbuch, § 50 Rn. 42.

[208] SCHMIDT/SCHMID in: Hamm, Beck'sches Rechtsanwalts-Handbuch, § 50 Rn. 43.

[209] SCHMIDT/SCHMIDT in: Hamm, Beck'sches Rechtsanwalts-Handbuch, § 50 Rn. 44a.

7.3.1 Pflichten des Auftragsverarbeiters

7.3.1.1 Unterstützungspflichten

Den Auftragsverarbeiter treffen umfassende Unterstützungspflichten. Gemäß Art. 28 Abs. 3 S. 2 lit. e DSGVO hat der Auftragsverarbeiter den Verantwortlichen mit geeigneten Maßnahmen bei der Gewährleistung der Betroffenenrechte zu unterstützen. Ferner ist er auch dazu verpflichtet, den Verantwortlichen bei der Einhaltung der Verpflichtungen nach Art. 32 – 26 DSGVO zu unterstützen, Art. 28 Abs. 3 S. 2 lit. f DSGVO.

7.3.1.2 Führen eines Verfahrensverzeichnisses

Der Auftragsverarbeiter ist zum Führen eines Verfahrensverzeichnisses gem. Art. 30 Abs. 2 DSGVO verpflichtet. Die konkreten Anforderungen sind in Art. 30 Abs. 2 DSGVO geregelt. Das Verzeichnis ist nach Art. 30 Abs. 3 DSGVO schriftlich zu führen. Die elektronische Form ist dabei nicht ausgeschlossen. Soweit ein Unternehmen oder eine Einrichtung weniger als 250 Mitarbeiter beschäftigt, die vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Person darstellt, die Verarbeitung nur gelegentlich erfolgt oder keine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DSGVO, Art. 10 DSGVO erfolgt, muss kein Verzeichnis geführt werden.

7.3.1.3 Drittlandsübermittlung

Auch der Auftragsverarbeiter muss bei der Drittlandsübermittlung die Bedingungen der Art. 44 ff. DSGVO (siehe Kapitel 7.1.11) beachten.

7.3.1.4 Ergreifen technischer und organisatorischer Maßnahmen der Datensicherheit, Art. 32 Abs. 1 DSGVO

Den Auftragsverarbeiter muss geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.[210]

7.4 Verantwortlichkeit im Projekt WearPrivate

Im Rahmen von WearPrivate stellt sich die Frage, wer beim Einsatz eines Brustgurtes am Arbeitsplatz Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist. Dafür ist zu bewerten, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet. In Betracht kommt die alleinige Verantwortlichkeit des Arbeitgebers und die Tätigkeit als Auftragsverarbeiter des Analyseservices sowie eine gemeinsame Verantwortlichkeit des Arbeitgebers und Analyseservices. Ferner sind auch der App-Anbieter und der Cloudservice, mit dem der Analyseservice arbeitet, zu betrachten. Um die Verantwortlichkeit im

[210] Siehe hierzu Kapitel 7.1.6.

Projekt zu klären, wurde ein Fragenkatalog erstellt und den Anwendungspartnern WearHealth und Neusta zur Verfügung gestellt; auf Grundlage des Feedbacks wurde die Verantwortlichkeit bewertet.[211]

7.4.1 Arbeitgeber

Wesentliche Entscheidungen hinsichtlich des Wearable-Einsatzes trifft der Arbeitgeber. Die Tatsache, dass er nicht selbst die Datenverarbeitung durchführt, ist unerheblich. Er entscheidet darüber, zu welchem Zweck die Daten der Arbeitnehmer erhoben werden sollen. Entschließt er sich dazu, den Gesundheitsschutz für die Arbeitnehmer zu erhöhen, kann er darüber entscheiden, wie dieses Ziel erreicht werden soll. Im Anwendungsfall von WearPrivate werden zu diesem Zweck der Fitnessgurt sowie die neu entwickelte App eingesetzt. Entscheidet sich der Arbeitgeber für diese Vorgehensweise, trifft er also die Entscheidung über den Zweck der Datenerhebung (Gesundheitsschutz, Stresslevelmessung), entscheidet über die Art der erhobenen Daten (HRV) und wählt das Mittel der Durchsetzung (Fitnessgurt, App). Der Arbeitgeber ist mithin als Verantwortlicher zu sehen.

7.4.2 Analyseservice

Neben dem Arbeitgeber, der im betrachteten Szenario entscheidet, ob und wie die Wearables eingesetzt werden, kommt auch noch der Analyseservice als Verantwortlicher in Betracht. Aus den unter 14.1 zu findenden Angaben von WearHealth zu ihrer eigenen Rolle im WearPrivate Szenario kann geschlossen werden, dass auch der Analyseservice als Verantwortlicher fungiert. Demnach besteht nicht nur eine direkte Beziehung zwischen Analyseservice und den betroffenen Personen, der Analyseservice übt auch die Kontrolle über die erhobenen Daten aus. Darüber hinaus besteht auch ein Eigeninteresse des Analyseservices an der Datenverarbeitung, da die Daten Teil des internen Algorithmus werden und dazu verwendet werden, das eigene Produkt zu verbessern.

Die oben genannten Pflichten des Verantwortlichen sind daher vom Analyseservice einzuhalten. Ferner ist ein Joint-Controller-Vertrag nach Art. 26 DSGVO mit dem Arbeitgeber zu schließen.

Nach Art. 26 Abs. 1 S. 2 DSGVO ist in diesem Vertrag in transparenter Form festzulegen, wer welche Verpflichtung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten nach Art. 13, 14 DSGVO nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. Darüber hinaus muss der Vertrag die tatsächlichen Funktionen der gemeinsam Verantwortlichen widerspiegeln, Art. 26 Abs. 1 S. 3 DSGVO. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben

[211] Den Fragenkatalog blanko sowie von beiden Partnern ausgefüllt, findet sich unter Kapitel 14.

werden, obwohl es nach Art. 26 Abs. 3 DSGVO für Betroffene möglich ist, bei beiden Verantwortlichen Betroffenenrechte nach den Art. 15 ff. DSGVO geltend zu machen.

7.4.3 App-Anbieter

Im vorliegenden Fall stellt sich insbesondere die Frage, ob auch der App-Anbieter als Auftragsverarbeiter zu betrachten ist. Mangels einer Entscheidung über Zweck und Mittel der Verarbeitung kann die Verantwortlichkeit des App-Anbieters ausgeschlossen werden, da die erhobenen Daten nicht verwendet werden, um das eigene Angebot zu verbessern. Allerdings könnte eine Auftragsverarbeitung vorliegen.

Dafür müsste der App-Anbieter die Datenverarbeitung im Auftrag der Verantwortlichen durchführen. Fraglich ist, ob der App-Anbieter hier tatsächlich eine Datenverarbeitung im Auftrag des Analyseservices oder des Arbeitgebers durchführt. Die Daten der Arbeitnehmer werden lokal auf dem Endgerät des Arbeitnehmers gespeichert und werden zu keinem Zeitpunkt auf den Servern des App-Anbieters verarbeitet. Allerdings werden die gesammelten Rohdaten von der App an den Cloudanbieter weitergegeben und dort dann vom Analyseservice verarbeitet; die Ergebnisse der Verarbeitung und auch mögliche Alerts werden in der App angezeigt.

Die Rolle des App-Anbieters ist an dieser Stelle zu bewerten. Es kommt hier entscheidend darauf an, wie es zur Datenübertragung von der App zur Cloud kommt, wo die Rohdaten anschließend verarbeitet werden. Im Falle von WearPrivate wird im Code der App festgelegt, an welchen Cloudserver die Daten übertragen werden. Dies führt dazu, dass vom App-Anbieter in diesem Zusammenhang keine relevanten Entscheidungen getroffen werden. Vielmehr liegt die Aufgabe bzw. Funktion des App-Anbieters lediglich in der Bereitstellung der App. Eine Verarbeitung personenbezogener Daten durch den App-Anbieter erfolgt nicht.

Würde der App-Anbieter allerdings darüber entscheiden, an welchen Server die Daten zur weiteren Verarbeitung geschickt werden, wäre eine Auftragsverarbeitung anzunehmen.

7.4.4 Cloudservice

Der Cloudservice wird personenbezogene Daten verarbeiten. Nach diesem Vertrag wird Cloud-Anbieter verpflichtet, nur nach Weisungen zu arbeiten, sowie die Vorschriften der DSGVO einzuhalten sind.

WearHealth arbeitet derzeit mit Amazon Web Services (AWS)-Cloud Computing zusammen, dabei werden einzelne oder mehrere Datenverarbeitungsvorgänge in einer sog. Cloud ausgelagert. Vorliegend werden die gesammelten Rohdaten der App an die AWS-Cloud weitergegeben und dort von WearHealth verarbeitet. WearHealth entscheidet, was mit den erhobenen Daten passiert, sobald

sie in die Cloud geladen wurden. Die gesamte Verarbeitung von WearHealth findet in der Cloud statt. Dies ist in der AWS-Cloud auch möglich. Auf der Homepage wird beschrieben, dass AWS-Service eine „Datenanalyse“ anbietet. [212]

AWS nimmt keine eigene Entscheidung hinsichtlich des Zwecks der Verarbeitung der personenbezogenen Daten vor. Dies behält sich WearHealth vor. AWS soll dabei keine eigenen Nutzungsrechte haben. Dies ist u.a. WearHealth vorbehalten. WearHealth überwacht AWS und koordiniert die Berechnungen, die AWS durchführt.

All die Punkte sprechen dafür, dass der Cloudservice so wie derzeit eingesetzt Auftragsverarbeiter nach Art. 28 DSGVO ist.

8 Übermittlung von personenbezogenen Daten in Drittländer

Einer genaueren Betrachtung bedarf auch die Übermittlung der Daten in ein Drittland. Sollten die Wearable-Daten der Arbeitnehmer im Projekt WearPrivate in einem Drittland verarbeitet werden, sollte zunächst geprüft werden, ob die Datenübermittlung in jenes Land zulässig ist. Als Drittländer gelten alle Länder, die nicht Mitglied der EU sind. Es zählen auch die EWR-Staaten Island, Liechtenstein und Norwegen zur Gruppe der Drittländer.[213] Auch das Vereinigte Königreich zählt seit dem vollzogenen Brexit als Drittland. [214] Zu beachten ist, dass Daten nicht beliebig in Drittländer übermittelt werden dürfen. Insbesondere müssen effektive Rechtsschutzmöglichkeiten zur Verfügung stehen. Der Drittlandstransfer ist nur möglich, soweit ein Erlaubnistatbestand der DSGVO gemäß Art. 45 ff. DSGVO einschlägig ist, beispielsweise wenn ein Angemessenheitsbeschluss für das in Rede stehende Land vorliegt. Daher muss im Projekt WearPrivate auch darauf geachtet werden, wohin Daten transferiert werden.

Die folgenden Erlaubnistatbestände können einen Datentransfer in ein Drittland ermöglichen:

- Angemessenheitsbeschluss der Kommission, Art. 45 DSGVO: Voraussetzungen finden sich in Art. 45 Abs. 2 DSGVO. (lit. a: Rechtsordnung des Drittlands bezüglich personenbezogener

---

[212] https://aws.amazon.com/de/big-data/datalakes-and-analytics/?hp=tile&tile=solutions abgerufen am 14.11.2022; https://aws.amazon.com/de/compliance/gdpr-center/ abgerufen am 14.11.2022.

[213] PAULY in Paal/Pauly, DS-GVO/BDSG, 3. Auflage 2021, Art. 44 Rn. 6.

[214] PAULY in Paal/Pauly, DS-GVO/BDSG, 3. Auflage 2021, Art. 44 Rn 7.

Daten; lit. b: unabhängige Datenschutzbehörden; lit. c: internationale Verpflichtungen bezüglich des Datenschutzes)[215]

- Geeignete Garantien (Standardvertragsklauseln), Art. 46 DSGV: Besonders wichtig sind hier die Standarddatenschutzklauseln der Kommission, Art. 46 Abs. 2 DSGVO. Dies sind von der Europäischen Kommission erlassene geeignete Garantien.[216]
- Verbindliche interne Datenschutzregeln, Art. 47 DSGVO
- Ausnahmen in Einzelfällen, Art. 49 DSGVO

Dass an den Angemessenheitsbeschluss hohe Anforderungen zu stellen sind, zeigen sich in den verschiedenen „Schrems"-Entscheidungen des Europäischen Gerichtshofes. Es geht jeweils um die Übermittlung von personenbezogenen Daten in die USA, zunächst aufgrund des sogenannten „Safe Harbor"-Abkommens, später aufgrund des „Privacy Shields". In beiden Fällen lag indes **kein** Angemessenheitsbeschluss vor, da die USA nicht als sicheres Drittland angesehen wurde. Jedoch bestanden jeweils Sonderregelungen für die USA, wonach sich bestimmte Unternehmen datenschutzrechtlichen Regelungen unterwerfen konnten (Selbstverpflichtung), wobei sie von US-Behörden überwacht wurden.[217] Das „Privacy Shield" war eine Erweiterung des „Safe Harbors", welche versuchte, auf die Kritikpunkte, die der EuGH im „Schrems I"-Urteil äußerte, zu reagieren (u.a. strengere Auflagen für den Zugriff auf Daten durch Behörden und erweiterte Rechtsschutzmöglichkeiten).[218] Jedoch wurden beide Sonderregelungen vom EuGH für nichtig erklärt.[219] Bei dem „Privacy Shield"-Abkommen kritisierte der Gerichtshof die zu weit reichenden Zugriffsmöglichkeiten der US-Geheimdienstbehörden und zudem die mangelhaften Rechtsschutzmöglichkeiten der betroffenen EU-Bürger.[220] Besonders problematisch ist, dass die Geheimdienste und Strafverfolgungsbehörden Zugriffsrechte auf alle Daten haben. Im Zuge dessen wurde der Clarifying Lawful Overseas Use of Data Act (CLOUD Act) erlassen.[221] Der CLOUD Act ist eine Erweiterung des US-Recht, die den geografischen Umfang von Strafverfolgungsanfragen der USA klärt

---

[215] ZERDICK in: Ehmann/Selmayr DSGVO, Art. 45 Rn. 7.

[216] ZERDICK in: Ehmann/Selmayr DSGVO, Art. 46 Rn. 10.

[217] PAULY in: Paal/Pauly DSGVO Art. 45 Rn. 9.

[218] PAULY in: Paal/Pauly DSGVO Art. 45 Rn. 17 f.

[219] EuGH, EuZW 2015, 881 (885 ff.) – Schrems I (Safe Harbor); EuGH, GRUR-RS. 2020, 16082, Rn. 201 – Schrems II.

[220] EuGH, GRUR-RS. 2020, 16082, Rn. 201 – Schrems II (Rn. 172 ff./Rn. 186 ff.)

[221] https://www.congress.gov/bill/115th-congress/house-bill/4943 abgerufen am 14.11.2022.

und Serviceanbietern neue Methoden eröffnet, Anfragen abzulehnen, die in Konflikt mit den Gesetzen oder nationalen Interessen stehen.[222] Jedoch haben durch diesen Act amerikanische Behörden weiterhin Zugriff auf sämtliche Unternehmens- und Kundendaten von Cloudanbietern, sofern das Unternehmen seinen Sitz in den USA hat. Neben dem CLOUD Act ist auch der Foreign Intelligence Surveillance Act (FISA) von 1978 (Section 702) relevant. Der FISA Act räumt insbesondere US-amerikanischen Geheimdiensten weitreichende Befugnisse ein, die nicht mit dem Verhältnismäßigkeitsgrundsatz der unionsrechtlichen Regelungen in Einklang zu bringen sind.[223] Diese weitreichenden Befugnisse der US-amerikanischen Behörden wurden allerdings durch das EU-US-Data-Privacy-Framework entschärft. Hierbei handelt es sich um einen Angemessenheitsbeschluss, der den Datentransfers zwischen der EU und der USA unter gewissen Umständen ohne Rückgriff auf andere Rechtsgrundlagen aus Kapitel V der DSGVO ermöglicht.[224] Der neue Angemessenheitsbeschluss greift mehrere Kritikpunkt aus den Urteilen des EuGHs zum Safe-Harbor-Abkommen und zum Privacy-Shield-Abkommen auf. So wird sowohl ein Rechtsschutzmechanismus für Unionsbürger im Data Privacy Framework enthalten sein, als auch eine Einschränkung der weitreichenden Befugnisse US-amerikanischer Behörden beim Zugriff auf personenbezogene Daten.[225] So regelt das Framework einen zweistufigen Rechtsschutzmechanismus, in dessen Rahmen sich Unionsbürger zunächst an eine Datenschutzbehörde ihres Heimatlandes wenden müssen, die das Anliegen an die US-Regierung weiterleitet.[226] Im Anschluss wird die Beschwerde vom Datenschutzbeauftragten der US-Geheimdienstkoordinationsstelle geprüft.[227] Im Anschluss daran besteht weiterhin die Möglichkeit für Unionsbürger beim quasi-gerichtlichen Data Protection Review Court Berufung einzulegen, ohne dass hierfür die Entscheidung über die Beschwerde bekannt sein muss.[228] Der Data Protection Review Court prüft die vorangegangene Entscheidung inhaltlich umfassend und teilt anschließend mit, dass eine verbindliche Entscheidung ergangen ist, allerdings nicht deren Inhalt.[229] Ferner übernimmt die US-

---

[222] https://aws.amazon.com/de/compliance/cloud-act/ abgerufen am 14.11.2022.

[223] PAULY in: Paal/Pauly, Art. 45 DSGVO Rn. 24c.

[224] https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/17_Angemessenheitsbeschluss-EU-US-DPF.html.

[225] GLOCKER, RDi 2023, 465 (466 Rn. 6).

[226] GLOCKER, RDi 2023, 465 (466 Rn. 8).

[227] A.a.O., Rn. 9.

[228] A.a.O., Rn. 10.

[229] Ebd.

Regierung die Begriffe der Erforderlichkeit und Verhältnismäßigkeit hinsichtlich der Rechtmäßigkeit behördlicher Zugriffe.[230]

Zu beachten ist allerdings, dass das Framework einen ähnlichen Selbstzertifizierungsmechanismus wie seine Vorgänger regelt. Nur die Datenübermittlungen an solche selbstzertifizierten Unternehmen sind vom neuen Angemessenheitsbeschluss erfasst.[231] Für eine Selbstzertifizierung bedarf es 4 Schritten: (1) Das Unternehmen muss eine Meldung an das Department of Commerce richten, in der es erklärt, sich an bestimmte Datenschutzpflichten zu halten; (2) Das Unternehmen muss sich für Beschwerden von Unionsbürgern entweder den europäischen Aufsichtsbehörden oder einem privatwirtschaftlichen Schiedsmechanismus unterwerfen[232]; (3) Das Unternehmen muss in seiner Datenschutzerklärung öffentlich versprechen, die Datenschutzpflichten des Data Privacy Frameworks einzuhalten[233] und (4) Das Unternehmen muss eine Verwaltungsgebühr zahlen.[234] Die Einhaltung der formellen Voraussetzungen wird vom U.S. Department of Commerce geprüft und der Name des Unternehmens wird anschließend veröffentlicht.[235]

Existiert kein Angemessenheitsbeschluss, so ist es erforderlich, dass geeignete Garantien und wirksame (verwaltungsrechtliche und gerichtliche) Rechtsbehelfe, also durchsetzbare Rechte zur Verfügung gestellt werden (Standarddatenschutzklauseln). Nicht ausreichend ist hier eine Ombudsperson. Es bedarf eines unabhängigen Gerichts, welches über datenschutzrechtliche Beschwerden entscheidet und berät. Welche Rechtsgrundlage für Drittlandstransfers im Projekt WearPrivate datenschutzfreundlich genutzt werden kann, ist vom Einzelfall abhängig und wird fortlaufend anhand des Anwendungsfalls geprüft.

---

[230] GLOCKER, RDi 2023, 465 (467 Rn. 12).

[231] GLOCKER, RDi 2023, 465 (467 Rn. 14).

[232] GLOCKER, RDi 2023, 465 (467 Rn. 15) mit Verweis auf: EU-U.S. Data Privacy Framework Principles, Ziffer 11.

[233] GLOCKER, RDi 2023, 465 (467 Rn. 15) mit Verweis auf: ErwG 50 des Angemessenheitsbeschlusses, C (2023) 4745 final.

[234] GLOCKER, RDi 2023, 465 (467 Rn. 15).

[235] GLOCKER, RDi 2023, 465 (467 Rn. 15) mit Verweis auf: Anhang III zum Angemessenheitsbeschluss, C (2023) 4745 final, S. 3.

8.1 Anwendung auf WearPrivate

Die Datenverarbeitung wird im Rahmen von WearPrivate von WearHealth innerhalb der AWS-Cloud durchgeführt.[236] Fraglich ist, ob durch diese Verarbeitung in der Cloud Daten in andere Länder übermittelt werden. Wird eine Datenübermittlung vorgenommen, ist zu prüfen, ob die Übermittlung auf eine Rechtsgrundlage gemäß der Art. 44 ff. DSGVO gestützt werden kann. Das Unternehmen Amazon, welches die AWS-Cloud anbietet, ist ein US-amerikanischer Konzern mit Hauptsitz in Seattle.

AWS ist ein Tochterunternehmen von Amazon.com. Amazon sitzt in Seattle, Washington und somit in den USA. Die USA sind ein Drittland. Für die Datenübermittlung in die USA könnte sich die AWS-Cloud auf den neuen Angemessenheitsbeschluss zwischen EU und USA berufen und müsste keine weitere Rechtsgrundlage heranziehen, soweit das Unternehmen ein selbstzertifiziertes Unternehmen im Sinne des Frameworks darstellt. Amazon stellt ein solches Unternehmen dar.[237]

Andernfalls wäre eine Berufung auf die Standarddatenschutzklauseln möglich oder die Berufung auf eine Einwilligung im Sinne des Art. 49 Abs. 1 S. 1 lit a DSGVO. Diese muss allerdings ausdrücklich abgegeben werden, wobei betroffene Personen zuvor aufgeklärt werden müssen. Die Einwilligung könnte über die App eingeholt werden. Aufzuzeigen ist den betroffenen Personen, welche Konsequenzen sich aus der Übermittlung in ein „unsicheres Drittland“ ergeben könnten. Insbesondere sind die Nutzer darüber zu informieren, dass weder ein Angemessenheitsbeschluss (bzw. wieso dieser im vorliegenden Fall nicht zur Anwendung kommt) noch geeignete Garantien zum Schutz der Daten vorliegen, Art. 49 Abs. 1 S. 1 lit. a DSGVO.

9 Technische und organisatorische Maßnahmen nach der DSGVO

Die DSGVO adressiert auch die Sicherheit der verarbeiteten personenbezogenen Daten. Die relevanten Regelungen finden sich in den Art. 24, 25 und 32 DSGVO. Unter technischen und organisatorischen Maßnahmen sind solche Maßnahmen zu verstehen, die dazu dienen, die Beachtung des Datenschutzes und der Datensicherheit bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten und den dazu betriebenen Verfahren sicherzustellen[238]. Technische Maßnahmen beziehen sich auf den

---

[236] Siehe hierzu: https://aws.amazon.com/de/big-data/datalakes-and-analytics/?hp=tile&tile=solutions, letzter Abruf 14.09.2022.

[237] GLOCKER, RDi 2023, 465 (468 Rn. 19).

[238] SCHMIDT/BRINK in: BeckOK DatenschutzR, Art. 24 DSGVO Rn. 14.

Datenverarbeitungsvorgang selbst, während organisatorische Maßnahmen den äußeren Ablauf der Datenverarbeitung betreffen.[239]

Aus Art. 24 DSGVO ergeben sich indes keine bestimmten Anforderungen an technische und organisatorische Maßnahmen: Die Vorschrift erlegt dem Verantwortlichen vielmehr allgemein die Pflicht auf, angemessene technische und organisatorische Maßnahmen zu ergreifen und einen Nachweis hierüber zu führen. Die allgemeine Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO wird durch Art. 24 Abs. 1 DSGVO mithin ergänzt. Über die Dokumentation zwecks Nachweispflicht hinaus ist der Verantwortliche auch dazu verpflichtet, die ergriffenen Maßnahmen regelmäßig zu überprüfen und ggf. zu aktualisieren, Art. 24 Abs. 1 S. 2 DSGVO.

Nähere Bestimmung hinsichtlich des Inhalts von technischen und organisatorischen Maßnahmen enthalten die Art. 25 und 32 DSGVO.

Art. 25 DSGVO regelt die Grundsätze „Privacy by Design“ und „Privacy by Default“, die den Datenschutz durch Technikgestaltung und den Datenschutz durch Voreinstellungen betrifft.

9.1 Privacy by Design, Art. 25 Abs. 1 DSGVO

Die grundsätzliche Bedeutung des Grundsatzes „Privacy by Design“ liegt in der Integrierung datenschutzfördernder Maßnahmen bereits im Entwicklungsstadium eines System- oder Prozessdesigns.[240]

9.2 Privacy by Default, Art. 25 Abs. 2 DSGVO

Der Grundsatz “Privacy by Default“ adressiert Datenschutz durch Voreinstellungen. Ziel ist es also, den Datenschutz bereits dadurch zu fördern, dass die Grund- bzw. Voreinstellungen bei einem Gerät bzw. bei einem Programm besonders datenschutzfreundlich ausgestaltet werden.

9.3 Sicherheit der Verarbeitung, Art. 32 DSGVO

Die zentrale Vorschrift in der DSGVO zu technischen und organisatorischen Maßnahmen ist Art. 32 DSGVO. Art. 32 DSGVO konkretisiert die allgemeine Vorschrift des Art. 24 Abs. 1 DSGVO.[241] Festgelegt wird in dieser Vorschrift, dass vom Verantwortlichen geeignete technische und organisatorische

---

[239] SCHMIDT/BRINK in: BeckOK DatenschutzR, Art. 24 DSGVO Rn. 15.

[240] HENSE in: Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Teil 33.2 Rn. 6.

[241] HLADJIK in: Ehmann/Selmayr, Art. 32 Rn. 1.

Maßnahmen zu ergreifen sind, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ferner zeigt die Vorschrift verschiedene Maßnahmen auf, durch die der Verantwortliche seine Verpflichtung erfüllen kann. Hierzu gehört beispielsweise die Pseudonymisierung oder Verschlüsselung (Abs. 1 lit. a). Art. 32 DSGVO dient der Sicherheit der Datenverarbeitung und gilt als Ausgestaltung des Grundsatzes der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO.[242] Über Integrität und Vertraulichkeit hinaus existieren weitere Gewährleistungsziele, deren Schutz auch durch Art. 32 DSGVO u.a. bezweckt wird.[243] Die Gewährleistungsziele stellen dabei solche Eigenschaften der rechtskonformen Datenverarbeitung dar, die es durch technische und organisatorische Maßnahmen zu erreichen gilt.[244] Zu den Gewährleistungszielen[245] zählen:

- Verfügbarkeit, Anforderung, dass personenbezogene Daten zur Verfügung stehen müssen und ordnungsgemäß im vorgesehenen Prozess verwendet, werden können
- Integrität, Einhaltung informationstechnischer Prozesse und Systeme und Einhaltung ihrer zweckbestimmten Funktionen sowie Einhaltung der Aktualität
- Vertraulichkeit, die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen kann
- Nichtverkettung, keine Zusammenführung von personenbezogenen Daten ohne rechtliche Grundlage
- Transparenz, Erkennbarkeit der Verarbeitungen

---

[242] SCHULTZE-MELLING in: Taeger/Gabel, Art. 32 DSGVO Rn. 1.

[243] 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 – Erprobungsfassung vom 25./26. April 2018, S. 11 ff.

[244] 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 – Erprobungsfassung vom 25./26. April 2018, S. 11.

[245] Hierzu: 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 – Erprobungsfassung vom 25./26. April 2018, S. 14 ff.; FREUND in: Schuster/Grützmacher IT-Recht, Art. 32 DSGVO Rn. 3 ff.

- Intervenierbarkeit, die Anforderung, dass den Betroffenen die Betroffenenrechte jederzeit wirksam gewährt und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen

Grundsätzlich ist bei der Bewertung von TOMs immer eine Risikoabwägung vorzunehmen und es sind solche Maßnahmen zu ergreifen, die dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessen sind. Zu berücksichtigen sind grundsätzlich solche Maßnahmen, die technisch und praktisch realisierbar sind. Dabei ist insbesondere zu beachten, welche Kategorie von Daten verarbeitet wird. Da im Szenario des Projekts WearPrivate zum größten Teil Gesundheitsdaten verarbeitet werden, besteht im betrachteten Fall ein besonderes Risiko für die Rechte der betroffenen Personen. Gesundheitsdaten stellen eine besonders sensible Kategorie von personenbezogenen Daten dar, hinsichtlich derer es eines besonderen Schutzes bedarf. Dementsprechend sind auch besondere Schutzmaßnahmen zu ergreifen, die über übliche TOMs hinausgehen. Hierbei ist zu unterscheiden nach solchen Maßnahmen, die von der App umgesetzt werden und solchen Maßnahmen, die vom Analysedienstleister und ggf. Cloud umzusetzen sind.

9.3.1 Angemessenes Schutzniveau

Art. 32 DSGVO wohnt eine Angemessenheits-, im Kern eine Verhältnismäßigkeitsprüfung, inne. Zu ergreifen sind nur solche TOMs, die mit einem angemessenen Aufwand erreicht werden können.[246] Zur Beurteilung der Angemessenheit des Schutzniveaus sind nach Art. 32 Abs. 2 DSGVO die Risiken der Verarbeitung miteinzubeziehen. Nach Art. 32 Abs. 2 DSGVO gehören hierzu insbesondere Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugter Zugang zu personenbezogenen Daten. Diese Aufzählung ist allerdings nicht abschließend[247] und es können im Einzelfall weitere Risiken danebentreten. Zu beachten sind stets die Eintrittswahrscheinlichkeit sowie die Schwere des Risikos.[248]

Erforderlich ist mithin eine umfassende Prüfung möglicher Risiken unter Einbeziehung der Eintrittswahrscheinlichkeit sowie auch der Schwere des möglichen Schadens vor dem Hintergrund der Sensibilität der verarbeiteten Daten. Eine generische Einschätzung des Schutzniveaus verbietet sich indes.

---

[246] FREUND in: Schuster/Grützmacher IT-Recht, Art. 32 DSGVO Rn. 18.

[247] SCHULTZE-MELLING in: Taeger/Gabel, Art. 32 DSGVO Rn. 23.

[248] S. Fn.: 172.

9.4 Überblick über die technischen und organisatorischen Maßnahmen

9.4.1 DSGVO

Im Folgenden erfolgt ein Überblick über die klassischen Maßnahmen zum Schutz der Gewährleistungsziele, nach dem Standard-Datenschutzmodell (SDM):[249]

Datenminimierung	Reduzierung von erfassten Rohdaten der betroffenen Personen auf das notwendige Mindestmaß
	Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
	Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
	Bevorzugung von automatisierten Verarbeitungsprozessen gegenüber von Entscheidungsprozessen (Begrenzung der Einflussnahme)
	Implementierung automatischer Sperr- und Löschroutinen und von Pseudonymisierungs- und Anonymisierungsverfahren (bestenfalls von Anfang an)
	Nur eingeschränktes Logging der Aktionen der betroffenen Personen
Verfügbarkeit	Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts → Logdateien
	Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
	Dokumentation der Syntax der Daten
	Redundanz von Hard- und Software sowie Infrastruktur
	Umsetzung von Reparaturstrategien und Ausweichprozessen
	Vertretungsregelungen für abwesende Mitarbeitende
Integrität	Einschränkung von Schreib- und Änderungsrechten
	Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptographiekonzepts
	Dokumentierte Zuweisung von Berechtigungen und Rollen
	Prozesse zur Aufrechterhaltung der Aktualität von Daten
	Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
	Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellung der Ist-Zustände von Prozessen

[249] Hierzu: 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 – Erprobungsfassung vom 25./26. April 2018, S. 22 ff.

	Regelmäßige Überprüfung der Wirksamkeit der ergriffenen technischen Maßnahmen und regelmäßige Überprüfung, ob die Maßnahmen dem Stand der Technik entsprechen **(Datenschutzmanagementsystem (DSMS))**
	Transportverschlüsselung bei Kommunikation mit anderen Diensten
	Möglichst lokale Datenspeicherung & Sicherung nach aktuellem Stand der Technik
Vertraulichkeit	Festlegung eines Rechte- und Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements
	Implementierung eines sicheren Authentisierungsverfahrens
	Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen
	Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle
	spezifizierte, für das Verarbeitungstätigkeit ausgestattete Umgebungen
	Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.)
	Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen
	Schutz vor äußeren Einflüssen (Spionage, Hacking)
	Vorbereitung und Sensibilisierung von Mitarbeitern für verschiedene **Situationen (Datenpannen, Ausübung und Geltendmachung von Betroffenenrechten)**
	Authentifizierung mittels sicherer/starker Passwörter oder Zwei-Faktor-Authentifizierung
	Keine Passwort-Speicherung im Klartext, ggf. Zugangstoken
	Eindeutige Kennungen für die App bestenfalls über zufallsgenerierte Token
Nichtverkettung	Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
	Programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten
	Regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
	Trennung nach Organisations-/Abteilungsgrenzen
	Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und eines sicheren Authentisierungsverfahrens

	Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle
	Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, Verarbeitung pseudonymer bzw. anonymisierter Daten
	Geregelte Zweckänderungsverfahren
Transparenz	Umfassende Dokumentation von allen Verarbeitungstätigkeiten
	Sicherstellung der Informiertheit von Nutzern betreffend aller Funktionalitäten der App, auch hinsichtlich Push-Benachrichtigungen und/oder Kameranutzung/Aktivierung von Ortungsdiensten und insbesondere auch hinsichtlich Weitervermittlungen
	Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verarbeitungstätigkeiten
	Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
	Dokumentation von Einwilligungen und Widersprüchen
	Protokollierung von Zugriffen und Änderungen
	Nachweis der Quellen von Daten (Authentizität)
	Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
	Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept
Intervenierbarkeit	Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
	Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
	Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verarbeitungstätigkeiten sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
	Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
	Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen,
	Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte
	Einrichtung eines Single Point of Contact (SPoC) für Betroffene
	Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

Die aufgezeigten Maßnahmen sind generisch und dienen als Überblick über klassische Schutzmaßnahmen für die Gewährleistungsziele. Die Maßnahmen sind jedoch im Einzelfall auf ihre Anwendbarkeit und ihre Sinnhaftigkeit zu prüfen. Angemessene TOMs können je nach Anwendungsfall variieren.

9.4.2 TDDDG

Das TDDDG fordert ebenfalls verschiedenen technische und organisatorische Schutzmaßnahmen, § 19 TDDDG.

Möglichkeit der jederzeitigen Beendigung der Nutzung des Dienstes
Inanspruchnahme des Dienstes nur geschützt gegen Kenntnisnahme Dritter
Nutzung des Dienstes ist pseudonym bzw. anonym zu ermöglichen
Weitervermittlung zu einem anderen Anbieter von digitalen Diensten ist dem Nutzer anzuzeigen
Sicherzustellen, dass kein unerlaubter Zugriff auf die für die Angebote ihrer digitalen Dienste genutzten technischen Einrichtungen möglich ist
Geschäftsmäßig angebotene digitale Dienste sind gegen Störungen zu sichern

9.5 Anwendung auf WearPrivate

Welche TOMs zum Einsatz kommen, richtet sich danach, welche Maßnahmen im Einzelfall sinnvoll und notwendig erscheinen. Hierfür nimmt der Verantwortliche grundsätzlich eine Prüfung vor, bei der das Risiko für die Rechte und Freiheiten der betroffenen Personen sowie deren Eintrittswahrscheinlichkeit einerseits und die Geeignetheit und Zumutbarkeit der Maßnahme für den Verantwortlichen andererseits gegeneinander abgewogen werden. Auf Seiten des Verantwortlichen werden hierbei die Implementierungskosten, der Stand der Technik sowie die Art, Umfang, Umstände und Zwecke der Verarbeitung – auf Seiten der betroffenen Personen streiten die Risiken der Verarbeitung und deren Schwere und Eintrittswahrscheinlichkeit.[250] Im Rahmen einer Verhältnismäßigkeitsprüfung sind diese Faktoren gegeneinander abzuwägen und in einen angemessenen Ausgleich zu bringen.[251] Hinsichtlich

[250] PILTZ in: Gola/Heckmann, Art. 32 DSGVO Rn. 13.

[251] PILTZ in: Gola/Heckmann, Art. 32 DSGVO Rn. 13.

des „Stands der Technik“ gilt, dass dieser nicht absolut zu befolgen ist, sondern vor dem Hintergrund der Implementierungskosten und den Umständen der Verarbeitung als Leitlinie heranzuziehen ist.[252]

Die DSGVO verfolgt auch bei den TOMs einen risikobasierten Ansatz.[253] Im WearPrivate-Szenario sind die Risiken für die betroffenen Personen aus verschiedenen Gründen als erhöht anzusehen. Zunächst ist darauf hinzuweisen, dass besonders sensible Daten, Gesundheitsdaten, der betroffenen Personen verarbeitet werden. Darüber hinaus erfolgt die Verarbeitung auch in einem besonderen Umfeld, dem Arbeitskontext. Beide Punkte tragen dazu bei, dass eine Offenlegung, die Vernichtung oder der Verlust der Daten für die betroffenen Personen besonders problematisch wäre. Die gesammelten Daten zur Herzratenvariabilität beinhalten ggf. Informationen zu Krankheiten oder sonstigen Auffälligkeiten, die für die betroffene Person besonders geheimhaltungsbedürftig sind. Ferner können Beschleunigungsdaten und Herzratenvariabilität auch eine Aussage über die Belastung der betroffenen Person geben, wodurch Informationen über die Arbeitsleistung der betroffenen Person gesammelt werden können. In beiden Fällen kann die ungewollte Offenlegung problematische Folgen mit sich bringen.

Neben der grundsätzlichen Schwere des Risikos ist auch die Eintrittswahrscheinlichkeit des Risikos zu prüfen. Im WearPrivate-Szenario sind mehrere Parteien an der Auswertung der gesammelten Daten beteiligt. So gibt es einen unabhängig handelnden App-Anbieter, der zumindest Auftragsverarbeiter sein kann, einen Analyseservice, der als Verantwortlicher anzusehen ist, mit ggf. einem weiteren Auftragsverarbeiter sowie den Arbeitgeber, der ebenfalls als Verantwortlicher handelt. Damit besteht eine längere Kette an Beteiligten mit zumindest theoretischem Zugang zu den personenbezogenen Daten der betroffenen Personen. Damit besteht eine Reihe an Angriffszielen bzw. möglichen Schwachpunkten, die zu einer ungewollten Offenlegung oder eines sonstigen Verlusts führen können. Hier gilt es allerdings zu beachten, dass in der derzeitigen Situation die App den am wenigsten gefährlichen Angriffspunkt bietet, da die Daten rein lokal gesammelt und auf dem Smartphone gespeichert werden sollen, weshalb die Daten zu keinem Zeitpunkt über die Server des Apphersstellers laufen werden. Dennoch sind Maßnahmen zur Sicherheit der App zu ergreifen. Zu diesen Maßnahmen finden sich ausführliche Ausführungen in D 3.1 unter Punkt 2.

---

[252] PILTZ in: Gola/Heckmann, Art. 32 DSGVO Rn. 14.

[253] PILTZ in: Gola/Heckmann, Art. 32 DSGVO Rn. 22.

9.5.1 Analyseservice

Anders verhält es sich mit dem Analyseservice. Der Analyseservice verarbeitet die gesammelten Daten der Mitarbeiter in der Cloud, ggf. mithilfe eines Auftragsverarbeiters. Aufgrund des direkten Kontakts mit den Daten sind weitere TOMs zu ergreifen. Ausführungen hierzu finden sich ebenfalls in D 3.1 unter Punkt 3. Ähnliches gilt auch für den vom Analyseservice in Anspruch genommenen Auftragsverarbeiter. Auch dieser muss die Sicherheit der Daten sicherstellen. Ferner muss der Analyseservice als Verantwortlicher auch prüfen, dass der Auftragsverarbeiter angemessene Maßnahmen ergreift., Art. 28 Abs. 1 DSGVO. Hierzu gehören unter anderem folgende Maßnahmen:

- die verschlüsselte Übertragung und Speicherung der Daten,
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Festlegung der Aufgaben und Verantwortlichkeiten der Mitarbeitenden
- Einrichtung von Sperr- und Löschfristen
- Dokumentation der Verarbeitungstätigkeiten sowie Tätigwerden lediglich auf und im Rahmen von dokumentierten Weisungen des Verantwortlichen
- Protokolle des Zugriffs auf die Daten
- Schutz vor äußeren Einflüssen
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Nutzung eines DSMS
- Vorbereitung und Sensibilisierung von Mitarbeitern für verschiedene Situationen
- Trennung nach Organisations-/Abteilungsgrenzen

Der Analyseservice kann zur weiteren Datenverarbeitung einen Cloudservice einschalten. Der Cloudservice wird üblicherweise als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO tätig. Der Verantwortliche hat nach Art. 28 Abs. 1 DSGVO sicherzustellen, dass nur mit Auftragsverarbeitern zusammengearbeitet wird, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Im Vorhinein ist mithin zu überprüfen, ob der Cloudservice diese Anforderungen einhält. Relevant könnte hier beispielsweise sein, ob Drittlandsübermittlungen vorgenommen werden.

9.5.2 Arbeitgeber

Den Arbeitgeber könnte ebenso die Verpflichtung treffen, Maßnahmen zu ergreifen, um die Datensicherheit sicherzustellen. Geplant ist, dass der Arbeitgeber nur die vom Analyseservice bereits verarbeiteten Daten in Form eines anonymisierten Gruppenberichts erhält. Mithin soll er keinen Zugriff auf erhobene Rohdaten haben, die keiner Anonymisierung unterzogen wurden. Die bloß anonymisierten Gruppenberichte fallen mangels personenbezogener Daten indes nicht in den Anwendungsbereich der DSGVO. Hinsichtlich der Gruppenberichte sind mithin auch die Regelungen hinsichtlich der TOM aus der DSGVO nicht einschlägig.

Allerdings sollte der Arbeitgeber bereits im Vorhinein Maßnahmen ergreifen, die dem Schutz der Daten seiner Arbeitnehmer dienen. Hierzu gehört auch, dass (soweit der Arbeitgeber die genutzten Geräte (wie Wearable und/oder Smartphone) ausgibt) Geräte genutzt werden, die die in Art. 25 DSGVO normierten Grundsätze Privacy by Design (Datenschutz durch Technikgestaltung) und Privacy by Default (Datenschutzfreundliche Voreinstellungen) umsetzen. Hier gilt, dass den Arbeitgeber nur eine Überprüfungspflicht im Rahmen des Möglichen treffen kann und er regelmäßig keinen Einblick in die internen Maßnahmen von Geräteherstellern haben dürfte. Trotzdem sind offenkundig nicht datenschutzkonforme Geräte nicht zu verwenden.

Ferner kommen insbesondere auch organisatorische Maßnahmen in Betracht. So wäre es sinnvoll, wenn der Arbeitgeber seine Arbeitnehmer vor der Datenverarbeitung ausführlich und in einem interaktiven Format informiert und sensibilisiert. Hierzu könnten Informationsveranstaltungen hilfreich sein, in denen transparent über alle Abläufe, Funktionen und die Kette der Verarbeitung informiert wird. Hierzu gehören insbesondere auch Informationen zu Push-Benachrichtigungen und anderen Diensten, auf die die verwendete App zugreift.

Da der Arbeitgeber mit dem Analysedienst sowie dem App-Entwickler weitere Akteure in die Verarbeitung zu seinen Zwecken miteinbezieht, hat er sicherzustellen, dass nur vertrauenswürdige und datenschutzkonform arbeitende Unternehmen eingeschaltet werden. Für den Einsatz eines Auftragsverarbeiters ergibt sich diese Verpflichtung direkt aus Art. 28 Abs. 1 DSGVO. Auch vor der Zusammenarbeit mit einem weiteren Verantwortlichen nach Art. 26 DSGVO sollte abgeklärt werden, dass dieser Sorge dafür trägt, dass die Pflichten der DSGVO eingehalten werden.

10 Datenverarbeitung zu wissenschaftlichen Forschungszwecken

Die Datenverarbeitung, die im Rahmen des Projekts stattfinden wird, muss ebenfalls im Einklang mit DSGVO, BDSG und dem saarländischen Datenschutzgesetz (SDSG) geschehen. Im Rahmen von

Nutzerstudien und dergleichen werden Daten erhoben und verarbeitet, und hierfür bedarf es einer entsprechenden Rechtsgrundlage.

Eine diesbezügliche Regelung findet sich in Art. 89 DSGVO. Dieser 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. Explizit wird hier auch die Pseudonymisierung angesprochen. Bei der Pseudonymisierung handelt es sich um eine Veränderung der Daten in der Form, dass ohne weitere Informationen keine Identifizierung der Person mehr möglich ist, auf die sich die personenbezogenen Daten beziehen. Aus Absatz 2 ergibt sich eine Sonderregelung zu Betroffenenrechten: Diese können eingeschränkt werden, soweit es für die Zwecke der wissenschaftlichen Forschung erforderlich ist.

Mit § 27 BDSG hat der deutsche Gesetzgeber eine eigene Regelung geschaffen, die die Verarbeitung von Daten zu Forschungszwecken genauer regelt. Gemäß § 27 Abs. 1 BDSG ist die Verarbeitung besonders sensibler Daten gemäß Art. 9 DSGVO dann zulässig, wenn sie erforderlich ist und die Interessen der Verantwortlichen die Interessen der Betroffenen **wesentlich** überwiegen.[254] Die Regelung des § 27 BDSG ist in gewisser Weise Ausfluss der Forschungs- und Wissenschaftsfreiheit, die in Deutschland gemäß Art. 5 Abs. 3 GG grundrechtlich gewährleistet ist. Um diesen Freiheiten gerecht zu werden, gibt es dementsprechend eine Privilegierung für wissenschaftliche Zwecke, da diese zumindest mittelbar der Gesellschaft dienen.[255] Zur Definition von „wissenschaftlichen Zwecken“ sind die Erwägungsründe 159 sowie 160 zur DSGVO heranzuziehen. Erforderlich ist nach Erwägungsrund 159 S. 2 eine weite Auslegung dieses Begriffs, wobei die „Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung“ miteinzubeziehen sind.

Die Frage, ob wissenschaftliche und/oder Forschungszwecke vorliegen, kann in persönlicher und in sachlicher Hinsicht beantwortet werden. Erfasst sind sowohl die öffentlich finanzierte wie auch die privat finanzierte Forschung.[256] Hierzu gehören auch Markt- und Meinungsforschung.[257] In sachlicher Hinsicht kommt es auf ein entscheidendes Merkmal an: die Datenverarbeitung muss einer Tätigkeit

---

[254] Im Saarland ist zudem § 23 Abs. 1 zu beachten.

[255] PAULY in: Paal/Pauly BDSG, Art. 27 Rn. 1; SCHANTZ in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 1347; Erwägungsrund 113 S. 4 zur DSGVO.

[256] PAULY in: Paal/Pauly BDSG, Art. 27 Rn. 4.

[257] KROHM in: Gola/Heckmann BDSG, § 27 Rn. 16; HORNUNG/HOFMANN, ZD-Beilage 2017, 1 (4).

dienen, die das Ziel hat, neue Erkenntnisse in methodischer und nachprüfbarer Art zu gewinnen.[258] Das Projekt WearPrivate entspricht diesen Voraussetzungen. So handelt es sich hier um ein öffentlich finanziertes Projekt, welches dazu dient, in einem noch wenig wissenschaftlich erarbeiteten Bereich neue Erkenntnisse zu gewinnen. Die Analyse des datenschutzfreundlichen Einsatzes von Wearables gerade im Beschäftigtenkontext erfordert ein interdisziplinäres Vorgehen, um die vorhandenen Interessen in Einklang zu bringen. So müssen die rechtlichen Anforderungen mit dem technisch Machbaren in Einklang gebracht werden.

Im Bereich der rechtlichen Analyse treffen mehrere Einzelbereiche aufeinander (z. B. Beschäftigtendatenschutz; Verarbeitung von Gesundheitsdaten, gemeinsame Verantwortlichkeit), die zwar zuvor schon einzeln betrachtet wurden, zu deren Überschneidungen sich jedoch kaum Literatur findet.

Dass das Projekt mithin wissenschaftlichen Zwecken dient, kann somit angenommen werden. Dies allein reicht jedoch nicht aus, um die Datenverarbeitung im Rahmen des Projekts zu rechtfertigen. Vielmehr muss die jeweilige Verarbeitung auch erforderlich sein. Erforderlichkeit liegt immer dann vor, wenn kein gleich geeignetes weniger belastendes Mittel verfügbar ist.[259] Die Erforderlichkeit ist insbesondere dann zu verneinen, wenn die Datenverarbeitung mit anonymen Daten möglich ist.[260] Dies folgt schon daraus, dass Art. 89 DSGVO eine angebrachte Anonymisierung der verarbeiteten Daten verlangt. Daher ist auch im Rahmen von WearPrivate eine sinnvolle Anonymisierung der Daten vorzunehmen. Dies lässt sich auch technisch umsetzen, soweit die Daten dann immer noch helfen, die Ziele von WearPrivate umzusetzen. Dies muss auch im Einzelfall betrachtet werden.

Des Weiteren müssen die Interessen des datenschutzrechtlich Verantwortlichen (also desjenigen, der auch die Nutzerstudien durchführt) **erheblich** überwiegen. Es liegen hier also erhöhte Anforderungen vor, um die Verarbeitung von besonders sensiblen personenbezogenen Daten zu Forschungs- und Wissenschaftszwecken zu rechtfertigen.[261] Daher ist eine Verhältnismäßigkeitsprüfung vorzunehmen. Jedoch gibt es gewisse Anhaltspunkte, die bei der Abwägung relevant sind. So ist beispielsweise

---

[258] KROHM in: Gola/Heckmann BDSG, § 27 Rn. 14; HORNUNG/HOFMANN, ZD-Beilage 2017, 1 (4); JARASS in: Jarass GrCh, Art. 13 Rn. 8 mwN.

[259] KROHM in: Gola/Heckmann BDSG, § 27 Rn. 22; SCHLÖSSER-ROST/KOCH in: BeckOK DatenschutzR, BDSG § 27 Rn. 30; BUCHNER/TINNEFELD in: Kühling/Buchner, BDSG § 27 Rn. 10a.

[260] GOLLA in: Specht/Mantz, DatenschutzR-Hdb, § 23 Rn. 29.

[261] BUCHNER/TINNEFELD in: Kühling/Buchner, BDSG § 27 Rn. 11.

entscheidend, dass die Forschung wissenschaftlichen Anforderungen genügt.[262] Ein mit Vorsicht zu betrachtendes Kriterium ist der Nutzen der Forschung für die Gesellschaft und Allgemeinheit, da dieser im Vorhinein nur schwer vorausgesagt werden kann.[263] Häufig ist nicht von Beginn an klar, in welche Richtung ein Projekt geht.

Die Interessen der Forschenden können dann überwiegen, wenn das Forschungsprojekt einen Beitrag für die Gesundheit und soziale Sicherheit der Bevölkerung bietet.[264]

10.1 Anwendung auf WearPrivate

An diese Leitlinie kann für das Projekt WearPrivate angeknüpft werden. So ist das Ziel des Projekts die Erhöhung der Arbeitssicherheit sowie eine Verbesserung der Gesundheitsvorsorge. Gerade in den betrachteten Anwendungsfällen zeigen sich die Vorteile, die sich durch das Forschungsvorhaben realisieren lassen. So können beim Wearable-Einsatz bei LKW-Fahrern Unfälle verhindert werden. Zudem kann beim Technologieeinsatz bei Personen, die besonders gefährliche Tätigkeiten ausüben, die Sicherheit am Arbeitsplatz erhöht werden.

Es zeigt sich mithin klar, dass das Forschungsprojekt WearPrivate dazu dient, den Gesundheitsschutz in der Bevölkerung zu verbessern. Zwar sind auch die Interessen der Personen miteinzubeziehen, deren Daten im Rahmen des Forschungsprojekts verarbeitet werden. Vor dem Hintergrund der Ziele des Projekts wiegen diese jedoch weniger schwer.

11 ePrivacy-Aspekte: Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz

11.1 Anwendbarkeit des TDDDG

Das TDDDG adressiert nicht nur den Datenschutz, sondern auch den Schutz der Privatsphäre von Endeinrichtungen und den Schutz des Fernmeldegeheimnisses.[265] Gerade im Bereich der App-Entwicklung muss daher das TDDDG mitbetrachtet werden.

---

[262] BUCHNER/TINNEFELD in: Kühling/Buchner, BDSG § 27 Rn. 12.

[263] GOLLA in: Specht/Mantz, DatenschutzR-Hdb, § 23 Rn. 30.

[264] BUCHNER/TINNEFELD in: Kühling/Buchner, BDSG § 27 Rn. 12.

[265] ECKHARDT/MÜHLENBECK/SCHWARTMANN in: Schwartmann/Jaspers/Eckhardt, TTDSG, § 1 Rn. 1.

Das TDDDG enthält laut § 1 Nr. 2 TDDDG verschiedene Regelungen zum Schutz personenbezogener Daten bei der Nutzung von digitalen Diensten; ferner werden auch die von Anbieter von digitalen Diensten zu beachtenden technischen sowie organisatorischen Vorkehrungen geregelt (§ 1 Nr. 5 TDDDG). Ein besonderes Thema ist des Weiteren auch der Schutz des Fernmeldegeheimnisses.

11.1.1 Anbieter von digitalen Diensten

Das TDDDG enthält in § 2 TDDDG verschiedene Begriffsbestimmungen. Im Kontext von WearPrivate von besonderer Bedeutung ist der Begriff des „Anbieter von digitalen Diensten". Ein Anbieter von digitalen Diensten ist gemäß § 2 Abs. 2 Nr. 1 TDDDG „jede natürliche oder juristische Person, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt". Der Begriff ist sehr weit gefasst.[266] Hiervon erfasst werden unter anderem auch Apps.[267]

11.1.2 Pflichten des Anbieters von digitalen Diensten

Der Datenschutz bei digitalen Diensten, Endeinrichtungen ist in den §§ 19 - 26 TDDDG geregelt.

11.1.2.1 § 19 TDDDG

§ 19 TDDDG enthält technische und organisatorische Vorkehrungen, die die Anbieter von digitalen Diensten zu beachten haben. § 19 TDDDG dient dazu, technische Vorkehrungen im Bereich des Datenschutzes bei digitalen Diensten zu regulieren.[268] Teilweise wird § 19 TDDDG auch als „bereichsspezifische Ausgestaltung der Art. 24, 32 DSGVO" ausgelegt.[269]

Da der Begriff der digitalen Dienste sehr weit ausgelegt wird, fällt eine ganze Reihe von natürlichen und juristischen Personen unter § 19 TDDDG. Da aber nicht bei allen dieselben Pflichten sinnvoll sind, bedarf es einer Einordnung hinsichtlich der Verantwortlichkeit des jeweiligen Anbieters von digitalen Diensten. So ist beispielsweise danach zu unterscheiden, ob der Anbieter von digitalen Diensten Soft- und/oder Hardware zur Nutzung anbietet und worüber er die rechtliche und faktische Verfügungsgewalt innehat.[270] In diesem Zusammenhang ist jeweils der „Stand der Technik" zu beachten. An dieser Stelle zeigen sich die Parallelen zu den Art. 24, 32 DSGVO.

---

[266] ETTIG in: Taeger/Gabel, § 2 TTDSG, Rn. 11.

[267] ETTIG in: Taeger/Gabel, § 2 TTDSG, Rn. 12; LOHSE in: Weber Rechtswörterbuch, Stichwort Telemedien.

[268] MOOS in: Taeger/Gabel, § 19 TTDSG, Rn. 2; RIECHERT in: Riechert/Wilmer TTDSG, § 19 Rn. 7.

[269] MOOS in: Taeger/Gabel, § 19 TTDSG, Rn. 3.

[270] ECKHARDT/LEPPERHOFF in: Schwartmann/Jaspers/Eckhardt, § 19 TTDSG, Rn. 78 ff.

Konkret sind folgende Maßnahmen in § 19 TDDDG geregelt:

- Jederzeitige Beendigung und geschützte Inanspruchnahme des Dienstes (§ 19 Abs. 1 Nr. 1 und Nr. 2 TDDDG)

Die jederzeitige Beendigung umfasst auch das Verbot einer Smartphone-App, die keine Möglichkeit zur Schließung anbietet bzw. auch manuell abgebrochene Internetverbindungen wieder automatisch aufbaut.[271] Die geschützte Inanspruchnahme des Dienstes kann durch die Vergabe von Passwörtern oder auch durch die Nutzung von Verschlüsselungsverfahren umgesetzt werden.[272]

- Anonyme und pseudonyme Nutzung (§ 19 Abs. 2 TDDDG)

Umstritten ist, ob die genannte Vorschrift auch im Anbieter-Nutzer-Verhältnis gilt; ob der Nutzer eines digitalen Dienstes dieses auch gegenüber dem Anbieter anonym nutzen kann.[273] Jedenfalls ist den Nutzern von digitalen Diensten, soweit es die technische Ausgestaltung des digitalen Dienstes zulässt, die pseudonyme Nutzung des digitalen Dienstes einzuräumen.[274] Über die Möglichkeit der anonymen Nutzung sind die Nutzer zu informieren.[275]

- Anzeige der Weitervermittlung (§ 19 Abs. 3 TDDDG)

Weitervermittlungen sind anzuzeigen. Typisches Anwendungsszenario von § 19 Abs. 3 TDDDG sind Websites, die Hyperlinks enthalten und damit auf andere Webseiten weitervermitteln.[276] Ferner sind auch die Weitervermittlung an weitere Anbieter von digitalen Diensten aufzuzeigen. Sinnvoll ist es, diese Information ebenso wie du zur pseudo- und anonymen Nutzung in der Datenschutzerklärung zu implementieren.

- Technische und organisatorische Vorkehrungen (§ 19 Abs. 4 TDDDG)
    - kein unerlaubter Zugriff auf die für ihr Angebot digitaler Dienste genutzten technischen Einrichtungen möglich und

---

[271] RIECHERT in: Riechert/Wilmer TTDSG, § 19 Rn. 7.

[272] RIECHERT in: Riechert/Wilmer TTDSG, § 19 Rn. 13.

[273] RIECHERT in: Riechert/Wilmer TTDSG, § 19 Rn. 15; hier ist v.a. die Diskussion um die *Klarnamenpflicht* relevant.

[274] RIECHERT in: Riechert/Wilmer TTDSG, § 19 Rn. 20.

[275] MOOS in: Taeger/Gabel, § 19 TTDSG, Rn. 22, 23.

[276] MOOS in: Taeger/Gabel, § 19 TTDSG, Rn. 25, 26.

- diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

11.1.2.2 Bestandsdaten

Bestandsdaten sind nach § 2 Abs. 2 Nr. 2 TDDDG „die personenbezogenen Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter von digitalen Diensten und dem Nutzer über die Nutzung von digitalen Diensten erforderlich ist“.

Die §§ 21 und 22 TDDDG treffen nähere Regelungen zum Umgang mit Bestandsdaten. Hierin wird darauf Bezug genommen wie mit einem Auskunftsverlangen von den in § 22 Abs. 3 TDDDG genannten Stellen (Bspw. Bundeskriminalamt, das Zollkriminalamt, der Verfassungsschutz) umzugehen ist.

11.1.2.3 Nutzungsdaten

Auch der Begriff der Nutzungsdaten werden in § 2 Abs. 2 TDDDG definiert. Nutzungsdaten sind nach § 2 Abs. 2 Nr. 3 TDDDG „die personenbezogenen Daten eines Nutzers von digitalen Diensten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von digitalen Diensten zu ermöglichen und abzurechnen“; dazu gehören insbesondere „Merkmale zur Identifikation des Nutzers (Nr. 1), Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung (Nr. 2) und Angaben über die vom Nutzer in Anspruch genommenen digitalen Dienste (Nr. 3).“

Auch bezüglich der Nutzungsdaten wird im TDDDG das Auskunftsverfahren (§ 24 TDDDG) bezüglich Nutzungsdaten geregelt. Auch hier wird geregelt, unter welchen Umständen bestimmten Stellen (Zollkriminalamt, Bundeskriminalamt, Verfassungsschutz) Auskunft über Nutzungsdaten gegeben werden können.

11.1.2.4 Schutz der Privatsphäre bei Endeinrichtungen

Die meist umstrittenen Vorschriften des TDDDG finden sich in den §§ 25, 26 TDDDG. In diesen Vorschriften wird der Schutz der Privatsphäre in Endeinrichtungen adressiert.

Unter einer Endeinrichtung wird nach § 2 Abs. 2 Nr. 6 TDDDG „jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet.“ Endeinrichtungen sind auch Smartphones und sonstige

Geräte aus dem Internet der Dinge.[277] Unter dem „Endnutzer“ ist ein Nutzer, der weder öffentliche Telekommunikationsnetze betreibt noch öffentlich zugängliche Telekommunikationsdienste erbringt, zu verstehen, § 3 Nr. 13 TKG.

Die Regelungen zum Schutz der Privatsphäre von Endeinrichtungen geht auf die ePrivacy-Richtlinie[278], genauer auf Art. 5 Abs. 3 ePrivacy-RL, zurück. Diese Regelung blieb auch mehr als 10 Jahre nach der letzten Novelle der ePrivacy-Richtlinie in Deutschland nicht umgesetzt[279]. Erst mit dem im Dezember 2021 in Kraft getretenen TTDSG und dem damit eingeführten § 25 TTDSG (heute § 25 TDDDG) setzte man schließlich die Regelungen der ePrivacy-Richtlinie um.[280]

In § 25 Abs. 1 TDDDG wurden die in der „Planet49“-Entscheidung[281] des EuGHs ausformulierten Anforderungen an eine Einwilligung in Cookies und ähnliche Technologien umgesetzt. Die Voraussetzungen für eine wirksame Einwilligung in diesem Sinne entsprechen denen der DSGVO. Ausnahmen von der Einwilligungspflicht finden sich nur in § 25 Abs. 2 TDDDG. Einer Einwilligung bedarf des demnach nicht

- „wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder
- wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann“

---

[277] ETTIG in: Taeger/Gabel, § 25 TTDSG Rn. 51.

[278] RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

[279] Auch, wenn man fälschlicherweise über einen langen Zeitraum die Umsetzung in den inzwischen außer Kraft getretenen § 15 Abs. 3 TMG reingelesen wurde.

[280] RIECHERT in: Riechert/Wilmer TTDSG, § 25 Rn. 2.

[281] EuGH, EuZW 2019, 916.

11.1.2.5 Anwendung auf WearPrivate

Als App-Hersteller ist Neusta als Anbieter von digitalen Diensten zu charakterisieren. Mit dieser Einordnung geht auch die Anwendbarkeit des TDDDG einher. Die oben beschrieben Vorschriften gilt es daher zu beachten.

11.1.2.5.1 Technische und organisatorische Vorkehrungen

Neusta hat als Anbieter digitaler Dienste die in § 19 TDDDG geregelten technischen und organisatorischen Vorkehrungen zu treffen. Erforderlich ist mithin, dass eine jederzeitige Schließung der App möglich ist und auch manuell die aufgebauten Verbindungen unterbrochen werden können, ohne dass es zu einem automatischen Wiederaufbau kommt. Die Weitervermittlung der Daten an den Analysedienstleister ist dem Nutzer ebenso anzuzeigen.

11.1.2.5.2 Bestandsdaten und Nutzungsdaten

Werden Nutzungs- und/oder Bestandsdaten erhoben und verarbeitet, sind die Vorgaben des TDDDG einzuhalten.

11.1.2.5.3 Schutz von Endeinrichtungen

Als Endeinrichtung lässt sich das Smartphone charakterisieren, auf dem die App installiert ist. Endnutzer ist die Person, die das Smartphone/die App bedient und nutzt. Der Schutz des Smartphones des Arbeitnehmers ist daher zu gewährleisten. Dies bringt unter anderem mit sich, dass der Neusta nur dann Cookies oder Trackingmechanismen im Sinne des § 25 TDDDG nutzen darf, wenn eine ausdrückliche Einwilligung des Endgerätenutzers vorliegt, die den Anforderungen der DSGVO entspricht.

Eine Ausnahme ist nur dann anzunehmen, wenn es sich um für die Erbringung der Leistung unbedingt erforderliche Technologien handelt, § 25 Abs. 2 Nr. 2 TDDDG.

12 Auswirkungen des Data Act und des EHDS

Wie unter 3.1.3 und 3.1.4 erklärt sind neben den datenschutzrechtlichen Vorgaben der DSGVO und der mitgliedstaatlichen Regelungen auch der Data Act und der zum derzeitigen Zeitpunkt[282] noch nicht in Kraft getretenen European Data Health Space.

[282] Stand: 26.04.2024.

12.1 Data Act

Der Anwendungsbereich des Data Act ist, wie unter 3.1.3 erklärt, eröffnet. Insbesondere ist der Anwendungsbereich des Data Acts nicht auf personenbezogene Daten beschränkt, sodass die Regelungen auch für anonymisierte Daten gelten.

12.2 EHDS

Neben dem Data Act wird auch der EHDS anwendbar sein (siehe hierzu Kapitel 3.1.4). Aus den geplanten Regelungen des EHDS können Pflichten für die Akteure in WearPrivate erwachsen. In Art. 3 Abs. 1 EHDS erhalten natürliche Personen unter anderem das Recht, auf ihre personenbezogenen elektronischen Gesundheitsdaten die im Rahmen der Primärnutzung elektronischer Gesundheitsdaten verarbeitet werden, sofort, kostenlos und in einem leicht lesbaren, gängigen und zugänglichen Format zuzugreifen. Ferner kann auch unter bestimmten Umständen eine elektronische Kopie, Art. 3 Abs. 2 EHDS, oder auch die Übermittlung von elektronischen Gesundheitsdaten an einen anderen Datenempfänger verlangt werden, bspw. in Art. 3 Abs. 8 EHDS.

12.2.1 Zugangsanspruch nach dem Data Act

Hinsichtlich solcher Daten, die durch ein IoT-Gerät generiert werden, gilt es zukünftig auch den erweiterten Zugangsanspruch aus Art. 4 DA zu beachten. Aus Art. 4 Abs. 1 DA folgt, dass der Dateninhaber dem Betroffenen bzw. Nutzer (Art. 2 Nr. 12 DA) den Zugang zu den Daten, die durch das IoT-Gerät generiert werden einzuräumen hat. Zu beachten ist, dass im DA nicht der Verantwortliche, sondern der Dateninhaber adressiert wird. Der Begriff des Dateninhabers ist in Art. 2 Nr. 13 DA definiert: Demnach ist Dateninhaber eine natürliche oder juristische Person, die nach dieser Verordnung, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten – zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat. Durch die sehr weitreichende Definition des Begriffs „Dateninhaber“ sind eine Reihe von Akteuren als solcher zu charakterisieren. Im Projektszenario gehören dazu sowohl App-Entwickler (Neusta) als auch Analysedienstleister (WearHealth), ggf. Cloudanbieter (AWS) und auch regelmäßig der Arbeitgeber. Alle Dateninhaber sind dazu verpflichtet, soweit es möglich ist, den Zugang zu Daten herzustellen, die über die genutzten Wearables generiert werden. Der Anspruch aus dem Data Act ist daher im Rahmen der Betroffenenrechte auch zu beachten.

13 Zusammenfassung der rechtlichen Anforderungen

Die rechtlichen Anforderungen können nicht pauschal erhoben werden. Sie sind im Lichte des jeweiligen Anwendungsfalls zu betrachten und richten sich auch danach, auf welche Rechtsgrundlagen abgestellt werden soll. Die folgende stichpunktartige Auflistung soll dazu dienen, einen Überblick über einzuhaltende rechtliche Anforderungen zu erhalten.

13.1 Anforderungen bei Erhebung einer Einwilligung

- Schriftliche/elektronische Form
- Angemessene Aufklärung der Arbeitnehmer
    - Datenschutzerklärung in einfache Sprache mit leichter Zugänglichkeit
    - Umsetzung: Implementierung in der App und Verlinkung/Erreichbarkeit mit einzelnem Klick
- Anpassung der Einwilligung an die Sensibilität der Daten
    - Umsetzung: Gesonderter Abschnitt in der Datenschutzerklärung mit Hinweis auf die Tatsache, dass Gesundheitsdaten verarbeitet werden und darauf, dass es sich um besonders sensible Daten handelt
- Verhinderung negativer Folgen bei Ablehnung der Einwilligung
    - Umsetzungsmaßnahmen: Bestenfalls Anonymisierung, sodass nicht offensichtlich wird, wer Einwilligung abgelehnt hat
    - Andernfalls: Vertragliche Zusicherung

13.2 Anforderungen bei einer Datenerhebung zum Zwecke des Beschäftigungsverhältnisses

- Erhebung nur von Daten mit Bezug zu Arbeitssicherheit und Gesundheitsschutz
    - Umsetzungsmaßnahmen: Begrenzung der Daten, die von der App an die Cloud geschickt werden
- Vermeidung der Totalüberwachung
    - Umsetzungsmaßnahme: Erfüllung von § 19 Abs. 1 TDDDG: Möglichkeit der jederzeitigen Beendigung der Nutzung des Dienstes (heißt: Möglichkeit, Datenerhebung zu beenden und Möglichkeit, Verbindung zur Cloud zu beenden)
- Maßnahmen der Stärkung und Sicherung von Transparenz und Selbstbestimmung

- Umsetzungsmaßnahmen: Siehe hierzu TOMS zur Sicherung der Transparenz unter Kapitel 9.4.1
    - Umsetzungsmaßnahme: Implementierung der 3 Sicherheitsstufen in der App mit Wahlmöglichkeit des Nutzers

13.3 Anforderungen an den Verantwortlichen

- Rechenschafts- und Nachweispflicht für die Einhaltung der Pflichten der DSGVO
    - Umsetzungsmaßnahme: Dokumentation sämtlicher Verarbeitungstätigkeiten
    - Dokumentation von erteilten Einwilligungen sowie der vorher erfolgten Information der Betroffenen
- Unterstützungspflicht bei der Geltendmachung von Betroffenenrechten
    - Umsetzungsmöglichkeit sind insbesondere Kontaktformulare, die direkt ausgefüllt und weitergeleitet werden
    - Oder: eigene Kategorie in der DE mit allen relevanten Informationen
- Sicherstellung der Sicherheit der Datenverarbeitung
    - Umsetzung: Ergreifung angemessener TOMs, siehe hierzu Kapitel 9

13.4 Anforderungen bei gemeinsamer Verantwortlichkeit

- Joint Controller Vertrag
    - Festlegung von Funktionen und Zuständigkeiten der gemeinsam Verantwortlichen
    - Festlegung des Ansprechpartners für die Geltendmachung von Betroffenenrechten

13.5 Anforderungen bei Datenübermittlungen in Drittländer

- Informationen zum Drittlandstransfer in der DE
- Erlaubnistatbestand nach Art. 45 ff. DSGVO
    - Bestenfalls: Angemessenheitsbeschluss, Art. 45 DSGVO
    - Sonst: Standarddatenschutzklausel, Ergreifung geeigneter Garantien

13.6 Anforderungen an die Datenerhebung zu Forschungszwecken

- Anonymisierung der Daten
- Wesentliches Überwiegen Interessen der Projektpartner

Anlage – Fragenkatalog zur Ermittlung der datenschutzrechtlichen Verantwortlichkeit des Analysedienstes (WearHealth) und des App-Entwicklers (Neusta)

Warum findet die Verarbeitung statt?

Wird die Verarbeitung von WearHealth/Neusta veranlasst?

Profitiert WearHealth/Neusta von der Verarbeitung? (Werden die Daten bspw. zur Verbesserung des eigenen Produkts verwendet?)

Trifft WearHealth/Neusta Entscheidungen über die Zwecke und Mittel der Verarbeitung?

Besteht ein tatsächlicher Einfluss auf die Zwecke der Verarbeitung von WearHealth/Neusta?

Beansprucht WearHealth/Neusta das „Eigentum“ an den verarbeiteten Daten?

Übt WearHealth/Neusta die Kontrolle über die erhobenen Daten aus?

Besteht eine direkte Beziehung zu den betroffenen Personen (z.B. Kunde)?

Besteht das Erfordernis einer sachverständigen Beurteilung durch WearHealth/Neusta (z.B. wegen besonderen Expertenwissens) bei der Datenverarbeitung?

Entscheidet WearHealth/Neusta darüber, wann welche Daten verarbeitet werden?

Trifft WearHealth/Neusta autonome Entscheidungen hinsichtlich der möglichen Einbindung von weiteren Dienstleistern?

Entscheidet WearHealth/Neusta über „wesentliche“ Mittel der Verarbeitung?

„Wesentliche“ Mittel: z.B. welche Daten verarbeitet werden, wie lange die Daten verarbeitet werden und wer Zugang zu den Daten hat.

Nicht wesentliche Mittel: z.B. die Entscheidung über Hardware und Software

Entscheidet WearHealth/Neusta über….

…über die Zwecke, für welche die Daten verarbeitet werden?

Verarbeitet WearHealth/Neusta die Daten für *eigene* Geschäftszwecke?

…wann welche Daten von betroffenen Personen erhoben werden?

…ob und wem die Daten zugänglich gemacht werden?

…wie lange die Daten aufbewahrt werden?

Wird WearHealth/Neusta auf eigene Initiative oder allein auf Weisung tätig?

Wird die Rechtsgrundlage der Verarbeitung von WearHealth/Neusta festgelegt?

Besteht ein wirtschaftliches Eigeninteresse an der Datenverarbeitung von WearHealth/Neusta?

A-1 WearHealth

Warum findet die Verarbeitung statt?

Wir verarbeiten Daten von Wearables, um unseren Service anzubieten, der Industrieunternehmen dabei hilft, die Sicherheit und Gesundheit ihrer Mitarbeiter zu verbessern.

Wird die Verarbeitung von WearHealth/Neusta veranlasst?

Ja

Profitiert WearHealth/Neusta von der Verarbeitung? (Werden die Daten bspw. zur Verbesserung des eigenen Produkts verwendet?)

WearHealth hat das Ziel, von dem datengetriebenen Service, den es seinen Kunden bietet, zu profitieren. Die Daten werden verwendet, um unseren Service ständig zu verbessern.

Trifft WearHealth/Neusta Entscheidungen über die Zwecke und Mittel der Verarbeitung?

Wie die Daten verwaltet, verarbeitet und genutzt werden, wird von WearHealth geplant, aber mit den Beteiligten in den einzelnen Unternehmen abgestimmt, z. B. mit den Datenschutzbeauftragten, den Betriebsräten und der Geschäftsführung

Besteht ein tatsächlicher Einfluss auf die Zwecke der Verarbeitung von WearHealth/Neusta?

Der Use Case, der Nutzen der Lösung und der Datenschutz bestimmen, wie die Daten verarbeitet werden

Beansprucht WearHealth/Neusta das „Eigentum“ an den verarbeiteten Daten?

Die anonymisierten und verarbeiteten Daten werden Teil des Algorithmus, der Eigentum von WearHealth ist.

Übt WearHealth/Neusta die Kontrolle über die erhobenen Daten aus?

Ja

Besteht eine direkte Beziehung zu den betroffenen Personen (z.B. Kunde)?

Ja, allerdings haben wir logische und physische Trennungen unserer Datenbanken je nach Verwendungszweck (z.B. Unternehmen sind bekannt, aber einzelne Benutzer nicht).

Besteht das Erfordernis einer sachverständigen Beurteilung durch WearHealth/Neusta (z.B. wegen besonderen Expertenwissens) bei der Datenverarbeitung?

Ja (Data Scientists, Biomedizintechniker und Arbeitswissenschaftler)

Entscheidet WearHealth/Neusta darüber, wann welche Daten verarbeitet werden?

- Ähnlich wie bei 4

Trifft WearHealth/Neusta autonome Entscheidungen hinsichtlich der möglichen Einbindung von weiteren Dienstleistern?

Nein

Entscheidet WearHealth/Neusta über „wesentliche“ Mittel der Verarbeitung?

Ähnlich wie bei 4

„Wesentliche“ Mittel: z.B. welche Daten verarbeitet werden, wie lange die Daten verarbeitet werden und wer Zugang zu den Daten hat.

Nicht wesentliche Mittel: z.B. die Entscheidung über Hardware und Software

Entscheidet WearHealth/Neusta über….

…über die Zwecke, für welche die Daten verarbeitet werden?

Die Daten werden entsprechend den Bedürfnissen des Kunden und dem definierten Anwendungsfall verarbeitet

Verarbeitet WearHealth/Neusta die Daten für *eigene* Geschäftszwecke?

Die Daten werden entsprechend den Bedürfnissen des Kunden und dem definierten Anwendungsfall verarbeitet

…wann welche Daten von betroffenen Personen erhoben werden?

Die Daten werden entsprechend den Bedürfnissen des Kunden und dem definierten Anwendungsfall erhoben

…ob und wem die Daten zugänglich gemacht werden?

Je nach Anwendungsfall haben wir Zugriffsrechte für Mitglieder unseres Teams definiert, die mit unseren Kunden abgestimmt sind.

…wie lange die Daten aufbewahrt werden?

Es wird gemeinsam mit dem Kunden definiert.

Wird WearHealth/Neusta auf eigene Initiative oder allein auf Weisung tätig?

Abhängig von der Art des Services

Wird die Rechtsgrundlage der Verarbeitung von WearHealth/Neusta festgelegt?

Ja.

Besteht ein wirtschaftliches Eigeninteresse an der Datenverarbeitung von WearHealth/Neusta?

Unser Interesse ist es, unseren Kunden einen zuverlässigen, datengetriebenen Service zu liefern.

A-2 Neusta

Warum findet die Verarbeitung statt?

Zum Auslesen der Daten aus einem Wearable auf das Smartphone und zur Weiterleitung derer an den Verarbeiter WearHealth. Es geht nichts auf irgendwelche neusta-Server.

Wird die Verarbeitung von WearHealth/Neusta veranlasst?

Die App sollte ja nichts tun, was der Nutzer vorher nicht zugelassen hat, von daher lautet die Antwort nein, falls diese Definition paßt.

Wenn es eher so ist, dass neusta ja den Programmcode geschrieben hat, was zu der Verarbeitung führt, dann lautet die Antwort „ja“.

Profitiert WearHealth/Neusta von der Verarbeitung? (Werden die Daten bspw. zur Verbesserung des eigenen Produkts verwendet?)

Nein.

Trifft WearHealth/Neusta Entscheidungen über die Zwecke und Mittel der Verarbeitung?

Nein.

Besteht ein tatsächlicher Einfluss auf die Zwecke der Verarbeitung von WearHealth/Neusta?

Nein.

Beansprucht WearHealth/Neusta das „Eigentum“ an den verarbeiteten Daten?

Nein.

Übt WearHealth/Neusta die Kontrolle über die erhobenen Daten aus?

Auch wieder eine Definitionsfrage. Nach unserer Vorstellung bleiben die Daten nur auf dem Gerät und gehen dann an WearHealth. Also es geht nichts an einen neusta-Server. Von daher würde ich sagen „nein“, außer die Definition möchte, dass die App eine Exportfunktion für die lokalen Daten hat, damit man nicht sagen kann, dass Daten in der App „gefangen“ sind.

Besteht eine direkte Beziehung zu den betroffenen Personen (z.B. Kunde)?

Nein.

Besteht das Erfordernis einer sachverständigen Beurteilung durch WearHealth/Neusta (z.B. wegen besonderen Expertenwissens) bei der Datenverarbeitung?

Instinktiv würde ich sagen „nein“, außer es zählt dazu auch das Wissen um die von WearHealth benötigten Datenformate/Schnittstellen, an die wir das Ganze dann senden sollen.

Entscheidet WearHealth/Neusta darüber, wann welche Daten verarbeitet werden?

Eigentlich auch nicht. Oder zählt dazu, dass der Programmcode unter Aspekten wie der letzten Weiterleitungszeit und der aktuellen Netzverbindung entscheidet, ob ein neuer Upload eines Datenpaketes getätigt werden soll?

Trifft WearHealth/Neusta autonome Entscheidungen hinsichtlich der möglichen Einbindung von weiteren Dienstleistern?

Nein.

Entscheidet WearHealth/Neusta über „wesentliche“ Mittel der Verarbeitung?

Unser Programmcode wird natürlich die Daten des Wearables auf dem Smartphone ggf. selektieren (z.B. Verwerfen der Bewegungsdaten älterer nicht hochgeladener Datenpakete). Je nachdem ob wir Exportfunktion einbauen, kann dies auch beeinflussen, wer auf die Daten zugreifen kann. Sonst denk ich aber eher nicht.

„Wesentliche“ Mittel: z.B. welche Daten verarbeitet werden, wie lange die Daten verarbeitet werden und wer Zugang zu den Daten hat.

Nicht wesentliche Mittel: z.B. die Entscheidung über Hardware und Software

Entscheidet WearHealth/Neusta über….

…über die Zwecke, für welche die Daten verarbeitet werden?

Nein.

Verarbeitet WearHealth/Neusta die Daten für *eigene* Geschäftszwecke?

Nein.

…wann welche Daten von betroffenen Personen erhoben werden?

Der Programmcode wird entscheiden, wann welche Daten aus dem Wearable auf das Smartphone gelesen werden. Und die Abfrage von Stammdaten durchführen.

…ob und wem die Daten zugänglich gemacht werden?

Der Programmcode wird entscheiden, wann die erhobenen Daten an WearHealth gesendet werden.

…wie lange die Daten aufbewahrt werden?

Der Programmcode wird z.B. nach erfolgreicher Übermittlung an WearHealth nicht länger benötigte Bewegungsdaten löschen können. Haben wir noch nicht in den Anforderungen, ob dies gewünscht ist.

Wird WearHealth/Neusta auf eigene Initiative oder allein auf Weisung tätig?

Nur auf Weisung.

Wird die Rechtsgrundlage der Verarbeitung von WearHealth/Neusta festgelegt?

Nein.

Besteht ein wirtschaftliches Eigeninteresse an der Datenverarbeitung von WearHealth/Neusta?

Nein.

Quellenverzeichnis

[1] Arnold, René/ Hillebrand, Annette/ Waldburger, Marting, Personal Data and Privacy – Final Report Wik Consult, Study for ofcom, 26.05.2015, Bad Honnef, abrufbar unter: https://www.ofcom.org.uk/__data/assets/pdf_file/0029/67088/personal_data_and_privacy.pdf

[2] Art.-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, abrufbar unter: https://www.lda.bayern.de/media/wp136_de.pdf

[3] Assion, Simon, TTDSG Telekommunikations-Telemedien-Datenschutz-Gesetz Handkommentar, 1. Auflage Baden-Baden 2022, Zit.: BEARBEITER in: Assion TTDSG, § Rn.

[4] Bitkom e.V., Bundesverband Informationswirtschaft Telekommunikation, BfDI Konsultation – Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK- Branche, 20.03.2020, abrufbar: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Bitkom.pdf;jsessionid=9C398EF915FEC35240940DA347948D38.intranet212?__blob=publicationFile&v=2, zuletzt abgerufen am 30.11.2024

[5] Bomhard, David/Merkle, Marieke, Der Entwurf eines EU Data Acts, RDi 2022, S. 168 - 176

[6] Brink, Stefan/ Wolff, Heinrich Amadeus, Beck`scher Onlinekommentar Datenschutzrecht, 47. Edition, 01.02.2024 München, Zit.: BEARBEITER in: BeckOK DatenschutzR, DSGVO/BDSG, Art./§ Rn.

[7] Bundesbeauftragter für Datenschutz und Informationssicherheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand 29.06.2020, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am 30.11.2024

[8] Bundesbeauftragter für Datenschutz und Informationssicherheit, Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/26TB_15_16.pdf;jsessionid=9B7E9C9B786BAF64133B617E536D3596.intranet241?__blob=publicationFile&v=7, zuletzt abgerufen am 30.11.2024

[9] Calliess, Christian/Ruffert, Matthias, EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 6. Auflage 2022, Zit.: BEARBEITER in: Calliess/Ruffert, Art. AEUV/EUV/GRC Rn.

[10] Competition and Markets Authority, Online platforms and digital advertising, 2019, abrufbar unter: https://assets.publishing.service.gov.uk/media/5ed0f75bd3bf7f4602e98330/Interim_report_---_web.pdf, zuletzt abgerufen am 30.11.2024

[11] Conradie, Niel Henk, The moral opportunities and perils of smart wearables for decisional autonomy, November 2021

[12] Deutsche Telekom AG, Stellungnahme der Deutschen Telekom anlässlich des öffentlichen Konsultationsverfahrens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK- Branche, 23.03.2020, abrufbar: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Deutsche-Telekom.pdf;jsessionid=9C398EF915FEC35240940DA347948D38.intranet212?__blob=publicationFile&v=3, zuletzt abgerufen am 30.11.2024

[13] Ebers, Martin/ Heinze, Christian/ Krügel, Tina/ Steinrötter, Björn, Künstliche Intelligenz und Robotik – Rechtshandbuch, 1. Auflage, München 2020, Zit.: *Bearbeiter* in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, § Rn.

[14] Ehmann, Eugen/ Selmayr, Martin, DS-GVO Kommentar, 3. Auflage, München 2024, Zit.: BEARBEITER in: Ehmann/Selmayr DSGVO, Art. Rn.

[15] Forgó, Nikolaus/ Helfrich, Marcus/Schneider, Jochen, Betrieblicher Datenschutz, Rechtshandbuch, 3. Auflage 2019, München

[16] Geppert, Martin/Schütz, Raimund, Beck`scher TKG Kommentar (Telekommunikationsgesetz, Telekommunikations-Telemedien-Datenschutz-Gesetz), 5. Auflage, München 2023, Zit.: BEARBEITER in: Beck`scher TKG-Kommentar, § Rn.

[17] Gerpott, Thorsten, Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO, MMR 2020, 739 - 744

[18] Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV), Stellungnahme des Gesamtverbandes der Deutschen Versicherungswirtschaft zum Öffentlichen Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Berlin, 23.03.2020, abrufbar: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/GDV.pdf;jsessionid=9C398EF915FEC35240940DA347948D38.intranet212?__blob=publicationFile&v=2, zuletzt abgerufen am 30.11.2024

[19] Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Stellungnahme zur Konsultation des BfDI zum Thema „Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Bonn, 19.03.2020, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellu

ngnahmen/GDD.pdf;jsessionid=9C398EF915FEC35240940DA347948D38.intranet212?__blob=publicationFile&v=2, zuletzt abgerufen am 30.11.2024

[20] Gierschmann, Sibylle/Baumgartner, Ulrich, Telekommunikations-Telemedien-Datenschutz-Gesetz, Kommentar, 1. Auflage, München 2023, Zit.: BEARBEITER in: Gierschmann/Baumgartner TTDSG, § Rn.

[21] Glocker, Felix, Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework, RDi 2023, S. 465 - 471

[22] Gola, Peter/Heckmann, Dirk, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, Kommentar, 3. Auflage, München 2022, Zit.: BEARBEITER in: Gola/Heckmann, DSGVO, Art. Rn.

[23] Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin, Das Recht der Europäischen Union, Band I, 79. Ergänzungslieferung – Stand Mai 2023, Zit.: BEARBEITER in: Grabitz/Hilf/Nettesheim, Art. AEUV/EUV/GRC Rn.

[24] Hamm, Christoph, Beck'sches Rechtsanwalts-Handbuch, 12. Auflage 2022, Zit.: BEARBEITER in: Hamm, Beck'sches Rechtsanwalts-Handbuch, § Rn.

[25] Hansen, Hauke/ Brechtel, Sandra, Zu den Anforderungen an die Einwilligung für Cookies und Werbung, GRUR-Prax 2020, 385

[26] Hornung, Gerrit/ Hofmann, Kai, Die Auswirkungen der europäischen Datenschutzreform auf die Markt- und Meinungsforschung, ZD-Beilage 2017, S. 1 – 16

[27] Hornung, Gerrit/ Wagner, Bernd, Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223 – 228

[28] https://www.apotheken-umschau.de/gesund-bleiben/psyche/herzratenvariabilitaet-stress-messen-gezielt-entspannen-848387.html, zuletzt abgerufen am 30.11.2024

[29] Jarass, Hans, Charta der Grundrechte der Europäischen Union, Kommentar, 4. Auflage, München 2021, Zit.: BEARBEITER in: Jarass GrCh, Art. Rn.

[30] Kollmer, Norbert/Klindt, Thomas/Schucht, Carsten, Arrbeitsschutzgesetz Kommentar, 1. Auflage, München 2021, Zit.: BEARBEITER in: Kollmer/Klindt/Schucht, § Rn.

[31] Kort, Michael, Neuer Beschäftigtendatenschutz und Industrie 4.0, RdA 2018, S. 24 – 33

[32] Kühling, Jürgen/Buchner, Benedikt, Datenschutz-Grundverordnung BDSG – Kommentar, 4. Auflage, München 2024, Zit.: BEARBEITER in: Kühling/Buchner, DSGVO/BDSG, Art./§ Rn.

[33] Kühling, Jürgen/ Klar, Manuel/Sackmann, Florian, Datenschutzrecht, 5. Auflage, Heidelberg 2021

[34] Laue, Philip/ Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 3. Auflage, Baden-Baden 2024, Zit.: BEARBEITER in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § Rn.

[35] Leupold, Andreas/ Wiebe, Andreas/ Glossner, Silke, IT-Recht – Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage 2021, Zit.: BEARBEITER in: Leupold/Wiebe/Glossner, Teil Rn.

[36] Linden, Thomas/Khandelwal, Rishabh/Harkous, Hamza/Fawaz, Kassem, The Privacy Policy Landscape After the GDPR in: Proceedings on Privacy Enhancing Technologies; 2020 (1); S. 47–64

[37] Malorny, Friederike, Auswahlentscheidungen durch künstlich intelligente Systeme, JuS 2022, S. 289 - 296

[38] Müller-Glöge, Rudi/ Preis, Ulrich/ Schmidt, Ingrid, Erfurter Kommentar zum Arbeitsrecht, 21. Auflage, München 2021, Zit.: BEARBEITER in: ErfK BDSG, § Rn.

[39] Paal, Boris/ Pauly, Daniel, Beck`sche Kompakt-Kommentare, Datenschutz-Grundverordnung, 3. Auflage, München 2021, Zit.: BEARBEITER in: Paal/Pauly DSGVO, Art. Rn.

[40] Plath, Kai-Uwe, Kommentar DSGVO/BDSG, 4. Auflage, Köln 2023; Zit.: BEARBEITER IN: Plath DSGVO/BDSG, Gesetz Art./§ Rn.

[41] Radtke, Tristan, Gemeinsame Verantwortlichkeit unter der DSGVO, Baden-Baden 2021

[42] Rauer, Nils/ Ettig, Claudia, Update Cookies – Aktuelle Rechtslage und Entwicklungen, ZD 2021, S. 18 - 24

[43] Riechert, Anne/ Wilmer, Thomas, Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG), 1. Auflage, Berlin 2022, Zit.: BEARBEITER in: Riechert/Wilmer, § Rn.

[44] Roßnagel, Alexander, Datenlöschung und Anonymisierung, ZD 2021, S. 188 – 192

[45] Säcker, Franz Jürgen / Körber, Tobias, TKG – TTDSG, 4. Auflage 2023, Frankfurt am Main, Zit.: BEARBEITER in: Säcker/Körber, § TTDSG/TKG Rn.

[46] Salemi, Simone/Wiedemann, Nils/Steffes Bianca, Data Sharing im Kontext digitaler Selbsvermessung in: Data Sharing – Datenkapitalismus bei Default, Posterproceedings Forum Privatheit 2023, DOI:

[47] Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841 – 1847

[48] Schantz, Peter/ Wolff, Heinrich Amadeus, Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, 1. Auflage, München 2017, Zit.: BEARBEITER in: Schantz/Wolff, Das neue Datenschutzrecht, Rn.

[49] Schaub, Günther, Arbeitsrecht-Handbuch, 19. Auflage, München 2021

[50] Schuster, Fabian /Grützmacher, Malte, IT-Recht, Kommentar, 1. Auflage 2020, Zit.: BEARBEITER in: Schuster/Grützmacher IT-Recht, Art. Gesetz Rn.

[51] Schwartmann, Rolf/Jaspers, Andreas/ Eckhardt, Jens, Kommentar TTDSG, 1. Auflage 2022, Zit.: BEARBEITER in: Schwartmann/Jaspers/Thüsing TTDSG, § Rn.

[52] Schröder, Georg, Datenschutzrecht für die Praxis, 4. Auflage 2021

[53] Sesing, Andreas, Cookie-Banner – Hilfe, das Internet ist kaputt!, MMR 2021, S. 544 - 549

[54] Simitis, Spiros/ Hornung, Gerrit/ Spiecker gen. Döhmann, Indra, NomosKommentar Datenschutzrecht, 2. Auflage, Baden-Baden 2024, Zit.: BEARBEITER in: Simitis/Hornung/Spiecker, DSGVO/BDSG Art./§ Rn

[55] Specht, Louisa/Mantz, Reto, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage, München 2019, Zit.: BEARBEITER in: Specht/Mantz, DatenschutzR-Hdb, § Rn.

[56] Specht-Riemenschneider, Louisa, Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?, ZRP 2022, S. 137 - 140

[57] Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien – Kommentar, 4. Auflage, München 2019, Zit.: BEARBEITER in: Spindler/Schuster, DSGVO Art. Rn.

[58] Steinrötter, Björn, Verhältnis von Data Act und DS-GVO, GRUR 2023, S. 216 - 226

[59] Streinz, Rudolf, Beck`sche Kurz-Kommentare, Band 57 EUV/AEUV, 3. Auflage, München 2018, Zit.: BEARBEITER in: Streinz EUV/AEUV, Art. Gesetz Rn.

[60] Stürmer, Verena, Löschen durch Anonymisieren?, ZD 2020, S. 626 - 631

[61] Sydow, Gernot/ Marsch, Nikolaus, NomosKommentar Europäische Datenschutzgrundverordnung, 3. Auflage, Baden-Baden 2022, Zit.: BEARBEITER in: Sydow/Marsch, Art. Rn.

[62] Taeger, Jürgen/ Gabel, Detlev, Kommentar DSGVO – BDSG - TTDSG, 4. Auflage, Frankfurt am Main 2022, Zit.: BEARBEITER in: Taeger/Gabel, DSGVO/BDSG Art./§ Rn.

[63] Thüsing, Gregor/ Rombey, Sebastian, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, ZD 2021, S. 548 – 553

[64] Verbraucherzentrale Bundesverband, ANONYMISIERUNG UNTER DER DSGVO, Stellungnahme des vzbv zur Konsultation des BfDI, Berlin 20.03.2020, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/vzbv.pdf;jsessionid=9C398EF915FEC35240940DA347948D38.intranet212?__blob=publicationFile&v=2, zuletzt abgerufen am 30.11.2024

[65] Weber, Klaus, Rechtswörterbuch, 28. Edition 01.05.2022, München

[66] Weichert, Thilo, Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten, NZA 2017, S. 565 – 570