UNIKASSEL VERSITÄT

Fachbereich Wirtschaftswissenschaften

Institut für Wirtschaftsrecht

# Rechtsfragen von Datenbrillen im Gesundheitsbereich

Rechtsgutachten zu den BMBF-Projekten IDeA und HIVE-Lab

Auftraggeber:

Internationales Zentrum für Ethik in den Wissenschaften (IZEW), Universität Tübingen

Prof. Dr. Gerrit Hornung, LL.M.

Ass. iur. Helmut Lurtz

Universität Kassel, Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht

Kassel, 28. Februar 2020

# Management Summary

**Rechtsfragen des Projekts IDeA**

I. Die DS-GVO ist für die Verarbeitung personenbezogener Daten durch Datenbrillen anwendbar. Insbesondere ist die Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DS-GVO auch für private Träger von Datenbrillen in der Regel nicht einschlägig.

II. Die Grundsätze des Art. 5 DS-GVO postulieren verbindliche Regelungen und finden Anwendung auf die Verarbeitung durch Datenbrillen. Aus ihnen ergeben sich jedoch keine besonderen Einschränkungen, die über die sonstigen Bestimmungen der DS-GVO hinausgehen. Gerade im medizinischen Forschungsbereich kann insbesondere eine Zweckänderung in vielen Fällen auf Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO gestützt werden.

III. Durch Datenbrillen werden mitunter personenbezogene Daten verarbeitet, die einen besonderen Schutz nach Art. 9 DS-GVO erfahren können (z.B. Gesundheitsdaten des Trägers). Lediglich bei einer Verwendungsabsicht bezüglich dieser Daten sind diese als sensibel i.S.d. Art. 9 Abs. 1 DS-GVO zu qualifizieren und die strengen Voraussetzungen des Art. 9 Abs. 2 DS-GVO zu beachten. Diese Verwendungsabsicht wird in diesem Anwendungsfall in aller Regel nur bezüglich der Daten des Trägers, nicht hingegen bezüglich der Umgebungsdaten vorliegen.

IV. Die datenschutzrechtliche Verantwortlichkeit des Forschungsprojekts IDeA richtet sich nach der genauen technischen Ausgestaltung der Anwendung, der rechtlichen Ausgestaltung des Forschungsprojekts IDeA, der jeweils verarbeitenden Projektpartner und der tatsächlichen Aufgabenverteilung.

1. Das ausschlaggebende Kriterium der datenschutzrechtlichen Verantwortlichkeitsbestimmung ist die (tatsächliche) Entscheidung über Zwecke und Mittel der Datenverarbeitung.

2. Jeder Verantwortliche ist dabei nur für die (Teil-)Verarbeitungen verantwortlich, für die er tatsächlich über die Zwecke und Mittel entscheidet.

3. Für die Verarbeitung von personenbezogenen Daten im Rahmen des Forschungsprojekts IDeA wird der jeweils verarbeitende Projektpartner als zumindest alleiniger Verantwortlicher einzustufen sein. Sind mehrere IDeA-Projektpartner an einer Datenverarbeitung beteiligt, kommen je nach Einzelfall zwei separate alleinige Verantwortlichkeiten, eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit in Betracht.

4. Die Verantwortlichkeitsverteilung mit weiteren Verantwortlichen (z.B. Hardwareanbieter) lässt sich nur im Einzelfall bestimmen. Selbst bei Vorliegen einer gemeinsamen Verantwortlichkeit, wäre das Forschungsprojekt IDeA bzw. seine jeweiligen Mitglieder nur für die Verarbeitungen verantwortlich, für die sie eine tatsächliche Entscheidungsbefugnis haben. Bleiben etwaige weitere Datenverarbeitungen des Hardwareanbieters verschleiert, wird diesbezüglich eine Verantwortlichkeit i.d.R. nicht vorliegen. Jedoch ist das Risiko dieser Unkenntnis bei der Beurteilung der Rechtmäßigkeit der eigenen Datenverarbeitungen zu berücksichtigen.

V. Die Rechtfertigung der Datenverarbeitung durch die Datenbrille ist nach drei Verarbeitungsrichtungen gesondert zu bewerten.

1. Verarbeitet der Anbieter personenbezogene Daten des Trägers der Datenbrille, so empfiehlt sich die Einholung einer ausdrücklichen Einwilligung. Sie erweist

sich als der einfachste und sicherste Weg der Legitimation in diesem Verarbeitungsverhältnis. Aufgrund der persönlichen Vorteile ist davon auszugehen, dass die Träger in aller Regel in die Datenverarbeitung einwilligen werden.

Die zweite Möglichkeit besteht in der Erforderlichkeit für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheitsbereich (Art. 9 Abs. 2 lit. h DS-GVO i.V.m. § 22 BDSG). Auch auf diesem Weg kann eine Datenverarbeitung legitimiert werden, da insbesondere die vorausgesetzte Erforderlichkeit für die medizinische Diagnostik und Behandlung im Gesundheitsbereich vorliegen wird. Neben dem Vorliegen des entsprechenden Behandlungszwecks sind spezielle Voraussetzungen einzuhalten, die im Ergebnis mehr Aufwand erfordern als eine Einwilligung.

Die dritte Möglichkeit besteht in der Erforderlichkeit für Forschungszwecke (Art. 9 Abs, 2 lit. j DS-GVO i.V.m. § 27 BDSG bzw. die jeweiligen landesrechtlichen Grundlagen). Sie setzt ein erhebliches Überwiegen der Interessen und strenge Garantien zum Schutz der Betroffenen voraus und stellt damit die höchsten – aber dennoch grundsätzlich erfüllbaren – Anforderungen an eine Verarbeitung.

2. Verarbeitet der Anbieter personenbezogene Daten von Dritten (z.B. Passanten) erweist sich eine Einwilligung aufgrund faktischer Gründe als untauglich. Neben der faktischen Unmöglichkeit, alle erforderlichen (ggf. sehr vielen) Einwilligungen einzuholen, darf die Bereitschaft unbekannter Dritter, eine solche zu erteilen, bezweifelt werden.

   Eine Möglichkeit ist eine Legitimation nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO bei Überwiegen von berechtigten Interessen. Erfolgt der Einsatz einer Datenbrille für private (nichtmedizinische) Zwecke, werden die Interessen der betroffenen Personen deutlich überwiegen und eine Rechtfertigung in aller Regel scheitern. Bei Zwecken, die zur Behandlung des Patienten (d.h. des Trägers der Datenbrille) medizinisch veranlasst sind, können hingegen die Interessen der Patienten überwiegen und eine Nutzung kann deshalb zulässig sein. Technische und organisatorische Maßnahmen (z.B. umgehende Löschung oder situationsbedingte Funktionen) bieten dabei eine gute Möglichkeit, die Abwägung der Interessen positiv zu beeinflussen und dadurch einen rechtmäßigen Betrieb der Anwendung zu ermöglichen.

3. Verarbeitet der Träger der Datenbrille personenbezogene Daten von Dritten, wird er sich ebenfalls auf berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO stützen (müssen). Hierbei sind dieselben Erwägungen wie im Verhältnis des Anbieters zu den Dritten maßgeblich. Eine Einwilligung erscheint hingegen für bestimmte eingeschränkte Fälle denkbar, insbesondere sofern ein Näheverhältnis zu Familienangehörigen oder engen Bekannten besteht.

VI. Eine Haftung der Betreiber von Datenbrillen für medizinische Zwecke ist grundsätzlich in zwei unterschiedliche Phasen zu trennen und gesondert zu bewerten: in eine Erprobungsphase und eine Nutzungsphase. Mangels einer Regelung von Haftungstatbeständen in den medizinrechtlichen Vorschriften ist dabei auf die allgemeinen Haftungsnormen zurückzugreifen.

1. Eine vertragliche Mängelhaftung ist je nach Ausgestaltung des Systems und der vertraglichen Regelung grundsätzlich denkbar. Sie wirkt hingegen nur inter partes, weshalb Dritte hieraus keine Ansprüche geltend machen können. Eine

Haftung kann grundsätzlich durch einen Haftungsausschluss begrenzt werden, jedoch muss sich dieser an die Grenzen des AGB-Rechts halten.

2. In der Erprobungsphase wird in der Regel keine Haftung des Betreibers bestehen. Das verschuldensunabhängige ProdHaftR ist mangels Inverkehrbringens des Produkts nicht anwendbar. Eine deliktische Haftung scheitert in aller Regel am mangelnden Verschulden des Betreibers.

3. In der Nutzungsphase ist eine Haftung des Betreibers in gewissen Situationen möglich. Eine Haftung nach dem ProdHaftG erscheint je nach Auffassung eines Fehlers i.S.d. § 3 ProdHaftG als denkbar. Die diesbezügliche Rechtslage ist bezüglich AR-Assistenzsystemen noch ungeklärt. Nach einem Vergleich mit neuartigen Systemen, die vergleichbare haftungsrechtliche Fragestellungen hervorrufen (z.B. automatisiertes Fahren), erscheinen bestimmte Haftungsszenarien vorstellbar. Zu einem ähnlichen Ergebnis gelangt eine deliktsrechtliche Haftung nach § 823 BGB.

**Rechtsfragen des Projekts HIVE-Lab**

I. Datenschutzrechtliche Vorgaben müssen nach Art. 2 Abs. 1 DS-GVO nur bei einer Verarbeitung von personenbezogenen Daten eingehalten werden. Werden im Rahmen der Leistungen des HIVE-Labs keine personenbezogenen Daten verarbeitet (z.B. durch Erhebung oder Speicherung), so sind auch keine datenschutzrechtlichen Anforderungen zu beachten.

II. Bei Verbundprojekten mit mehreren Forschungspartnern bestehen hinsichtlich der Verantwortlichkeitsverteilung mehrere Möglichkeiten. Eine Möglichkeit ist die Gründung einer juristischen Person oder einer rechtsfähigen Personengesellschaft für das Verbundprojekt, die dann als Verantwortliche für die Verarbeitung von personenbezogenen Daten in Betracht kommen kann (z.B. eine GbR). Sofern keine juristische Person oder rechtsfähige Personengesellschaft besteht, muss für jede Forschungseinrichtung des Verbundprojekts jeweils geprüft werden, ob diese über die Zwecke und Mittel der einzelnen Datenverarbeitungen tatsächlich entscheiden.

   Wird ein Beteiligter lediglich als Auftragsverarbeiter für einen Verantwortlichen tätig, ist auf die Einhaltung von Art. 28 DSGVO zu achten und insbesondere ein entsprechender Vertrag abzuschließen.

III. Die Rechtfertigung der Datenverarbeitungen der an HIVE-Lab beteiligten Forschungsprojekte bemisst sich je nach der einzelnen Verarbeitung personenbezogener Daten.

   1. Im Rahmen der Forschung des HIVE-Labs werden auch besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO verarbeitet. Dementsprechend sind im Falle einer Verwendungsabsicht bezüglich dieser Daten die strengeren Anforderungen des Art. 9 Abs. 2 DS-GVO einzuhalten. Vorliegend kommen insbesondere die Erforderlichkeit für wissenschaftliche Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz) oder eine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) in Betracht. Für sonstige personenbezogene Daten kommen eine Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO) sowie die Erforderlichkeit für legitime Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO) in Frage.

   2. Auch im Bereich der medizinischen Forschung ist zwischen verschiedenen Stufen der Datenverarbeitung zu unterscheiden. Jeder dieser Stufen enthält unterschiedlich schwere Eingriffe in die Rechte und Freiheiten der Betroffenen.

3. Werden für das Body of Knowledge personenbezogene Daten erhoben, ist aufgrund des Erforderlichkeitsprinzip (über Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz) unter anderem eine Pseudonymisierung durchzuführen sowie ein Identitätsmanagementsystem zu implementieren.

4. Sofern in der Body of Knowledge personenbezogene Daten angepasst und verändert werden, ist insbesondere auf die sachliche Richtigkeit der Daten zu achten.

5. Aufgrund der Ausnahme von dem Prinzip der Speicherbegrenzung in Art. 5 lit. e HS. 2 DS-GVO dürfen für wissenschaftliche Forschungszwecke vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen personenbezogene Daten länger gespeichert werden als dies für den ursprünglichen Zweck erforderlich ist. Bei einer langfristigen Speicherung und Nutzung sind diese Daten zu anonymisieren oder zu pseudonymisieren.

6. Der Zweck der Nutzung ist nach dem Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DS-GVO klar zu bestimmen. In der Regel gelten Sekundärnutzungen für wissenschaftliche Forschungszwecke nach Art. 5 Abs. 1 lit. b DS-GVO „nicht als unvereinbar mit den ursprünglichen Zwecken“ und verstoßen mithin nicht gegen den Zweckbindungsgrundsatz. Diese Weiterverarbeitungen sind jedoch zu anonymisieren (Art. 89 Abs. 1 Satz 4 DS-GVO). Eine Ausnahme hiervon besteht nur, sofern die Zwecke der wissenschaftlichen Forschung sonst nicht erfüllt werden können.

7. Eine rechtmäßige Verarbeitung von personenbezogenen Daten (erst recht sensiblen Daten i.S.d. Art. 9 Abs. 1 DS-GVO) ist umso schwieriger, je mehr Personen Zugriff erhalten und je entfernter dieser Personenkreis von dem Forschungsprojekt HIVE-Lab ist. Sofern HIVE-Lab-externe Forschungsprojekte oder Unternehmen auf personenbezogene Daten zugreifen, sind diese vor dem externen Zugriff zu anonymisieren.

IV. Selbst wenn die Datenverarbeitung grundsätzlich zulässig ist, enthält das Datenschutzrecht weitere Anforderungen an ihre Durchführung. Neben Art. 25 und 32 DS-GVO sieht auch Art. 89 Abs. 1 DS-GVO (ebenso wie die deutschen Gesetze, z.B. § 27 Abs. 1 Satz 2 BDSG, § 24 Abs. 1 Satz 2 HDSIG) technische und organisatorische Maßnahmen vor. Als technische und organisatorische Maßnahmen für die wissenschaftliche Forschung im medizinischen Bereich bieten sich unter anderem eine Anonymisierung und eine Pseudonymisierung an.

V. Eine Einwilligung muss im Bereich der medizinischen Forschung unter anderem für einen oder mehrere bestimmte Zwecke (Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO), freiwillig (Art. 4 Nr. 11 DS-GVO), vor der Verarbeitung informiert (Art. 4 Nr. 11 DS-GVO) und ausdrücklich (Art. 9 Abs. 2 lit. a DS-GVO) erklärt werden.

VI. Im Verhältnis zwischen einem Forschungsprojekt des HIVE-Labs und einem Dritten (z.B. Testperson) gelten die bereits genannten haftungsrechtlichen Erwägungen. Im Verhältnis zwischen dem HIVE-Lab (im Falle einer juristischen Person oder einer rechtsfähigen Personengesellschaft) und den teilnehmenden Forschungsprojekten muss das Verhältnis der Projekte bzw. Projektpartner zueinander vertraglich geregelt werden. Besondere haftungsrechtliche Hürden sind für das HIVE-Lab bzw. dessen Beteiligte nicht ersichtlich.

**Inhaltsverzeichnis**

# 1 Hintergrund und Ausgestaltung des Gutachtens

Die Universität Kassel verfasst im Unterauftrag des Internationalen Zentrums für Ethik in den Wissenschaften **(**IZEW) der Universität Tübingen jeweils ein Rechtsgutachten zu den BMBF-Forschungsprojekten „Integriertes Diagnose- und e-Assistenzsystem für Patienten mit altersbedingter Makuladegeneration (IDeA)“ und „Interaktive Systeme in virtuellen und realen Räumen – Innovative Technologien für ein gesundes Leben: HIVE-Lab“. Die beiden Projekte sind in mehrfacher Hinsicht ähnlich und miteinander verbunden. Zum einen behandeln beide Projekte verwandte Inhalte, die dementsprechend überwiegend ähnliche Rechtsprobleme hervorrufen. So stellt sich die übergeordnete Frage, wie die Nutzung von Datenbrillen im Gesundheitsbereich datenschutzrechtlich zu beurteilen ist. Zum anderen stimmt in beiden Projekten die Besetzung teilweise überein, sodass auch eine übergreifende Behandlung möglich und ausdrücklich erwünscht ist. Bereits im Projektantrag von IDeA ist eine Zusammenarbeit mit HIVE-Lab vorgesehen, um einerseits die Evaluationen effizienter und vergleichbarer zu machen und andererseits Synergien in den Studien herzustellen.

In Abstimmung mit dem Auftraggeber wurden die beiden Unteraufträge deshalb ebenfalls in enger Abstimmung angefertigt und hier gemeinsam vorgelegt. Teil 2 behandelt das Projekt IDeA, Teil 3 das Projekt HIVE-Lab. Durch die Zusammenfassung der beiden Gutachten zu einem gesamten Gutachten, bestehend aus zwei Teilen, kann eine tiefere Behandlung von Rechtsfragen, die beide Projekte betreffen, erreicht werden. Für ein werthaltigeres und zielführenderes Ergebnis werden im Gutachten in beiden Teilen Schwerpunkte gebildet, um so die aktuellsten und wichtigsten Rechtsfragen zu klären.

# 2 Rechtsfragen des Projekts IDeA

Ziel des Projektes ist es, ein auf Virtual- und Augmented-Reality-Technologien (VR/AR) basierendes technisches System zu entwickeln, das ältere Menschen mit Makuladegeneration bei der Bewältigung ihres Alltags unterstützt und ihre medizinische Behandlung optimiert. Konkret sollen VR/AR-Brillen entwickelt werden,

1. den Patienten helfen, Gesichtsfeldstörungen auszugleichen, indem alternative Zusatzfunktionen in noch funktionierende Sichtbereiche projiziert werden,
2. nicht im Labor, sondern im Alltag kontinuierlich Frühdiagnostik betreiben, indem die Sehfunktion der Patienten gemessen wird
3. und eine telemedizinische Befundung durch Augenarzt und Operateure ermöglichen.

## 2.1 Anwendungsszenarien und verarbeitete (personenbezogene) Daten

Für die Ermöglichung der einzelnen Funktionen der Brille werden jeweils unterschiedliche personenbezogene Daten verarbeitet. Diese Funktionen sind die Diagnose-, Trainings-, Assistenz-, Informationsaustausch- und Plattformfunktion. Hinzu treten denkbare Zusatzfunktionen z.B. im Automotive-Bereich.

### 2.1.1 Diagnose

Die Diagnosefunktion der Anwendung soll die Sehfunktion des Trägers der Brille untersuchen. Dabei soll die Nutzung der Brille möglichst in Alltagsaktivitäten integriert werden, um so die Dauer der einzelnen Testsitzungen zu verkürzen, ohne die Validität des Testverfahrens herabzusetzen. Sehfelddefekte verändern das Blickbewegungsverhalten. Es sollen Merkmale pervasiver Fixationsdaten und Augenbewegungsmuster identifiziert werden, die Rückschlüsse auf die Progression von Sehfelddefekten (Lage, Größe und Schweregrad) zulassen sowie ein Vorhersagemodell (predictive model) für die AMD-Verlaufsüberwachung entwickelt werden. Es werden sowohl Augenbewegungsdaten aus kontrollierten Laborexperimenten als auch Blickverhalten während Alltagshandlungen untersucht. Für die Diagnosefunktion sind dabei folgende Ausgestaltungen und Einsatzmöglichkeiten denkbar und geplant:

- Eine Datenbrille ohne oder mit Szenekamera
- Nutzung in häuslicher Umgebung oder außerhalb
- Die Testdurchführung wird automatisch gestartet oder manuell initiiert
- Die Informationen werden auf dem Gerät lokal oder extern verarbeitet
- Erfüllt das Auswertungsergebnis die festgelegten Erwartungen, empfiehlt die Anwendung einen Arzt zu konsultieren oder erledigt dies automatisch; optional vereinbart die Anwendung einen Termin mit dem Arzt; optional informiert die Anwendung den Arzt über das Ergebnis des Tests bzw. ggf. über das Nichtbestehen des Tests (die Information wird mit einem Patientenidentifikator übermittelt, durch den der Arzt die Information zuordnen kann);

Für die Diagnosefunktion sollen folgende Daten des Trägers verarbeitet werden:

- Alter und Geschlecht
- Erkrankung der Herzkranzgefäße
- Schlaganfall
- Halsschlagader-Operation
- Belastungsbedingte Beschwerden

- Blutdruck
- Bluthochdruck
- Blutzucker
- Blutfette (Cholesterin und Triglyzeride)
- Rauchen
- Körpergröße, Gewicht und Bauchumfang
- Körperliche Aktivität/Sport
- Fehlsichtigkeit
- Bekannte Augenerkrankungen
- Erkrankungen in der Familie
- Anamnese der Augen
    - Sehfähigkeit in der Kindheit
    - Datum der ersten Brille
    - Schielen in der Kindheit
    - Augenoperationen
    - Laser-Eingriffe am Auge
    - Augenverletzungen
    - Glaukom (Grüner Star)
    - Netzhautablösung
    - Entzündung im Auge (Uveitis)
    - Verschlechterung des Sehens
    - Augentropfen

### 2.1.2 Training

Die Trainingsfunktion besteht aus einem impliziten Fixationstraining. Dabei werden Augenbewegungen im freien Verfahren in Bezug auf ihre „Fixationsgüte“ qualifiziert und implizite Trainingskonzepte für den Alltag entwickelt. Die initiale Entwicklung erfolgt dabei über die Methode des simulierten Sehfelddefektes in VR. Trainingsmethoden beinhalten zusätzliche Manipulationen der Sehinhalte, die die Entwicklung eines exzentrischen Fixationsortes optimieren (z.B. Augmentierung des Sehfelddefektes durch binokulare Präsentation, Präsentation von Defektrandbereichen oder systematische Maskierung von Bildinhalten).

Für die Trainingsfunktion sind dabei folgende Ausgestaltungen und Einsatzmöglichkeiten denkbar und geplant:

- Eine Datenbrille ohne oder mit Szenekamera
- Nutzung in häuslicher Umgebung oder außerhalb
- Mögliche Erweiterung: Eingabe persönlicher Daten bei Initialisierung
- Training beinhaltet Veränderung von Sehinhalten, die entweder zu Sehbeeinträchtigung führen können oder solche nicht hervorrufen
- Modus A: Gerät bittet um Erlaubnis, Training zu starten; Modus B: Nutzer startet Training selbsttägig

- Analyse des Trainings wird auf dem Gerät gespeichert oder die Analyse-Ergebnisse werden automatisch an den Arzt übermittelt oder es erfolgt keine Auswertung.

Für die Trainingsfunktion sollen folgende Daten des Trägers verarbeitet werden:

1. Während der Aufnahme (nur lokal auf dem PC des Trägers gespeichert):
   - Datum und Uhrzeit des Starts sowie des Endes der Aufnahme
   - Position der Augen auf den virtuellen Bildschirmen (X und Y-Koordinaten für beide Augen)
   - Pupillendurchmesser der beiden Augen
   - Wahl der App (beispielsweise „Standard-Perimeter“, „Jahrmarkt“ oder andere)
   - Falls der Nutzer mit der VR-App noch weitere Spiele spielt: Screenrecordings der Spiele mit Metainformationen, welche Art von graphischen Objekten an welchen Stellen auf dem Bildschirm zu sehen waren
   - Spracheingaben des Nutzers (ggf. realisiert mit einem Online-System, d.h. Senden der Spracheingabe zu einem Server, dort Verarbeitung und Rücksendung von Steuerbefehlen)
   - Sprachausgaben des Systems
   - Videoaufnahme beider Augen
   - Kopfneigung in den drei Raumrichtungen
2. Weitergegebene Daten an den Augenarzt (via Datenübertragung oder USB-Diskette):
   - Nur noch aufbereitete Daten in der Form, welche Punkte in der Perimetriemessung der Nutzer gesehen hat und welche nicht
   - Anzahl, Datum, Uhrzeit und Zeitdauer der Messungen
   - Der Augenarzt hat zusätzlich auch die in MedStage[1] hinterlegten Daten vorliegen (s.o.)

### 2.1.3 Assistenzfunktion

Es werden zwei Arten von AR/VR-basierten Assistenzfunktionen entwickelt: zum einen werden nachlassende Sehfunktionen kompensiert (z.B. Vergrößerung zur Leseunterstützung, Kontrastverstärkung) und zum anderen werden zusätzliche Informationen in das intakte Gesichtsfeld projiziert (z.B. Lokalisationshilfen bei Greif- und Zielbewegungen, semantische Umcodierung von Farben in Symbole). Es werden erste Ansätze für Kontextbewusstsein entwickelt, d.h. das System setzt Funktionen selektiv in Situationen ein, in denen der Nutzer sie benötigt.

### 2.1.4 Informationsaustausch durch Schnittstellen (z.B. mit Ärzten)

Nutzerschnittstellen sollen Patienten Zugang zu den diagnostischen und assistiven Funktionen erlauben (z.B. zum Zu- oder Abschalten von Assistenten). Daneben sollen die Schnittstellen eine vereinfachte Kommunikation für räumlich oder zeitlich getrennte Akteure bereitstellen (z.B. telemedizinische Konsultation zwischen Arzt und Patient im Altersheim; virtuelle Konferenz zur Übergabe zwischen Ärzten). Diese Schnittstellen ermöglichen zudem einen Zugang zu Patientendaten, die durch die entwickelten Diagnose- und Assistenzfunktionen gesammelt

[1] MedStage ist eine webbasierte Datenbank des Projektpartners Talkingeyes & More GmbH zur u.a. Speiche rung von medizinischen Daten und zur standardisierten ärztlichen Auswertung von medizinischen Daten. https://www.talkingeyes-and-more.de/Content/Article.aspx?JOURNAL_ID=12&CATE GORY_ID=118&ARTICLE_ID=563.

wurden (z.B. Einbindung realer Szenen aus dem Alltag des Patienten mit Overlay-Visualisierung der Augenbewegungen).

Folgende (personenbezogene) Daten werden dabei verarbeitet:

- Videoaufnahmen der Umgebung
- Ergebnisse einer Bilderkennung von Objekten in der Umgebung (deshalb ggf. auch Personen und Kfz-Kennzeichnen und ähnliches)
- Uhrzeit als fortlaufender Zeitstempel der Aktionen des Nutzers
- Position des Nutzers (Längen- und Breitengrad)
- Daraus abgeleitet Bewegungsinformationen (Geschwindigkeit etc.) und Kontextinformationen über die Umgebung
- Interaktionsdaten mit der AR-Welt

### 2.1.5 Plattform

Um all diese Funktionen zu vereinen, bedarf es einer Softwarearchitektur und -plattform. Durch eine offene Architektur wird die Anbindung verschiedener Endgeräte und die Zusammenarbeit der verschiedenen Anwendungen ermöglicht. Diese Cloud-Plattform bietet die Basis für die konkrete Anwendungsentwicklung, insbesondere durch die Bereitstellung von Bibliotheken und Komponenten.

Für die Cloud-Plattform sollen folgende Daten des Trägers verarbeitet werden:

- Verbindungsdaten wie Datum und Uhrzeit des jeweiligen Zugriffs sowie die IP-Adresse des Internetanschlusses
- In dieser Cloud sollen sowohl die MedStage-Daten als auch die Blickdaten aus allen Szenarien gespeichert werden
- In dieser Cloud wird auch eine (Echtzeit)-Verarbeitung der aufgenommenen Blick- und Umgebungsdaten durchgeführt, um in Echtzeit zu berechnen, welche Dinge der Träger in seiner Umgebung wahrnimmt und wie sich seine Sehleistung entwickelt.

### 2.1.6 Möglicher Zusatz: Automotive

Eine perspektivisch denkbare Erweiterung der Lösung ist die Anwendung in anderen Umgebungen, wie etwa dem Automotive-Bereich. Ohne genauere Kenntnis der möglichen Anwendung könnten folgende (personenbezogene) Daten verarbeitet werden:

1. Eye-Tracking-Daten
   - Datum und Uhrzeit des Starts und Endes der Aufnahmen
   - Position der Augen auf einem virtuellen Bildschirm (X,Y-Koordinaten für linkes und rechtes Auge)
   - Vektor der Blickrichtung
   - Pupillendurchmesser über Zeit für linkes und rechtes Auge
   - Spracheingaben des Fahrers (ggf. Realisiert mit einem Online-System, d.h. Senden der Spracheingabe zu einem Server, dort Verarbeitung und Rücksendung von Steuerbefehlen)
   - Sprachausgaben des Systems
   - Videoaufnahme des linken und rechten Auges
   - Kopfneigung in den drei Raumrichtungen

- Video des Gesichts des Fahrers

2. Daten vom Fahrzeug (Auswahl) oder Fahrsimulator
   - Uhrzeit als fortlaufender Zeitstempel
   - Position des Fahrzeugs (Längen- und Breitengrad)
   - Bewegungsinformationen (Geschwindigkeit etc.)
   - Interaktionsdaten (Gaspedal- und Bremspedaleinstellungen, Lenkradwinkel)
   - Weitere Einstellungsparameter vom Fahrzeug (z.B. Modus des Fahrassistenzsystems)
   - Umgebungsdaten (Videoaufnahmen des Straßenverkehrs)
   - Bilderkennungsdaten (erkannte Objekte)
   - Abschnitt der Strecke im Experiment (Modul-ID)

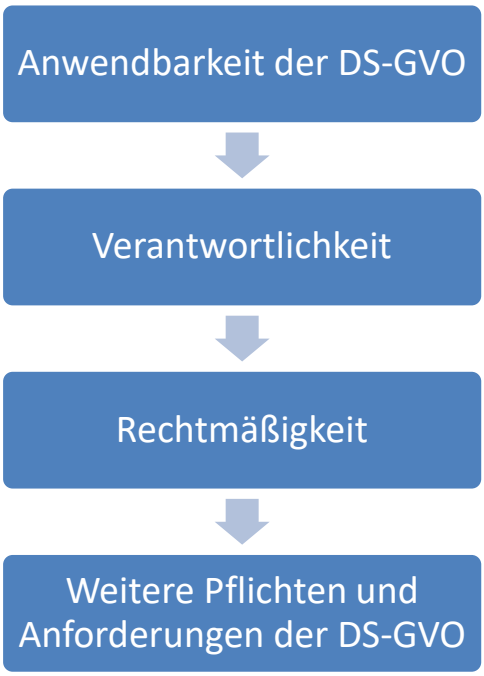
## 2.2 (Datenschutz-)Rechtliche Prüfung

Die datenschutzrechtliche Rechtslage richtet sich maßgeblich nach der Datenschutz-Grundverordnung (DS-GVO). In einem ersten Schritt soll deshalb geprüft werden, ob die DS-GVO überhaupt anwendbar ist. Nur dann sind datenschutzrechtliche Regeln überhaupt zu beachten.

In einem zweiten Schritt ist die Verantwortlichkeit zu prüfen, also wer für die Verarbeitung verantwortlich ist und damit für die Einhaltung der Normen der DS-GVO sorgen muss.

In einem dritten Schritt wird sodann geprüft, ob die jeweilige Datenverarbeitung tatsächlich rechtmäßig ist.

Wird auch die dritte Hürde gemeistert, ist in einem vierten Schritt zu fragen, welche Anforderungen die DS-GVO an die an sich rechtmäßige Verarbeitung stellt.




Als letztes sollen als Annex ausgewählte haftungsrechtliche Herausforderungen von Datenbrillen im Gesundheitsbereich betrachtet werden.

### 2.2.1 Anwendbarkeit der DS-GVO

Datenschutzrechtliche Herausforderungen stellen sich nur, sofern die DS-GVO überhaupt anwendbar ist. Sie gilt nach Art. 2 Abs. 1 DS-GVO 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. In Datenbrillen werden Daten automatisiert verarbeitet. In den erläuterten Anwendungsszenarien werden überdiese in vielfältiger Form personenbezogene Daten sowohl über den Träger einer Datenbrille als auch über andere Personen verarbeitet.

Die DS-GVO findet nach Art. 2 Abs. 2 lit. c DS-GVO allerdings insbesondere keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (sog. Haushaltsausnahme). Die wohl häufigste Nutzungsart von Datenbrillen ist der private Gebrauch von Endkunden, die sie zu privaten (Bequemlichkeits-)Zwecken nutzen und damit prima facie unter den Ausnahmetatbestand fallen würden. Genauso wird der typische Nutzer der in IDeA entwickelten Datenbrille diese nicht kommerziell, sondern vielmehr zur Behandlung seiner Augenkrankheit nutzen – also nach umgangssprachlichem Verständnis „privat".

Bei der Anwendbarkeit der DS-GVO könnte also zu unterscheiden sein. Denn während sich Anbieter von Datenbrillen, behandelnde Ärzte, Cloud- und sonstige Plattformanbieter jedenfalls nicht auf die Haushaltsausnahme berufen können und in jedem Fall die DS-GVO zu beachten haben, könnten sich die Träger der Brille ggf. auf die Ausnahme berufen.

Wegen ihres Ausnahmecharakters, dem nur schwer kalkulierbaren Risiko und der Gewährleistung eines effektiven Datenschutzes ist der Ausnahmetatbestand hingegen eng auszulegen.[2] Er soll den nicht-wirtschaftlichen Datenumgang von Privatpersonen nicht generell aus dem Schutz der DS-GVO herausnehmen, sondern nur einer unangemessenen Anwendung der weiten und offenen Tatbestände der DS-GVO auf rein private Sachverhalte entgegenwirken.

Im öffentlichen Raum können durch Datenbrillen eine Vielzahl an Personen heimlich aufgenommen werden, und die ständige Gefahr gefilmt zu werden, kann zu einem Überwachungsdruck führen. Werden Datenbrillen in privaten Räumlichkeiten genutzt, ist zwar die Gefährdung aufgrund des kleineren Kreises an betroffenen Personen und der oftmals vorhandenen Information und Transparenz geringer, aber der Verlust der Verfügungsgewalt über die Informationen, etwa durch das Hochladen ins Internet, führt in aller Regel ebenfalls zur Anwendbarkeit des Datenschutzrechts.[3] Dementsprechend entschied auch der EuGH, dass Kamerasysteme, die den öffentlichen Raum erfassen, stets in den Anwendungsbereich der DS-GVO fallen.[4] Dies muss auch für Datenbrillen oder andere Wearables gelten, mit denen der Träger in der Lage ist, seine Umgebung in Bild und Ton zu erfassen.

Folgende Kriterien lassen sich für die Bestimmung von ausschließlich persönlichen oder familiären Tätigkeiten i.S.d. Art. 2 Abs. 2 lit. c DS-GVO heranziehen:[5]

- Größe und Bestimmbarkeit (bzw. Kontrollierbarkeit) der betroffenen Personen: Die Auswirkungen einer Verarbeitung in der Öffentlichkeit ist wesentlich größer als in einer geschlossenen Gruppe.
- Soziales (Nähe-)Verhältnis der betroffenen Personen (z.B. persönliche oder familiäre Beziehung): Hintergrund ist ein drohender Kontrollverlust der Betroffenen über ihre

---

2 Simitis/Hornung/Spiecker gen. Döhmann-*Roßnagel*, Art. 2 Rn. 23.

3 *Schwenke*, NJW 2018, 823 (827).

4 EuGH, EuZW 2015, 234 (236), Rn. 34 f.

5 *Artikel-29-Datenschutzgruppe*, Annex 2, 2012, 4.

Daten[6]; verlassen die Daten den „privaten Herrschaftsraum“ der Privatpersonen, so können Dritte – berechtigt oder nicht – zugreifen.[7]

- Umfang und Häufigkeit der Verarbeitung: Die Natur der persönlichen Verarbeitung versteht sich nach historischer Auslegung und auch nach dem Sinn und Zweck der Norm eher in eine intrinsische Richtung als in eine extrinsische. Daraus folgt, dass eher eine seltenere Verarbeitung gemeint ist. Eine häufige und umfangreiche Erhebung ähnelt eher einer professionellen und gewerblichen Nutzung, die dann auch datenschutzrechtliche Pflichten nach sich ziehen muss.
- Verarbeitung durch einen einzigen oder mehreren Verantwortlichen: Die Verarbeitung durch eine größere Anzahl von Verantwortlichen spricht für eine professionellere Verarbeitung, bei der die Auferlegung von Pflichten leichter gerechtfertigt erscheint.
- (Negative) Auswirkung auf andere: Einschüchterungseffekte (z.B. Überwachungsgefühl durch Nutzung von Google Glass einer großen Gruppe) sprechen gegen die Annahme der Ausnahmeregelung.

Aufgrund dieser Kriterien lassen sich folgende typisierende Fallgruppen bilden: [8]

- Eine Nutzung für berufliche und kommerzielle Zwecke ist nicht von der Ausnahme erfasst.
- In öffentlichen Bereichen ist die Haushaltsausnahme nicht einschlägig.
- Private Aufnahmen mehrerer Personen sind eher nicht erfasst.
- Medizinische Gründe stellen hingegen typischerweise persönliche Angelegenheiten dar.[9]

Letztlich handelt es sich auch bei der Entscheidung über die Haushaltsausnahme um eine Abwägung der Interessen unter Berücksichtigung der Schutzbedürftigkeit der betroffenen Personen und der Belastungen, die die Anwendung der DS-GVO für die privat agierenden Träger der Sehhilfe mit sich bringen würde. Wie bereits festgestellt, überwiegen die Interessen der betroffenen Personen in aller Regel. Dies kann nur durch gravierende Gründe aufgewogen werden. Die Unterstützung zur Ausgleichung körperlicher Nachteile durch eine Sehhilfe (Unterstützungsfunktion) dient dem Zweck der Verbesserung bzw. Herstellung der eigenen Lebensqualität. Bereits der Natur der Sache nach handelt es sich dabei nicht um eine Angelegenheit Dritter, sondern der eigenen Person. Dennoch erscheint es nicht verhältnismäßig, jede Datenverarbeitung zur persönlichen gesundheitlichen Unterstützung komplett aus dem Anwendungsbereich der DS-GVO auszunehmen. Gerade im öffentlichen Bereich werden vor dem Hintergrund der Rechtsprechung des EuGHs die Interessen der zahlreichen Betroffenen überwiegen. Das Interesse der Träger an dem Ausgleich der gesundheitlichen Nachteile findet im Rahmen der Abwägung der Interessen ausreichend Berücksichtigung.[10]

Im Ergebnis kann sich der private Träger der Datenbrille für die Nutzung für medizinische Zwecke nur in einigen Fällen auf die Haushaltsausnahme berufen. So könnte die Haushaltsausnahme für AMD-kranke Personen bei einer Nutzung zuhause oder bei Bekannten in einem

---

6 *Lang* 2008, 258.

7 *Schwenke* 2016, 204.

8 *Schwenke* 2016, 202 ff.

9 *Schwenke* 2016, 209.

10 So auch der EuGH zur DSRL, der eine privater Videoüberwachung unter Miterfassung öffentlichen Raums nicht unter die Haushaltsausnahme gefasst hat und feststellte, dass die berechtigten Interessen des Schutzes des Eigentums, der Gesundheit und des Lebens in Art. 7 lit. f, Art. 11 Abs. 2 und Art. 13 Abs. 1 lit. d und g DSRL zu berücksichtigen seien, EuGH, EUZW 2015, 234 (236), Rn. 34.

überschaubaren, abgegrenzten und für den Nutzer bekannten Betroffenenkreis greifen. In diesem Fall wären die Anforderungen der DS-GVO nicht zu beachten.[11] Im öffentlichen Raum sind hingegen höhere Anforderungen zu stellen und die DS-GVO wird selbst bei einer medizinischen Veranlassung vollständig anwendbar sein. Letztlich erfolgt die Entscheidung der Anwendbarkeit auf einer Abwägung der Interessen im Einzelfall, weshalb es ratsam erscheint im Zweifel von der Anwendbarkeit der DS-GVO auszugehen.

Zu beachten ist, dass das Gesetz mit dem Wortlaut „ausschließlich" eindeutig vorschreibt, dass eine Mischfunktion nicht erfasst sein soll. Wird die Kamera sowohl für eine Trainings- bzw. Unterstützungsfunktion als auch für andere Zwecke (z.B. Unterstützung zu beruflichen Zwecken) benutzt, kann diese ihre Einstufung als rein familiär verlieren.

### 2.2.2 Auswirkung der Datenschutzgrundsätze auf die Datenverarbeitung

Die Normen der DS-GVO sind auf den allgemeinen Grundsätzen des Art. 5 DS-GVO aufgebaut.[12] Den Grundsätzen wohnen dabei zwei Charaktereigenschaften inne.[13] Zum einen sind sie Programmsätze, die mit Kernbegriffen[14] das elementare Regelungsprogramm der DS-GVO beschreiben, zum anderen postulieren sie verbindliche Regelungen, deren Missachtung ein Bußgeld gem. Art. 83 Abs. 5 lit. a DS-GVO nach sich ziehen kann.[15]

Von besonderer Bedeutung ist der Grundsatz der *Zweckbindung* gem. Art. 5 Abs. 1 lit. b DS-GVO. Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Hierdurch sollen mögliche Daten- und Informationsströme eingegrenzt werden.[16] An diese Zwecke ist die verarbeitende Stelle grundsätzlich gebunden. Zur Erreichung dieses Ziels wird dieser Grundsatz durch die Grundsätze der Datenminimierung und der Speicherbegrenzung flankiert.[17] Der Zweck ist eine Art Anker für die – auch künftige[18] – Datenverarbeitung.[19] Der Verantwortliche ist verpflichtet einen bestimmten Zweck zu bestimmen, und er ist hinsichtlich der Art, dem Umfang und der Speicherdauer an diesen Zweck gebunden. Datenverarbeitungen, die darüber hinausgehen, also für die Zweckerreichung nicht erforderlich, angemessen oder auf das notwendige Maß beschränkt sind, verstoßen gegen den Zweckbindungsgrundsatz und sind rechtswidrig.

Werden durch Datenbrillen personenbezogene Daten erhoben, so ist aufgrund des Zweckbindungsgrundsatzes festzulegen, ob die Daten nur für die Behandlung und Unterstützung des einzelnen Nutzers oder auch der Veröffentlichung dienen oder eine Analyse – ggf. mit einer Verknüpfung – der Daten zu anderen Zwecken erfolgen soll. Eine spätere Weiterverarbeitung der personenbezogenen Daten zu anderen als den ursprünglichen Zwecken ist zwar nicht strikt ausgeschlossen, jedoch ist die Zweckänderung nur unter den strengen Voraussetzungen der Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO und Art. 6 Abs. 4 DS-GVO möglich.

---

11 Weitere Verantwortliche, wie etwa das Forschungsprojekt IDeA, das Auswertungen mit den erhobenen personenbezogenen Daten der Umgebung anstellen will, können sich hingegen nicht auf die Haushaltsausnahme berufen.

12 Simitis/Hornung/Spiecker Döhmann-*Roßnagel*, Art. 5 DS-GVO Rn. 1.

13 Paal/Pauly-*Frenzel*, Art. 5 DS-GVO Rn. 1.

14 *Albrecht*/*Jotzo* 2017, 50.

15 Kritisch zur Sanktionierung wegen fehlender Bestimmtheit von Art. 5 DS-GVO s. Paal/Pauly-*Frenzel*, Art. 5, DS-GVO Rn. 2; eingeschränkte Interpretation der Sanktionierbarkeit aus diesem Grund bei Simitis/Hornung/Spiecker gen. Döhmann-*Roßnagel*, Art. 5 DS-GVO Rn. 18, 22.

16 So zutreffend *Britz*, EuGRZ 2009, 1 (10); Paal/Pauly-*Frenzel*, Art. 5 DS-GVO Rn. 23.

17 Vgl. *Artikel-29-Datenschutzgruppe*, WP 203, 2013, 4: die Zweckfestlegung ist zwingende Voraussetzung dieser anderen Grundsätze.

18 *Artikel-29-Datenschutzgruppe*, WP 203, 2013, 4; *Monreal*, ZD 2016, 507 (509).

19 Paal/Pauly-*Frenzel*, Art. 5 DS-GVO Rn. 23.

Ein möglicher Weg – gerade in der medizinischen Forschung – ist es, die Zweckfestlegung im Moment der Datenerhebung für mehrere Zwecke gleichzeitig vorzunehmen. Die Zweckbestimmung muss dennoch eindeutig sein; eine Blankobestimmung der Zwecke ist nicht zulässig.[20] So können bei einem Forschungsprojekt alle angedachten Zwecke aufgeführt werden, selbst wenn manche nun im Laufe des Projekts nicht mehr verfolgt werden.

**Exkurs: Zweckänderungen**

Stößt ein Forschungspartner bei der Verarbeitung der personenbezogenen Daten auf neue Erkenntnisse und Auswertungsmöglichkeiten und beabsichtigt diese nun auch für andere Zwecke zu verarbeiten, so steht der damit verbundenen Zweckänderung der Grundsatz der Zweckbindung aus Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO entgegen. Eine solche weitere Verarbeitung ist nur möglich, sofern die strengen Regeln einer Zweckänderung gewahrt werden.

Eine Möglichkeit einer zulässigen Weiterverarbeitung besteht in der Vereinbarkeitsprüfung nach Art. 6 Abs. 4 DS-GVO. Hiernach soll durch eine sogenannte Kompatibilitätsprüfung festgestellt werden, ob die Verarbeitungen zu zwei unterschiedlichen Zwecken miteinander vereinbar (also kompatibel) sind. Die Norm nennt dabei – nicht abschließend – Kriterien[21] als Hilfestellungen bzw. Leitlinien für diese Beurteilung. Dabei sind alle Umstände des Einzelfalls zu berücksichtigen, weshalb die Vereinbarkeit von verschiedenen Verarbeitungszwecken stets von Fall zu Fall zu bestimmen ist.[22]

Die zweite Möglichkeit der zulässigen Weiterverarbeitung besteht in der Verarbeitung zu Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken nach Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO. Der Begriff der wissenschaftlichen Forschungszwecke wird dabei weit gefasst und beinhaltet unter anderem die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen (EG 159 Satz 2 DS-GVO). Der Grund der Privilegierung besteht darin, dass diese Verwendungszwecke typischerweise nicht auf eine Person abzielen.[23]

Die gem. Art. 6 Abs. 4 DS-GVO stets erforderliche Kompatibilität wird in diesem Fall gem. Art. 5 Abs. 1 lit. b i.V.m. Art. 89 DS-GVO vermutet (EG 50, 156 DS-GVO). Diese Vermutung darf hingegen nicht als allumfassender Freifahrtschein für sämtliche Verarbeitungszwecke verstanden werden.[24] Die Rechtsfolge dieser Privilegierung ist genau genommen nicht die automatische Vereinbarkeit des Primär- und Sekundärzwecks. Sie entbindet richtigerweise nicht von der Prüfung der Vereinbarkeit der beiden Zwecke.[25] Vielmehr sind bei jeder Weiterverarbeitung alle Umstände des Einzelfalls zu berücksichtigen.[26] Dennoch wird im Regelfall eine Vereinbarkeit vorliegen.[27] Als Ausgleich für die Privilegierung müssen jedoch geeignete Garantien (durch technische und organisatorische Maßnahmen) zum Schutz der Betroffenenrechte gewährleistet werden.[28] Gerade im medizinischen Forschungsbereich kann eine Zweckänderung in vielen Fällen auf Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO gestützt werden.

---

20 Simitis/Hornung/Spiecker gen. Döhmann-*Roßnagel*, Art. 5 DS-GVO Rn. 79.

21 Z.B. die Verbindung zwischen den Zwecken, der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden und die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen.

22 So auch zur DSRL. *Artikel-29-Datenschutzgruppe* WP 203, 40.

23 Simitis/Hornung/Spiecker gen. Döhmann-*Roßnagel*, Art. 5 DS-GVO Rn. 104.

24 So ausdrücklich *EDPS* 2020, 22.

25 Simitis/Hornung/Spiecker gen. Döhmann-*Roßnagel*, Art. 5 DS-GVO Rn. 109.

26 *EDPS* 2020, 22.

27 *EDPS* 2020, 22; Simitis/Hornung/Spiecker gen. Döhmann-*Roßnagel*, Art. 5 DS-GVO Rn. 109.

28 S. hierzu Kap. 3.3 und 3.4.

### 2.2.3 Besondere Arten von Daten i.S.d. Art. 9 DS-GVO

Die Verordnung stellt besonders „sensible“ personenbezogene Daten unter einen besonderen Schutz. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist nach Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt. Von diesem Grundsatz eröffnet Absatz 2 einige Ausnahmen, die eine Verarbeitung dennoch ermöglichen.

Auf den ersten Blick erscheint es, dass in Bildaufnahmen fast alle der in Art. 9 Abs. 1 DS-GVO genannten Informationen enthalten sein können. So können durch Bildaufnahmen der Umgebung die rassische und ethnische Herkunft (Hautfarbe), politische Meinungen (Transparente, Buttons), religiöse oder weltanschauliche Überzeugungen (Tragen religiöser Abzeichen), Gewerkschaftszugehörigkeit (Teilnahme an Demonstrationen), biometrische Daten (praktisch jedes Gesichtsbild), Gesundheitsdaten (erkennbare körperliche Gebrechen) und Daten zum Sexualleben oder der sexuellen Orientierung (sexuell konnotierte Handlungen wie Küsse) offenbart werden.

Ein solch weites Verständnis von Art. 9 DS-GVO würde viele Bereiche der Datenverarbeitung – insbesondere die von Video- und Bilddaten – stark einschränken. Aus diesem Grund wird nach herrschender Auffassung durch eine teleologische Reduktion der Anwendungsbereich der Norm eingeschränkt ausgelegt. Unter verschiedenen solcher Lösungsansätze erscheint die Berücksichtigung einer spezifischen Verwendungsabsicht am überzeugendsten.[29]

Bei der Nutzung von Datenbrillen ist zwischen zwei Anwendungsmöglichkeiten zu unterscheiden: zum einen die Verarbeitung der Gesundheitsdaten des Trägers sowie zum anderen die Verarbeitung der Daten der durch die Datenbrille erfassten Dritten.

Werden also die Gesundheitsdaten (z.B. Augenkrankheit) des Trägers verarbeitet, liegen aufgrund der Verwendungsabsicht der Verarbeitung zur Behandlung dieser Augenkrankheit sensible personenbezogene Daten i.S.d. Art. 9 Abs. 1 DS-GVO vor. Dementsprechend sind bezüglich dieser Verarbeitung die strengeren Regeln des Art. 9 Abs. 2 DS-GVO zu beachten. Erfasst die Kamera (oder sonstige Funktionen wie das Mikrophon) der Datenbrille hingegen Daten anderer Personen, die zwar prima facie als sensibel i.S.d. Art. 9 Abs. 1 DS-GVO eingestuft werden könnten, aber nur als ungewollte, aber unvermeidbare „Nebenfolge“ der medizinischen Verwendung der Brille verarbeitet werden, so sind diese Daten mangels einer Verwendungsabsicht nicht als sensibel i.S.d. Art. 9 Abs. 1 DS-GVO zu qualifizieren. Die Verwendungsabsicht zielt in diesem Fall nicht auf die Verarbeitung beispielsweise der religiösen Zugehörigkeit der erfassten ein christliches Kreuz tragenden Dritten, sondern weiterhin der Behandlung und gesundheitlichen Unterstützung des Trägers der Brille. Die strengen Voraussetzungen des Art. 9 Abs. 2 DS-GVO sind bezüglich dieser Verarbeitung nicht einzuhalten.

### 2.2.4 Datenschutzrechtliche Verantwortlichkeit

Ist das Datenschutzrecht anwendbar, müssen die einzelnen Anforderungen der DS-GVO eingehalten werden – und zwar in erster Linie vom Verantwortlichen.[30] Die Frage der Verantwortlichkeit ist letztlich eine Art Verantwortungszuweisung. Geklärt werden soll, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und gegenüber wem die betroffenen

---

[29] S. *Schneider/Schindler*, ZD 2018, 463 ff. m.w.N. zur Diskussion und alternativen Lösungen.

[30] Die DS-GVO hat gegenüber dem bisherigen Datenschutzrecht deutlich mehr Pflichten, die auch den Auftragsverarbeiter treffen. Die zentrale Zuweisung erfolgt aber nach wie vor zum Verantwortlichen.

Personen ihre Rechte ausüben können.[31] Bliebe die Lage ungeklärt, so würden aller Voraussicht nach die datenschutzrechtlichen Regelungen unwirksam und die betroffenen Personen schutzlos bleiben.[32] Die Frage der Verantwortlichkeit sagt jedoch nur wenig über die Rechtmäßigkeit der Verarbeitung oder die Qualität und Quantität der zu ergreifenden Maßnahmen aus. Selbst wenn beispielsweise zwei Anbieter einer Datenbrille gemeinsam oder jeweils einzeln verantwortlich sind, kann es durchaus sein, dass ein Anbieter wesentlich strengeren Anforderungen genügen und dementsprechend wesentlich umfangreichere Maßnahmen als der andere Anbieter ergreifen muss.

#### 2.2.4.1 Gesetzliche Regelungen zu den einzelnen datenschutzrechtlichen Rollen

Bei einer Verarbeitung von personenbezogenen Daten besteht – wenn die DS-GVO anwendbar ist – in jedem Fall mindestens ein Verantwortlicher im datenschutzrechtlichen Sinne und mindestens eine betroffene Person. Ein *Verantwortlicher* ist nach Art. 4 Nr. 7 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die *betroffene Person* ist gemäß Art. 4 Nr. 1 DS-GVO diejenige (identifizierte oder identifizierbare) natürliche Person, auf die sich die personenbezogenen Daten beziehen.

Mit der technischen Entwicklung geht in vielen neuen Verarbeitungsszenarien auch eine rasante Vergrößerung der Anzahl an Beteiligten einher. So richtete im Gesundheitsbereich eine Behörde eine nationale Schnittstelle zur Regelung des Austauschs von Patientendaten zwischen Gesundheitsdiensten ein, an der Verantwortliche in einer fünfstelligen Zahl mitwirkten.[33] Sind an einer Datenverarbeitung auf der verarbeitenden Seite mehrere Parteien beteiligt, kommen noch weitere Beteiligungsformen außer der Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO in Betracht. So könnte eine *Auftragsverarbeitung* nach Art. 4 Nr. 8 DS-GVO vorliegen. Diese liegt vor, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Eine weitere mögliche Mitwirkung ist die *gemeinsame Verantwortlichkeit*, die ebenfalls in Art. 4 Nr. 7 DS-GVO erwähnt wird; hier sind mehrere Parteien für eine Verarbeitung datenschutzrechtlich gemeinsam verantwortlich.[34] Die letzte Möglichkeit ist die Beteiligungsform des Dritten nach Art. 4 Nr. 10 DS-GVO. *Dritter* ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Zusammenfassend können das Konsortium des Forschungsprojekts IDeA (sofern es hinreichend organisatorisch verselbstständigt ist) bzw. seine Mitglieder vier mögliche datenschutzrechtliche Rollen einnehmen:

- (Alleiniger) Verantwortlicher (Art. 4 Nr. 7 DS-GVO),
- Gemeinsam Verantwortlicher (Art. 4 Nr. 7 DS-GVO),
- Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) oder
- Dritter (Art. 4 Nr. 10 DS-GVO).

Eine andere Beteiligungsmöglichkeit an der Datenverarbeitung besteht nicht.

---

[31] *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 6, die zur DS-RL ergangen ist. Im Vergleich zur DS-GVO ergeben sich außer terminologischen keine darüber hinausgehenden Unterschiede.

[32] *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 9.

[33] *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 29.

[34] Die Norm des Art. 4 Nr. 7 DS-GVO wird durch Art. 26 DS-GVO ergänzt, der verfahrensrechtliche Voraussetzungen aufstellt.

Beteiligen sich mindestens zwei Parteien an einer Verarbeitung, so kommen dementsprechend (nur) drei Konstellationen in Betracht:

- Eine alleinige Verantwortlichkeit eines Beteiligten und eine Auftragsverarbeitung des anderen. Ein Verantwortlicher legt dabei die Zwecke und Mittel alleine fest. Der Auftragsverarbeiter hat keine (genügende) Entscheidungsbefugnis über Zwecke und Mittel der Verarbeitung.
- Eine gemeinsame Verantwortlichkeit. Beide Verantwortliche entscheiden gemeinsam über Zwecke und Mittel der Verarbeitung.
- Zwei alleinige Verantwortlichkeiten. Jede der Parteien entscheidet alleine über ihre Zwecke und Mittel der Verarbeitung.

#### 2.2.4.2 Abgrenzung der einzelnen Verantwortlichkeitsformen

Das entscheidende Kriterium zur Abgrenzung der einzelnen Verantwortlichkeitsformen ist gemäß der Legaldefinition in Art. 4 Nr. 7 DS-GVO die Entscheidung über Zwecke und Mittel.

Die Abgrenzung erfolgt dabei unter einer Gesamtschau aller – tatsächlicher, rechtlicher und vertraglicher – Umstände durch einen faktischen Ansatz.[35] Die Art-29-Datenschutzgruppe schlägt deshalb als Hilfestellung folgende Fragestellungen vor: „Warum wird diese Verarbeitung durchgeführt? Wer hat sie veranlasst? Bei wem liegt de facto die Verantwortlichkeit?“[36] Als Indikatoren kommen zudem der rein faktische Grad der tatsächlich ausgeübten Kontrolle, der vermittelte Eindruck sowie die daraus entstehenden berechtigten Erwartungen der betroffenen Personen in Betracht.[37]

##### 2.2.4.2.1 Alleinige Verantwortlichkeit

Verantwortlicher ist nach Art. 4 Nr. 7 DS-GVO „die natürliche oder juristische Person […], die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Die Entscheidung über die Mittel setzt sich aus solchen, die für den Zweck essenziell sind und solchen, die für diesen abdingbar sind zusammen. Die Entscheidung, welche genaue Software oder Hardware zur Datenverarbeitung genutzt wird, ist für den Verantwortlichen in den meisten Fällen eher delegierbar als die Frage, welche genauen Datenkategorien erfasst werden und wie diese ausgewertet werden sollen. Folglich führt eine gewisse Entscheidungsbefugnis über die Mittel nicht zwangsläufig zu einer Verantwortlichkeit, sondern kann eine andere Form der Beteiligung (z.B. Auftragsverarbeitung) darstellen. Die Entscheidung über den Zweck der Verarbeitung resultiert hingegen stets in einer Einstufung als Verantwortlicher.[38] Der Entscheidung über die Zwecke wird also eine höhere Bedeutung beigemessen als der Entscheidung über die Mittel.[39]

##### 2.2.4.2.2 Gemeinsame Verantwortlichkeit

Eine gemeinsame Verantwortlichkeit liegt nach Art. 26 Abs. 1 DS-GVO vor, sofern die Verantwortlichen gemeinsam über Mittel und Zwecke entscheiden. Wurde also in einem ersten Schritt festgestellt, dass über die Zwecke oder die entscheidenden Mittel entschieden wurde, ist in einem zweiten Schritt zu prüfen, ob diese Entscheidung gemeinsam erfolgte.

---

35 *Kremer*, CR 2019, 225 (227).

36 *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 11. Die Stellungnahme der Artikel-29-Datenschutzgruppe bezieht sich noch auf die DSRL. Die Erwägungen sind jedoch auch auf die DS-GVO übertragbar.

37 *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 14.

38 *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 17.

39 *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 17 f.

Die Beurteilung der gemeinsamen Entscheidung erfolgt entsprechend der über die alleinige Verarbeitung. Auch an dieser Stelle ist ein funktionaler Ansatz anzuwenden, der die tatsächlichen Umstände analysiert. Die tatsächlichen Umstände können jedoch durch die vertragliche Vereinbarung der Parteien beeinflusst werden, da es ihnen grundsätzlich frei obliegt, ihren jeweiligen Verantwortungsbereich abzugrenzen.[40] Verlässt die vertragliche Vereinbarung die Grenzen des rechtlich Zulässigen oder weicht sie von den tatsächlichen Abläufen ab, so verliert sie allerdings ihre beeinflussende Wirkung für die Bestimmung des Charakters.[41]

Der Grad der Beeinflussung der Datenverarbeitungsprozesse kann dabei bei jedem Verantwortlichen unterschiedlich sein.[42] Die Beziehung zwischen den jeweiligen Verantwortlichen kann dabei sehr vielfältig sein. So können die Zwecke oder die wesentlichen Mittel gemeinsam entschieden worden sein. Genauso kann sich eine gemeinsame Verantwortlichkeit bei einer Entscheidung nur über bestimmte Teile der Verarbeitung und ihre Zwecke oder wesentlichen Mittel ergeben. Für die Teile, über die nicht gemeinsam entschieden wurde, sind die jeweiligen Verantwortlichen dann alleine verantwortlich. Die gemeinsame Verantwortlichkeit wurde in der Entscheidung des EuGH in Sachen „Fashion-ID“ nämlich ausdrücklich auf diejenigen Vorgänge begrenzt, über die der jeweilige Verantwortliche tatsächlich (mit)entschieden hat.[43] Die Folge dieser neuen Tendenz der Rechtsprechung ist, dass nun alle Verarbeitungen genau auf die jeweiligen Verantwortlichkeiten geprüft werden müssen. Falls eine gemeinsame Verantwortlichkeit für zumindest gewisse Teile der Verarbeitung vorliegt, muss nach Art. 26 Abs. 1 und 2 DS-GVO eine Vereinbarung über die Verteilung der datenschutzrechtlichen Pflichten (v.a. Transparenzpflichten und Erfüllung der Betroffenenrechte) geschlossen werden. Die Benennung einer Anlaufstelle ist möglich, aber nicht verpflichtend. Die Vereinbarung muss die tatsächlichen Funktionen und Beziehungen der Beteiligten widerspiegeln.

Die Rechtsprechung legt den Begriff der gemeinsamen Verantwortlichkeit weit aus.[44] Der Sinn dieser weiten Interpretation ist der umfassende Schutz für die betroffenen Personen.[45] Gerade bei undurchsichtigen Datenverarbeitungen, an denen eine Vielzahl an Verarbeitern beteiligt sind, ist es für die betroffenen Personen schwierig, den juristisch richtigen Verantwortlichen zu finden. Eine rechtliche Geltendmachung der Rechte gegenüber den falschen (Nicht-)Verantwortlichen birgt ein Kostenrisiko für die betroffenen Personen und würde diese aufgrund dieser Unsicherheit oftmals von einer Geltendmachung abhalten.

Der EuGH differenziert bei der Beurteilung der Entscheidung über die Zwecke und wesentlichen Mittel zwischen der Entscheidung über die Zwecke und der über die wesentlichen Mittel. Eine gemeinsame Entscheidung über die wesentlichen *Mittel* liegt nach Auffassung des EuGHs vor, sobald ein subjektives und ein objektives Element vorliegen. Die Verantwortlichen müssen zum einen zumindest abstrakte Kenntnis über die wesentlichen Mittel (subjektives Element) haben. In dem Fall von Fashion-ID wusste der Websitebetreiber, dass Facebook das eingebundene Plug-In als Werkzeug zur Verarbeitung von personenbezogenen Daten der Websitebesucher nutzt.[46] Zum anderen müssen die Verantwortlichen einen „entscheidenden“ Beitrag zur Verarbeitung der personenbezogenen Daten leisten (objektives Element). Hierbei soll allerdings bereits eine bloße Ursächlichkeit genügen. Im Fall von Fashion-ID war dies gegeben:

---

40 *Schreiber*, ZD 2019, 55 (57).

41 Fraglich ist, ob hieraus eine Rechtswidrigkeit der Verarbeitung resultiert, da keine wirksame Vereinbarung nach Art. 26 Abs. 1 Satz 2 DS-GVO besteht. Dies vertritt zumindest *Schreiber*, ZD 2019, 55 (55).

42 *Kremer*, CR 2019, 225 (228).

43 EuGH, ZD 2019, 455 (457), Rn. 85.

44 EuGH, ZD 2018, 469; EuGH, ZD 2018, 357; EuGH, MMR 2019, 579.

45 *Gierschmann*, ZD 2020, 69 (70).

46 EuGH MMR 2019, 579 (582), Rn. 77.

Ohne eine Einbindung des Plug-Ins durch den Websitebetreiber wäre die Verarbeitung durch Facebook nicht möglich gewesen.

Eine gemeinsame Entscheidung über den *Zweck* liegt nach Auffassung des EuGHs vor, sofern drei Elemente kumulativ vorliegen: ein objektives und subjektives Element sowie ein Konnex zwischen den Zwecken.[47] Hinsichtlich der objektiven Voraussetzung reicht es aus, dass beide ein wirtschaftliches Interesse verfolgen. Das subjektive Element kann bereits vorliegen, wenn der eine Verantwortliche der Verarbeitung (zu diesen Zwecken) stillschweigend einwilligt. Ob nun eine Kenntnis des konkreten Zwecks erforderlich ist oder es genügt, dass der andere Verantwortliche abstrakt um die wesentlichen Zwecke Bescheid weiß, wird nicht genauer erläutert. Nicht zuletzt aufgrund der weiten Auslegung der gemeinsamen Verantwortlichkeit, ist im Zweifel davon auszugehen, dass eine Kenntnis um die abstrakten Zwecke genügt. Die beiden Zwecke muss zudem ein Konnex verbinden. Der wirtschaftliche Vorteil des einen muss nach dem EuGH das Gegenstück des wirtschaftlichen Vorteils des anderen bilden.[48]

#### 2.2.4.2.3 Auftragsverarbeitung

Ein Auftragsverarbeiter verarbeitet gem. Art. 4 Nr. 8 DS-GVO personenbezogene Daten im Auftrag des Verantwortlichen. Aus datenschutzrechtlicher Sicht handelt der Auftragsverarbeiter zur Erreichung des vom Verantwortlichen festgelegten Zwecks – mithin in seinem Interesse. Das wirtschaftliche (Eigen-)Interesse des Auftragsverarbeiters beschränkt sich dabei grundsätzlich auf die Erfüllung der Verpflichtungen gegenüber dem Verantwortlichen und die aus dieser Erfüllung resultierenden Vergütungsansprüche.[49] Dementsprechend treffen auch die datenschutzrechtlichen Verpflichtungen (z.B. die Betroffenenrechte) hauptsächlich den Verantwortlichen. Zur Verhinderung von möglichen Umgehungen durch geschickte Auslagerungen und eines daraus resultierenden Absinkens des Datenschutzniveaus, postuliert Art. 28 DS-GVO bestimmte Anforderungen an den Verantwortlichen und den Auftragsverarbeiter. So treffen den Verantwortlichen bestimmte Pflichten bei der Auswahl und Eignung der Auftragsverarbeiter sowie der Ausgestaltung des Auftragsverhältnisses. Da der Auftragsverarbeiter personenbezogene Daten – zwar im Auftrag des Verantwortlichen – verarbeitet, sind auch ihm im Vertrag gewisse datenschutzrechtlichen Pflichten aufzuerlegen. Diese bewegen sich insbesondere im Bereich der Vertraulichkeit und der Sicherheit der Verarbeitung (s. Art. 28 DS-GVO).[50] Darüber hinaus richten sich – anders als nach früherem Recht – etliche Pflichten explizit auch an den Auftragsverarbeiter.

Das entscheidende – aber gesetzlich nicht weiter erläuterte – Abgrenzungsmerkmal zwischen der Auftragsverarbeitung und der (alleinigen und gemeinsamen) Verantwortlichkeit ist mithin die fehlende Entscheidungsgewalt hinsichtlich des Zwecks und der tragenden Mittel.

#### 2.2.4.2.4 Abgrenzungskriterien

Nicht zuletzt aufgrund der immer verzwickteren Verflechtung der Parteien bei Verarbeitungen von personenbezogenen Daten können de lege lata die genauen Rollen nur im Einzelfall bestimmt werden. Um diesem zugegeben sehr pragmatischen Ansatz eine gewisse Orientierung zu geben, können aufgrund der aktuellen Rechtsprechung des EuGHs einige Orientierungspunkte zusammengefasst werden.

##### 2.2.4.2.4.1 Alleinige Verantwortlichkeit

Die alleinige Verantwortlichkeit zeichnen folgende zwingenden Kriterien aus:

---

47 S. hierzu ausführlicher *Lurtz*/*Schindler*, VuR 2019, 468 (474f.).

48 EuGH MMR 2019, 579 (582), Rn. 80.

49 Simitis/Hornung/Spiecker Döhmann-*Petri*, Art. 28 Rn. 3.

50 *Artikel-29-Datenschutzgruppe*, WP 169, 2010, 7.

- Das Verhältnis der Beteiligten ist frei von Weisungen.
- Zwecke und wesentliche Mittel werden nicht gemeinsam, sondern einzeln entschieden.

#### 2.2.4.2.4.2 Gemeinsame Verantwortlichkeit[51]:

Die gemeinsame Verantwortlichkeit zeichnen folgende zwingenden Kriterien aus:

- Das Verhältnis der Beteiligten ist frei von Weisungen.
- Zwecke und wesentliche Mittel werden gemeinsam entschieden.
- Der Zweck des einen (gemeinsamen) Verantwortlichen ist das (wirtschaftliche) Gegenstück des anderen.[52] So reicht es aus, wenn ein Verantwortlicher als „Gegenleistung" Daten bei kostenlosen Dienstleistungen erhält.[53]
- Die beiden Verantwortlichen verfolgen denselben Zweck, wobei das Eigeninteresse am Verarbeitungsziel ausreichen kann.[54]

Folgende Anhaltspunkte sprechen zudem für eine gemeinsame Verantwortlichkeit:[55]

- Der Zweck der Verarbeitung kann nur durch Kumulation aller Einzelbeiträge erreicht werden.
- Die Beteiligten sind nur gemeinsam in der Lage, allen Pflichten der DS-GVO nachzukommen. So kann beispielsweise eine Einwilligung für ein Social-Plug-In in einigen Fällen nur durch einen Websitebetreiber eingeholt werden, da der Plug-In-Betreiber im Zweifel gar nichts oder wenn überhaupt, nur nachträglich und damit zu spät von der Datenverarbeitung aufgrund der Einbindung des Plug-ins erfährt.

#### 2.2.4.2.4.3 Auftragsverarbeitung

Die Auftragsverarbeitung zeichnen folgende zwingenden Kriterien aus:

- Ein Beteiligter erteilt dem anderen Beteiligen eine Weisung oder unterliegt zumindest Bindungen hinsichtlich des Zwecks und der wesentlichen Mittel.
- Der Zweck wird von mindestens einem Beteiligten vorgegeben und mindestens ein Beteiligter hat keinen Einfluss auf den Zweck der Verarbeitung.
- Der Zweck der Verarbeitung steht nicht in Relation zu dem verfolgten Eigeninteresse. Weder stimmen sie überein, noch stehen sie in einem wechselseitigen Verhältnis oder der eine Zweck wird durch den anderen erst möglich gemacht. Es besteht zudem kein wirtschaftliches Interesse am Ergebnis der Verarbeitung.[56]
- Der Auftragsverarbeiter hat keinen Einfluss auf die Entscheidung über die Rechtsgrundlage.
- Es besteht kein Einfluss darauf, ob und an wen Daten übermittelt werden.
- Die Aufbewahrungsdauer der Daten wird nicht beeinflusst.

Die folgende Graphik des Europäischen Datenschutzbeauftragten (aus dem Englischen übersetzt) soll als Wegweiser zur Prüfung der Verantwortlichkeitsverteilung dienen.[57]

---

51 *Kremer*, CR 2019, 225 (228).

52 *Lurtz/Schindler*, VuR 2019, 468 (474 f.).

53 *Gierschmann*, ZD 2020, 69 (72).

54 *Gierschmann*, ZD 2020, 69 (72).

55 *Kremer*, CR 2019, 225 (228).

56 *Gierschmann*, ZD 2020, 69 (72).

57 Das Diagramm wurde auf Deutsch übersetzt, *EDPS* 2019, 32.

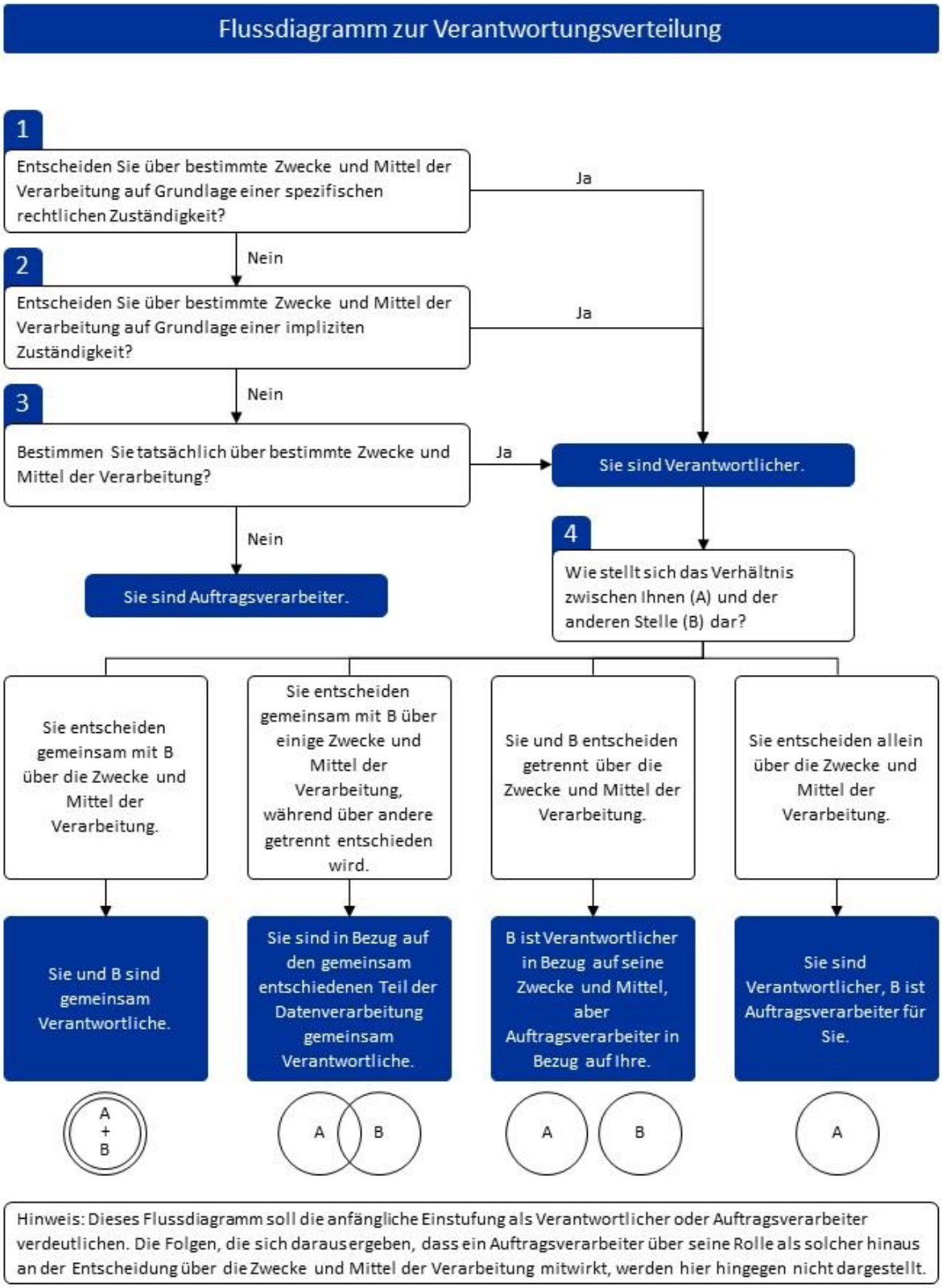



*Abbildung 1Flussdiagramm zur Verantwortlichkeitsverteilung des Europäischen Datenschutzbeauftragten (übersetzt)*

#### 2.2.4.3 Zwischenergebnis

Im Fall von Datenbrillen im Gesundheitsbereich bestehen drei denkbare Datenverarbeitungskonstellationen:

- Anbieter – Träger,
- Anbieter – Dritte und
- Träger – Dritte.

Innerhalb dieser Verarbeitungskonstellationen ist darüber hinaus in aller Regel das mögliche Verhältnis zwischen mehreren Anbietern zu unterscheiden. Es ist davon auszugehen, dass nicht nur ein Anbieter die gesamte Verarbeitung durchführt, sondern mehrere zusammenwirken. Wie diese Zusammenarbeit erfolgt, ist sehr unterschiedlich und kann nur im konkreten Einzelfall betrachtet werden. In dem Wissen, dass in der Praxis mehrere Beteiligte mitwirken, soll deshalb exemplarisch zwischen einem Anbieter der Software und einem Anbieter der Hardware unterschieden werden. Für das Verständnis der Verteilung der Verantwortlichkeit reicht hingegen diese Unterscheidung. Diese kann anschließend beliebig oft weiterentwickelt werden.

In dem Szenario entwickelt das Konsortium von IDeA die Software für die Datenbrille zur Unterstützung und Behandlung von AMD-kranken Personen. Diese Software wird auf der Hardware eines dritten (Hardware-)Anbieters betrieben. Der Hardwareanbieter wird sich dabei häufig nicht nur auf den Verkauf des Geräts beschränken, sondern mitunter eine oder mehrere Funktionalitäten bieten. So kann er Speicherplatz für die mittels der Brille erhobenen Daten zur Verfügung stellen oder die Daten in einer Cloud-Plattform analysieren.[58] Der Hardwareanbieter erhält dabei – sei es auch nur zur Produktoptimierung oder Wartung – Zugriff auf bestimmte Datenverarbeitungen durch die Datenbrille. Diese sind dem Softwarebetreiber und dem Träger nicht immer in voller Gänze bekannt. Demnach erfolgen sowohl Datenverarbeitungen des Softwareanbieters als auch des Hardwareanbieters.

Wenn der Hardwareanbieter in Bezug zu IDeA bezüglich eines Teils der Datenverarbeitung über die wesentlichen Mittel und Zwecke entscheidet, ist er auch Verantwortlicher. Dies gilt für die andere Seite entsprechend. Nur sobald der Softwareanbieter über die Zwecke und wesentlichen Mittel des Hardwareanbieters (mit-)entscheidet (sich also z.B. nicht auf die Analyse der Daten zu ihm vorgegebenen Zwecken beschränkt), kann eine Verantwortlichkeit für Datenverarbeitungen des Hardwareanbieters angenommen werden. Dies gilt jedoch nur für die Zwecke und Mittel, die sie jeweils kontrollieren können.[59] Verarbeitet beispielsweise der Hardwareanbieter ohne Wissen des Softwareanbieters personenbezogene Daten für andere Zwecke, so ist nur der Hardwareanbieter Verantwortlicher bezüglich dieser Verarbeitung, der Softwareanbieter hingegen nicht. Jedoch ist bei der Beurteilung der Rechtmäßigkeit im zweiten Schritt die Gefahr einer anderen Nutzung (erschwerend) zu berücksichtigen.[60] Je mehr der Softwareanbieter über die weiteren Datenverarbeitungen des Hardwareanbieters weiß, desto eher wird eine gemeinsame Verantwortlichkeit angenommen werden. Je weniger er weiß, desto höhere Anforderungen sind wiederum an die Rechtfertigung seiner (also des Softwareunternehmens) zu stellen (z.B. eine höhere Informationspflicht über mögliche weitere Datenverarbeitungen oder höhere Anforderungen an die Informiertheit einer Einwilligung).

---

58 Dasselbe gilt für den Software-Hersteller, d.h. seine Software ermöglicht ihm den Zugriff auf die gesamte Hardware oder Teile von ihr, und er erhält ebenfalls Daten zu Speicher- oder Analysezwecken.

59 EuGH, MMR 2019, 579 (582), Rn. 76.

60 S. Kap. 2.2.5.

### 2.2.5 Rechtfertigung der Datenverarbeitung(en)

Nach dem datenschutzrechtlichen Verbotsprinzip ist jede Datenverarbeitung verboten, außer sie wird durch eine Rechtsgrundlage ausdrücklich gerechtfertigt. Diese Rechtsgrundlagen finden sich in Art. 6 DS-GVO. Werden sensible Daten i.S.d. Art. 9 Abs. 1 DS-GVO verarbeitet, sind zusätzlich die strengeren Voraussetzungen des Art. 9 Abs. 2 DS-GVO zu beachten.

Der Betrieb einer Datenbrille (zu medizinischen Zwecken) besteht typischerweise aus mehreren Datenverarbeitungen. Diese erfolgen zu unterschiedlichen Zwecken, durch unterschiedliche Personen sowie in unterschiedlicher Art und Weise; sie unterliegen deshalb auch unterschiedlichen rechtlichen Anforderungen. Aus diesem Grund muss die datenschutzrechtliche Rechtfertigung für diese Zwecke, Verantwortlichen und Verarbeitungsformen jeweils getrennt erfolgen.

Bei dem Betrieb von Datenbrillen – auch zu medizinischen Zwecken – stellen sich drei Verarbeitungsrichtungen:

- Anbieter – Träger,
- Anbieter – Dritte und
- Träger – Dritte.

Die erste Verarbeitungsrichtung ist die Verarbeitung von personenbezogenen Daten des Trägers der Datenbrille durch den oder die Anbieter. Erfahrungsgemäß arbeiten bei dem Betrieb einer solchen Datenbrille zahlreiche Unternehmen zusammen; siehe hierzu in etwa die Aufgabenaufteilung des Forschungsprojekt IDeA. Jeder dieser Verantwortlichen bedarf einer Rechtfertigung für die jeweilige Datenverarbeitung. Die zweite Verarbeitungsrichtung betrifft die Verarbeitung der personenbezogenen Daten von Dritten, die von der Datenbrille durch Video- oder Audiogeräte erfasst werden. Die dritte Verarbeitungsrichtung betrifft ebenfalls die Verarbeitung der Daten der Dritten, diesmal jedoch durch den Träger der Datenbrille; in aller Regel handelt es sich dabei um einen Verbraucher, der die Brille weder zu kommerziellen noch zu wissenschaftlichen Zwecken nutzt.

#### 2.2.5.1 Anbieter – Träger

Die Datenbrille verarbeitet einerseits Daten der Umgebung (z.B. Räumlichkeiten, Personen oder sonstige Gegenstände) und andererseits Daten des Trägers. Letztere beziehen sich direkt auf seinen Körper und sind damit stets personenbezogen. Letztlich gilt aber dasselbe für viele Umgebungsdaten, weil sie z. B. über das persönliche Umfeld des Trägers Auskunft geben oder zumindest – wenn Standort- und Zeitinformationen verfügbar sind – seine Bewegung dokumentieren.

Im Verhältnis des Anbieters zum Träger der Datenbrille werden also zum einen die in Kap. 2.1 genannten Daten (z.B. Pupillendurchmesser, Anamnese der Augen oder Blutzucker) und zum anderen Umgebungsdaten etwa über die Wohnsituation, den sozialen Umgang oder Gewohnheiten verarbeitet. Letztere fallen schon in der Regel nicht unter. Art. 9 Abs. 1 DS-GVO. Zudem beschränkt sich die Verwendungsabsicht des Anbieters auf die Behandlung und Unterstützung des Patienten (Träger); die dabei miterfassten Daten über die Wohnung und darin befindlichen religiösen Symbole oder eine Teilnahme an einer Demonstration mögen zwar etwas über die religiöse Überzeugung oder die politische Meinung verraten, eine diesbezügliche Verwendungsabsicht liegt jedoch nicht vor.

Anders verhält es sich hinsichtlich der personenbezogenen Daten, die für die Behandlung und Unterstützung aufgrund der AMD-Erkrankung erhoben und weiterverarbeitet werden, wie etwa die unterschiedlichen Messwerte der Augen. Diese, wie auch eine Vielzahl der anderen

genannten Daten[61], beziehen sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, und aus ihnen gehen regelmäßig Informationen über deren Gesundheitszustand hervor, sodass offensichtlich Gesundheitsdaten i.S.d. Art. 4 Nr. 15 DS-GVO vorliegen. In diesem Fall besteht auch eine diesbezügliche Verwendungsabsicht des Anbieters der Datenbrille. Sensible Daten werden durch Art. 9 Abs. 1 DS-GVO besonders geschützt.[62] Dementsprechend bedarf es zu ihrer Rechtfertigung einer besonderen in Art. 9 Abs. 2 DS-GVO genannten Rechtsgrundlage.

Bei einer Datenverarbeitung durch eine Datenbrille im Gesundheitsbereich kommen grundsätzlich folgende Rechtsgrundlagen in Betracht:

- Ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO)
- Erforderlichkeit für die medizinische Diagnostik oder zur Versorgung oder Behandlung im Gesundheits- oder Sozialbereich (Art. 9 Abs. 2 lit. h DS-GVO)
- Erforderlichkeit für wissenschaftliche oder historische Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO)

#### 2.2.5.1.1 Ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO)

Eine Möglichkeit, die Datenverarbeitung zwischen dem Anbieter und dem Träger zu legitimieren, ist eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO.

Neben den allgemeinen Anforderungen an eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 7 und Art. 4 Nr. 11 DS-GVO sind nach Art. 9 Abs. 2 lit. a DS-GVO aufgrund der Schutzbedürftigkeit der sensiblen Daten besondere Anforderungen an die Einwilligung zu stellen. Die Einwilligung muss – wie stets – für einen oder mehrere festgelegte Zwecke festgelegt sein (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO). Sie muss zudem freiwillig und in informierter Weise abgegeben werden (Art. 4 Nr. 11 DS-GVO). Darüber hinaus verlangt Art. 9 Abs. 2 lit. a DS-GVO eine ausdrückliche Einwilligung; eine konkludent erteilte Einwilligung genügt mithin nicht. Obwohl weder Art. 9 Abs. 2 lit. a DS-GVO noch Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO eine Schriftform verlangen, ist dies mit Blick auf die Rechenschaftspflicht sehr zu empfehlen (zu den genauen Voraussetzungen und Ausgestaltung einer Einwilligung im medizinischen (Forschungs-)Bereich siehe Kap. 3.5).[63]

Für die ordnungsgemäße und vollständige Funktionsfähigkeit der Datenbrille zu medizinischen Zwecken ist eine Verarbeitung der in Kap. 2.1 genannten Daten unerlässlich. Der Träger einer solchen Datenbrille wird in aller Regel einer Datenverarbeitung seine Einwilligung erteilen, da er genau den Mehrwert wünscht, der nur durch diese Datenverarbeitung entsteht. Diese Annahme bestätigten die Erkenntnisse im Forschungsprojekt IDeA.

#### 2.2.5.1.2 Erforderlichkeit für wissenschaftliche Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO)

Auch ohne eine Einwilligung ist eine Verarbeitung von sensiblen Daten nach Art. 9 Abs. 2 lit. j DS-GVO i.V.m. § 27 Abs. 1 BDSG bzw. der entsprechenden landesrechtlichen Norm möglich, sofern die Verarbeitung für wissenschaftliche Forschungszwecke erforderlich sind und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

Wissenschaftliche Forschungszwecke im Sinne der DS-GVO sind dabei weit auszulegen und umfassen die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung (EG 159 Satz 2 DS-GVO). Das

---

61 S. umfassend Kap. 2.1.

62 S. hierzu Kap. 2.2.3.

63 Simitis/Hornung/Spiecker Döhmann-*Petri*, Art. 4 Rn. 33.

Forschungsprojekt IDeA zielt darauf ab, ältere Menschen mit Makuladegeneration bei der Bewältigung ihres Alltags zu unterstützen und ihre medizinische Behandlung zu optimieren. Dabei werden bisher unerforschte Methoden angewandt und miteinander kombiniert. Dementsprechend liegt ein wissenschaftlicher Forschungszweck für diejenigen Anbieter bzw. Forschungseinrichtungen vor, die die entsprechenden Zwecke verfolgen.

Art. 9 Abs. 2 lit. j DS-GVO eröffnet – unter anderem – dem nationalen Gesetzgeber die Möglichkeit eigene Regeln bezüglich dieser Materie zu treffen (sog. Öffnungsklausel).[64] Von dieser Möglichkeit haben die deutschen Gesetzgeber Gebrauch gemacht und mit § 27 Abs. 1 BDSG sowie entsprechenden Regelungen in den Landesdatenschutzgesetzen die Verarbeitung von sensiblen Daten für den Forschungsbereich geregelt.[65] Durch diese Privilegierung versucht der Gesetzgeber dem erhöhten Bedarf der wissenschaftlichen Forschung (gerade im medizinischen Bereich) an einer erhöhten Anzahl an sensiblen Daten gerecht zu werden. Um jedoch den Schutz der sensiblen Daten nicht zu vernachlässigen, stellt der Gesetzgeber besondere Anforderungen an die Verarbeitung. Nach Art. 9 Abs. 2 lit. j i.V.m. 89 Abs. 1 Satz 1 und 2 DS-GVO muss eine solche Verarbeitung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung unterliegen. Mit diesen Garantien soll sichergestellt werden, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird (z.B. Pseudonymisierung). § 27 BDSG konkretisiert diese Anforderungen und verlangt unter anderem in Absatz 3 Satz 1 eine Anonymisierung, sobald dies nach dem Forschungszweck möglich ist, es sei denn berechtigte Interessen stehen entgegen. Eine Veröffentlichung ist nur bei Einwilligung der Betroffenen möglich. Es kann hingegen vorkommen, dass der Forschungszweck es erforderlich macht, Daten betroffenen Personen zuzuordnen.[66] Sich über lange Zeiträume erstreckende (Langzeit-)Studien sind nur durch die langfristige Konsultation der betroffenen Personen möglich.[67] In diesem Fall ist eine Anonymisierung nicht möglich, ggf. aber eine Pseudonymisierung.

Die Verarbeitung muss darüber hinaus erforderlich sein und die Interessen des Verantwortlichen an der Verarbeitung müssen die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

Die Verarbeitung ist erforderlich, sofern kein gleich geeignetes, weniger belastendes Mittel zur Erreichung des Forschungszwecks besteht. Dies kann u.a. eine Verarbeitung von anonymen oder pseudonymen Daten sein.

Für die Erreichung des Zwecks der Unterstützung von älteren Personen mit Makuladegeneration bei der Bewältigung ihres Alltags und der Optimierung der medizinischen Behandlung dieser Krankheit bedürfen die einzelnen Elemente der Anwendung in IDeA der Verarbeitung von einer Vielzahl an personenbezogenen Daten. Dabei bedarf die Behandlungs- und Trainingsfunktion unter anderem der einzelnen Informationen der aktuellen und vergangenen Augeneigenschaften. Nur durch diese Informationen kann das Fixationstraining durchgeführt werden. Für das Fixationstraining sind in einigen Fällen auch Informationen der Umgebung

---

64 Es ist umstritten, ob § 27 BDSG eine eigene Rechtsgrundlage darstellt oder lediglich die Voraussetzungen der Verarbeitung in diesem Bereich konkretisiert und auf eine andere Rechtsgrundlage (i.d.R. Art. 6 Abs. 1 UAbs. 1 lit. f) gestützt werden muss. Im Ergebnis läuft dies jedoch auf dasselbe Ergebnis hinaus, da beide Nomen eine Erforderlichkeitsprüfung mit einer Interessenabwägung voraussetzen und diese identisch ausfallen wird. S. hierzu genauer, BeckOK Datenschutzrecht-*Schlösser-Rost,* § 27 BDSG Rn. 4 ff. m.w.N.

65 Neben der Norm des § 27 BDSG bestehen auch weitere landesrechtliche Normen, die auf Art. 9 Abs. 2 lit. j DS-GVO fußen und damit ebenfalls eine mögliche Rechtsgrundlage sein können. Öffentliche Stellen (z.B. Hochschulen) des Landes können sich auf die Landesdatenschutzgesetze stützen. So bietet das Hessische Datenschutzgesetz in § 43 HDSIG eine Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten.

66 BeckOK Datenschutzrecht-*Schlösser-Rost,* § 27 BDSG Rn. 38.

67 *Herbst,* DuD 2016, 371 (374).

erforderlich, da diese durch die Software zu Trainingszwecken manipuliert werden. Das Forschungsergebnis der Optimierung der Behandlung und der Verbesserung der Unterstützung der Kranken kann in diesem Fall nur dadurch erreicht werden, dass die Entwicklung der Erkrankung eines konkreten Patienten über einen gewissen Zeitraum beobachtet wird. Nur so kann bspw. die Software des Fixationstrainings optimiert und optimiert werden. Für diese Anwendung ist es hingegen nicht erforderlich, dass die Identität des konkreten Patienten bekannt ist. Es genügt vielmehr, wenn die Software den Verlauf einem bestimmten Pseudonym zuordnen kann.

Eine Übermittlung der personenbezogenen Daten an weitere Verantwortliche (z.B. Augenarzt, Optiker oder Hausarzt) ist nur insoweit für die Erreichung der wissenschaftlichen Zwecke erforderlich, als das Forschungsergebnis nicht durch mildere Mittel erreicht werden kann. Gerade im medizinischen Forschungsbereich erscheint eine Zusammenarbeit mit medizinischem Fachpersonal für die Validierung der Forschungsergebnisse aufgrund der genaueren medizinischen oder praktischen Kenntnisse unerlässlich. Hierbei ist jedoch nach den für den jeweiligen Verantwortlichen notwendigen Daten(-kategorien) und den Datenempfängern zu differenzieren. Eine Übermittlung der genauen Fixationsdaten an den Augenarzt und Optiker ist dem Forschungszweck dienlich, da die Daten auf ihre Aussagekraft und Sinnhaftigkeit überprüft, die Ergebnisse bewertet und zudem Verbesserungsvorschläge hinsichtlich der Messmethoden gemacht werden können. Eine Übermittlung an den Hausarzt wird für die wissenschaftliche Forschung hingegen voraussichtlich nur wenig Erkenntnisse bringen, weswegen diesbezüglich eine Erforderlichkeit nicht vorliegen wird.

Ein milderes Mittel im Bereich der medizinischen Forschung ist eine Trennung von identifizierenden Daten und medizinischen Daten.[68] Durch ein Rollenkonzept kann dem medizinischen Fachpersonal ein umfassender Zugriff ermöglicht werden, während der Zugriff durch das technische Personal, das nur die Funktionalität einer Anwendung bearbeitet, auf einen für diesen Arbeitsschritt erforderlichen Zugriff beschränkt wird.

Nach der Erforderlichkeitsprüfung müssen im Rahmen der Abwägung die Interessen des Verantwortlichen an der Verarbeitung den Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Auf der einen Seite stehen das generelle wissenschaftliche Interesse – mit der dahinter stehenden Forschungsfreiheit – sowie das konkrete Ziel des Forschungsvorhabens mit einer möglichen Bedeutung für das Gemeinwohl (gerade im Bereich der medizinischen Forschung, vgl. EG 157 DS-GVO).[69] Auf der anderen Seite steht das allgemeine Persönlichkeitsrecht in Form der informationellen Selbstbestimmung der betroffenen Personen. Aufgrund der Sensibilität, die in Art. 9 Abs. 1 DS-GVO besonderen Schutz erfährt, ist der Schutzbedarf grundsätzlich sehr hoch. Zwischen diesen beiden Interessen muss eine Abwägung im Einzelfall vorgenommen werden, wobei diese „erheblich" zugunsten der Interessen des Verantwortlichen ausfallen muss.[70] Im Rahmen der wissenschaftlichen Forschung erscheint dies zwar nicht ausgeschlossen, aber durchaus als erhebliche Hürde. Wenn ein Verantwortlicher sich nicht auf dieses Risiko einlassen möchte, sollte er den bereits beschriebenen Weg einer ausdrücklichen Einwilligung wählen. In den IDeA-Szenarien sollte dies möglich sein, da ohnehin ein individueller Kontakt zu den Trägern besteht.

---

68 *Pommerening*/*Müller* 2014, 64 f.

69 BeckOK Datenschutzrecht-*Schlösser-Rost*, § 27 BDSG, Rn. 31.

70 BeckOK Datenschutzrecht-*Schlösser-Rost*, § 27 BDSG, Rn. 33.

#### 2.2.5.1.3 Erforderlichkeit für die medizinische Diagnostik oder zur Versorgung oder Behandlung im Gesundheits- oder Sozialbereich (Art. 9 Abs. 2 lit. h DS-GVO)

Eine weitere Möglichkeit stellt die Legitimation aufgrund der Erforderlichkeit für die medizinische Diagnostik oder zur Versorgung oder Behandlung im Gesundheits- oder Sozialbereich nach Art. 9 Abs. 2 lit. h DS-GVO dar.

Die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich umfasst im Wesentlichen alle gesundheitsbezogenen Leistungen. Sowohl präventive, diagnostische als auch nachsorgende gesundheitsbezogene Leistungen sind vom Tatbestand des Art. 9 Abs. 2 lit. h DS-GVO erfasst. Die Diagnostik ist eine Untergruppe von medizinischen Behandlungen und wird rein klarstellend gesondert erwähnt.[71] Die altersbedingte Makuladegeneration ist eine Augenkrankheit und damit im Gesundheitsbereich anzusiedeln. Durch die Behandlungs- und Trainingsfunktion der Anwendung in IDeA sollen an AMD erkrankte Personen versorgt und behandelt werden. Wenn der Anbieter also diese Zwecke verfolgt, ist eine Zulässigkeit auf Basis von Art. 9 Abs. 2 lit. h DS-GVO möglich.

Auch diese Norm eröffnet dem nationalen Gesetzgeber die Möglichkeit, eigene Regeln bezüglich dieser Materie zu treffen (sog. Öffnungsklausel). Die deutschen Gesetzgeber haben von der Öffnungsklausel durch die Verabschiedung des § 22 Abs. 1 Satz 1 lit. b BDSG und entsprechenden Regelungen in den Landesdatenschutzgesetzen Gebrauch gemacht und unter anderem den Bereich der medizinischen Diagnostik sowie der Versorgung oder Behandlung im Gesundheitsbereich geregelt. Neben diesen Normen bestehen im deutschen Gesundheitsdatenschutzrecht noch weitere Normen, die manche Bereiche speziell und vorrangig regeln. Die verdrängende Wirkung dieser Spezialgesetze reicht jedoch nur soweit, wie sie die Materie tatsächlich regeln. Wird nur die materiell-rechtliche Zulässigkeit geregelt, müssen die prozeduralen Voraussetzungen des § 22 BDSG weiter beachtet werden.[72] So bemisst sich eine Datenverarbeitung in Krankenhäusern nach Landeskrankenhausgesetzen oder bei kirchlicher Trägerschaft nach kirchlichem Recht.[73] Daneben bestehen noch weitere spezifische Datenschutzregelungen im Medizinrecht (z.B. TPG, MPG, InfSchG).

Die entscheidende Voraussetzung ist in allen Fällen die Erforderlichkeit für die medizinische Diagnostik oder Versorgung oder Behandlung im Gesundheitsbereich. Folglich dürfen keine milderen Mittel zur Erreichung dieses Zwecks vorliegen. Um eine möglichst effektive und individuelle Behandlung der Patienten zu gewährleisten, erscheint es erforderlich, aktuelle und individuelle Gesundheitsdaten zu verarbeiten. Auch erscheint es ebenfalls erforderlich, ältere Gesundheitsdaten zu speichern, um so den Krankheitsverlauf beobachten zu können.

An dieser Stelle ist nochmal genau zu prüfen, ob wirklich alle erhobenen personenbezogenen Daten für den Zweck der Behandlung und Versorgung des Betroffenen erforderlich sind. Offensichtlich erforderlich sind alle Daten, die die Sehfähigkeit des Betroffenen betreffen. Für die Unterstützungs-, Trainings- und Diagnosefunktion dürfte es hingegen beispielsweise nicht erforderlich sein, zu wissen ob und wie viel der Betroffene raucht. Denkbar ist, dass diese Information zu Forschungszwecken relevant ist und dann auf die entsprechenden Rechtsgrundlagen gestützt werden kann.

Die Übermittlung der personenbezogenen Daten an Ärzte (z.B. Augenarzt und Hausarzt) sowie an weiteres medizinisches Fachpersonal (z.B. Optiker) ist für die Behandlung der Patienten erforderlich. Hierbei ist die Identität des Patienten zur Betrachtung des Krankheitsverlaufs über

---

71 Simitis/Hornung/Spiecker Döhmann-*Petri*, Art. 4 Rn. 83.

72 BeckOK Datenschutzrecht-*Albers/Veit*, § 22 BDSG Rn. 7; Kühling/Buchner/*Weichert*, Art. 9 Rn. 168 ff.

73 Kühling/Buchner-*Weichert*, Art. 9 Rn. 170 ff.

einen längeren Zeitraum und für Rückfragen erforderlich. Ein milderes Mittel, wie eine Pseudonymisierung, ist nicht ersichtlich.

Eine weitere Bedingung ist der Geheimhaltungsschutz in § 22 Abs. 1 Nr. 1 lit. b und c BDSG. Es wird eine Verarbeitung durch Fachpersonal vorausgesetzt, das einer besonderen Geheimhaltungspflicht unterliegt. Im Gegensatz zur Vorgängerregelung in Art. 8 Abs. 3 DSRL verlangt Art. 9 Abs. 3 DS-GVO nicht mehr generell die Verarbeitung durch ärztliches Personal.[74] Voraussetzung ist lediglich die fachliche Eignung für die Handlung und eine Geheimhaltungspflicht.

#### 2.2.5.1.4 Zwischenergebnis

Eine Verarbeitung von Gesundheitsdaten des Trägers der Datenbrille ist vorliegend grundsätzlich nach allen Rechtsgrundlagen möglich.

Die einfachste und empfehlenswerteste Methode ist dabei die Einwilligung. Sie bietet den Vorteil einer Erlaubnis der umfassenden Datenverarbeitung ohne die Einhaltung von speziellen normierten Pflichten (z.B. § 22 Abs. 2 BDSG). In aller Regel wird eine Einwilligung der Träger aufgrund ihres intrinsischen Interesses an der Datenverarbeitung, durch die letztlich die Funktion und damit die Behandlung und Unterstützung erst ermöglicht wird, relativ leicht zu erlangen sein.

Auch eine Rechtfertigung über die gesetzlichen Tatbestände des Art. 9 Abs. 2 lit. h i.V.m. § 22 BDSG und Art. 9 Abs. 2 lit. j i.V.m. § 27 BDSG (bzw. die jeweiligen landesrechtlichen Grundlagen) ist möglich. Diese Wege erfordern hingegen das Vorliegen eines entsprechenden Forschungs- oder Behandlungszwecks durch den konkret beteiligten Verantwortlichen sowie die Einhaltung von speziellen Voraussetzungen, die im Ergebnis mehr Aufwand erfordern als eine Einwilligung. Innerhalb dieser beiden Tatbestände erscheint der Weg über Art. 9 Abs. 2 lit. h i.V.m. § 22 BDSG einfacher und sicherer, da hier insbesondere kein erhebliches Überwiegen der Interessen vorliegen muss.

### 2.2.5.2 Anbieter – Dritte

Die Datenbrille verarbeitet auch personenbezogene Daten von anderen Personen als dem Träger – also von mitunter unbekannten Dritten. Gerade für die Nutzung der Unterstützungsfunktion wird die Brille auch außerhalb der Wohnung des Trägers genutzt und die Video- und Audiofunktion erfasst auch personenbezogene Daten von meist unbekannten Dritten. So werden im Rahmen der Unterstützungsfunktion der Datenbrille beispielsweise bei der Erkennung einer Ampel auch die Passanten im Blickfeld der Kamera der Brille erfasst.

Die womöglich (mit-)erhobenen Daten, könnten zwar prima facie als sensible Daten auch unter Art. 9 DSGVO fallen (weil sie beispielsweise auf die Religionszugehörigkeit schließen lassen). Wie bereits erläutert, ist die Anwendung der Norm aber mangels diesbezüglicher Verwendungsabsicht abzulehnen.[75]

#### 2.2.5.2.1 Untauglichkeit von Einwilligungen

Eine mögliche Rechtsgrundlage ist die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO. Eine Einwilligung ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung der betroffenen Person in Form einer

---

74 Simitis/Hornung/Spiecker Döhmann-*Petri*, Art. 4 Rn. 89.

75 S. hierzu Kap. 2.2.3. Sollen hingegen sensible Daten bewusst verarbeitet werden, etwa zur Analyse von Emotionen Dritter, sind die strengen Anforderungen des Art. 9 DS-GVO zu beachten. In diesem Szenario müssten, wie auch in Kap. 2.2.5.1, mögliche Ausnahmetatbestände in Art. 9 Abs. 2 DS-GVO gesucht werden. Die einfachste Möglichkeit ist eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO, was einen solchen Anwendungsfall auf einen dem Träger bekannten Personenkreis einschränken würde.

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 (Art. 4 Nr. 11 DS-GVO).

Für den Fall von Datenbrillen eignet sich die Einwilligung insbesondere aus faktischen Gründen jedenfalls nicht allgemein. Eine Einwilligungserklärung ist im Voraus einzuholen,[76] und zwar von allen betroffenen Personen. Die Ermittlung und Kontaktierung aller Personen werden sich als undurchführbar erweisen. Dies gilt schon für bekannte Personen, erst recht aber für zufällig aufgenommene Passanten. Darüber hinaus ist aufgrund der Erfahrungen mit Datenbrillen in der Öffentlichkeit davon auszugehen, dass die meisten Personen nicht einwilligen werden.[77] Allenfalls in eng begrenzten Anwendungsszenarien (Brillenträger verlässt den häuslichen Bereich nicht und trifft dort nur auf einen kleinen Kreis bekannter Personen) kann mit der Einwilligung gearbeitet werden.

#### 2.2.5.2.2 Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO (legitime Interessen)

Die maßgebliche Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten der Umgebung durch Datenbrillen ist Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Dieser erlaubt die Verarbeitung, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Diese Norm ist für die Praxis neben der Einwilligung die wichtigste Rechtsgrundlage. Stärke, aber auch gleichzeitig Schwäche dieses Erlaubnistatbestandes ist seine Offenheit und Flexibilität.[78]

##### 2.2.5.2.2.1 Erforderlichkeit

Die Datenverarbeitung muss nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich sein.

Die erste Anforderung der Norm ist also ein berechtigtes Interesse, wobei sich dieses sowohl auf den Verantwortlichen (hier der Anbieter) als auch auf einen Dritten (hier insbesondere der Träger) beziehen kann. Der Begriff des berechtigten Interesses ist dabei sehr weit zu verstehen. Neben rechtlichen und wirtschaftlichen sind auch ideelle Interessen umfasst.[79] Das Interesse an der medizinischen Behandlung der Personen mit Makuladegeneration ist als berechtigt zu bewerten, zumal es Teil des grundrechtlichen geschützten Recht auf Unversehrtheit (Art. 3 GRCh) ist. Zudem kann sich das Interesse an der Unterstützung bei der Bewältigung des Alltags der sichtbeschränkten Erkrankten auf die Würde des Menschen (Art. 1 GRCh) stützen, nach der es jedem Menschen ermöglicht werden soll, selbstbestimmt zu leben. Das wirtschaftliche Interesse der Betreiber von Datenbrillen zur Verwirklichung ihres Geschäftsmodells ist als Teil der grundrechtlich geschützten unternehmerischen Freiheit (Art. 16 GRCh) ebenfalls als berechtigt zu bewerten. Das darüberhinausgehende (sekundäre) gesellschaftliche Interesse an der medizinischen Weiterentwicklung, das letztlich der Gesellschaft als Ganzes zugutekommt, ist als ideelles Interesse ebenfalls zu berücksichtigen.

Die zweite Anforderung ist die Erforderlichkeit der Datenverarbeitung zur Wahrung des berechtigten Interesses. Sie ist erforderlich, wenn kein geeignetes und milderes Mittel zur

---

76 Paal/Pauly-*Ernst*, Art. 4 DS-GVO Rn. 64.

77 https://www.sueddeutsche.de/digital/datenbrille-google-fuerchtet-glassholes-1.1892992.

78 Simitis/Hornung/Spiecker gen. Döhmann-*Schantz*, Art. 6 Abs. 1 DS-GVO Rn. 86.

79 Simitis/Hornung/Spiecker gen. Döhmann-*Schantz*, Art. 6 Abs. 1 DS-GVO Rn. 98.

Umsetzung des berechtigten Interesses verfügbar ist,[80] dieses also beispielsweise nicht mit anonymisierten Daten erreicht werden kann.[81]

Der Zweck der Erhebung der Daten besteht neben der möglichst frühzeitigen Diagnose der Erkrankung bzw. das frühzeitige Erkennen der Entwicklungen der fortschreitenden Krankheit, auch in dem Training zur Verbesserung der Sicht sowie die Assistenzfunktion zur besseren Alltagsbewältigung.

Alle diese Verwendungszwecke sind nicht nur auf eine möglichst vollständige Erfassung der Gesundheitsdaten des Trägers angewiesen, die bereits unter 2.2.5.1 behandelt wurde. Vielmehr ist insbesondere die Verbesserung der Sicht und die Assistenzfunktion in Alltagssituationen nur möglich, wenn die Brille in – grundsätzlich beliebigen – derartigen Situationen getragen wird und dabei das jeweilige Umgebungssetting, in dem der Träger sich befindet, ebenfalls erfasst wird. So erfordert etwa die Unterstützung bei alltäglichen Handlungen wie dem Lesen von Verpackungen in einem Supermarkt durch die Vergrößerung von Objekten die Erhebung von Umgebungsdaten. Da vielfach nicht vorher klar sein wird, welche Form der Unterstützung der Träger benötigt, erfordert eine flexible und optimale Erbringung der Unterstützungsleistung eine möglichst vollständige Erhebung der Umgebungsdaten. Wurde die (unterstützte) Handlung des Trägers beendet, bedarf es hingegen keiner Assistenzhandlung mehr, sodass dann auch keine Erforderlichkeit für eine weitere Verarbeitung (z.B. Speicherung) für diesen Zweck vorliegt. Eine technische Ausgestaltungsmöglichkeit zur Löschung der nicht mehr erforderlichen Daten wäre die Nutzung eines Ringpuffers (s. in etwa bei Dash-Cams).

Freilich bedarf der Augenarzt diese Daten, um sich z. B. in ihre egozentrische Perspektive hineinzuversetzen und mit Hilfe von Overlay-Visualisierungen die Blickstrategien schnell und intuitiv zu analysieren. Will der Träger nun solche Situationen speichern und dem Augenarzt zur Verfügung stellen oder gar eine Echtzeitübertragung herstellen, so kann der Träger durchaus darauf verwiesen werden, solche Verarbeitungen in einer abgeschlossenen privaten Umgebung durchzuführen, in der keine Rechte Dritter beeinträchtigt werden. Der Zweck kann in diesem Fall auch durch ein milderes Mittel erreicht werden.

#### 2.2.5.2.2.2 Abwägung

Der nächste Prüfungsschritt des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist eine umfassende Interessenabwägung. Diese wird nach dem Vorstehenden relevant, soweit die Verarbeitung der Daten von Dritten erforderlich ist (also zur kurzzeitigen Speicherung im Rahmen eines Ringpuffers).

Die Datenverarbeitung ist nur zulässig, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Letztlich befinden sich damit in der Waagschale des Verantwortlichen seine legitimen wirtschaftlichen Interessen (unternehmerische Freiheit, Art. 16 GRCh), insbesondere aber die Interessen der Brillenträger (Recht auf Unversehrtheit aus Art. 3 GRCh sowie Würde des Menschen nach Art. 1 GRCh). Auf der Seite der betroffenen Personen befinden sich insbesondere das Persönlichkeitsrecht sowie die Auswirkungen, die eine Verarbeitung für diese mit sich bringt (Art. 7 und 8 GRCh). Diese Interessen müssen in einer eigenständigen und eigenverantwortlichen Abwägung mit den Interessen des Verarbeiters zueinander ins Verhältnis gesetzt werden.

Folgende Abwägungskriterien beeinflussen die Erhebung von personenbezogenen Daten bei Datenbrillen (nicht nur für medizinische Zwecke):

2.2.5.2.2.2.1 Art und Umfang der Daten

---

80 Auernhammer-*Kramer*, Art. 6 DS-GVO Rn. 17.

81 *Wolff* in Schantz/Wolff 2017, Rn. 647.

Zunächst ist festzuhalten, dass Video- und Audioaufnahmen in diesem Anwendungsfall i.d.R. keine sensiblen Daten i.S.d. Art. 9 DS-GVO sind.[82] Eine besondere Schutzbedürftigkeit aufgrund der Art der Daten ergibt sich nicht.

Eingriffserhöhend wirkt die potenziell erhebliche Streubreite des Eingriffs.[83] Durch die Nutzung einer Datenbrille in der Öffentlichkeit werden eine große Zahl an Grundrechtsträgern einem Eingriff ausgesetzt sein. Selbst bei individuell betrachtet geringfügigen Eingriffen ergibt sich aufgrund der massenhaften Erfassung auch eine entsprechende Zahl an Grundrechtsverletzungen.[84]

Ferner haben die Betroffenen keinerlei zurechenbaren Anlass für eine Datenerhebung gegeben.[85] Die Nutzung von Datenbrillen erfolgt in den allermeisten Fällen ohne ausdrückliches, mutmaßliches oder konkludentes Näheverhältnis zu den Betroffenen.[86]

2.2.5.2.2.2.2 Charakter als öffentlich zugängliche Daten

Obwohl öffentlich zugängliche Daten im Gegensatz zur alten Rechtslage nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG a.F. und § 29 Abs. 1 Satz 1 Nr. 2 BDSG a.F. keine explizite normative Privilegierung mehr erfahren, ist diese Eigenschaft dennoch i.R.d. Abwägung des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zu berücksichtigen.[87]

Hintergrund ist die andere Erwartung der betroffenen Personen, die jedenfalls faktisch keine Erwartung mehr haben (können), dass die Daten vertraulich bleiben. Vielmehr rechnen sie, dass die Informationen in der Öffentlichkeit von anderen wahrgenommen werden. Hieraus folgt jedoch nicht, dass öffentlich zugängliche Daten zu beliebigen Zwecken nutzbar sind.[88]

2.2.5.2.2.2.3 Modalitäten der Datenerhebung

Die Modalitäten der Datenverarbeitung wirken sich ebenfalls auf die Abwägung aus. Eingriffserhöhend ist die fehlende Transparenz von Datenbrillen zu berücksichtigen. Typischerweise erkennen Dritte (z.B. Passanten) erst gar nicht, dass ihre personenbezogenen Daten durch die Datenbrille verarbeitet werden.[89] Selbst wenn sie die Datenbrille und die damit einhergehende Datenverarbeitungsmöglichkeit erkennen, bleibt die genaue Art der Verwendung verschleiert. Ob das von der betroffenen Person gemachte Bild nur für die Trainingsfunktion erhoben und sodann umgehend gelöscht wird oder aber nachträglich weiterverarbeitet, womöglich sogar veröffentlicht wird, ist für den Betroffenen nicht ersichtlich.

Darüber hinaus wirkt sich auch die Visualisierungsperspektive eingriffserhöhend aus. Durch Datenbrillen werden Bilder aus frontaler Perspektive und oftmals aus unmittelbarer Nähe aufgenommen. Diese erlauben Rückschlüsse über Emotionen und Krankheiten des Gegenübers.

---

82 S. Kap. 2.2.3.

83 Schweizerisches Bundesgericht, Urteil vom 31.5.2012, 1C_230/2011, EuGRZ 2012, 522, unter 10.6.1; *Spiecker gen. Döhmann*, CR 2010, 311 (316); *Dreier/Spiecker gen. Döhmann* 2010, 92 f., 99 f.; *Klar* 2012, 90, 215 f.; das BVerfG verwendet dieses Kriterium sehr oft, s. z.B. zur Kfz-Kennzeichenerfassung BVerfGE 120, 378.

84 *Herfurth*, ZD 2018, 514 (517); s. u.a. BVerfGE 115, 320.

85 *Lindner*, ZUM 2010, 292 (293); *Dreier/Spiecker gen. Döhmann* 2010, 93; *Klar* 2012, 215 f.

86 *Spiecker gen. Döhmann*, CR 2010, 311 (316); *Dreier/Spiecker gen. Döhmann* 2010, 94; zum Kriterium s. u.a. BVerfGE 120, 378, Rn. 78.

87 Ebenso Simitis/Hornung/Spiecker gen. Döhmann-*Schantz*, Art. 6 Abs. 1 DS-GVO Rn. 131 m.w.N.; Gola et al.- *Schulz*, Art. 6 DS-GVO Rn. 53; Plath-*Plath*, Art. 6 DS-GVO Rn. 21.

88 *Spiecker gen. Döhmann*, CR 2010, 311 (315), wonach der Mensch als soziales Wesen zwangsläufig Informationsgeber ist, weshalb die Informationen, die ohnehin jedermann zugänglich sind, einen geringeren Schutz genießen sollen.

89 *Spiecker gen. Döhmann*, CR 2010, 311 (316 f.); s.a. *Klar* 2012, 89 f.

Zudem kommt erschwerend hinzu, dass aufgrund der Möglichkeit der Echtzeitübertragung die Daten an Dritte übertragen werden können und eine Verbreitung der Daten damit ggf. nicht kontrolliert werden kann. In dem geplanten Szenario der Unterstützung des Trägers durch eine nahe Bezugsperson bei bestimmten den Träger überfordernden Tätigkeiten (z.B. PIN-Eingabe bei einem Einkauf oder Überquerung einer unübersichtlichen Straße) ist es nicht auszuschließen, dass die Bezugspersonen die Daten verbreiten.

Die Gefahr der zweckfremden Nutzung durch den Träger in Form einer weiteren Datenverwendung (z.B. Veröffentlichung) nach der Datenerhebung hat ebenfalls einen Einfluss auf die Eingriffsintensität. Erfolgt die weitere Verarbeitung – wie hier – lediglich für interne Zwecke innerhalb des oder der Verantwortlichen, idealerweise innerhalb eines eingeschränkten Bearbeiterkreises und abgesichert durch technische und organisatorische Maßnahmen, so hat nur eine kleiner Personenkreis Zugang zu den Daten. Dieser Personenkreis hat im Fall von IDeA auch ein berechtigtes und abgrenzbares Interesse an der Verarbeitung Informationen. Werden also die erhobenen Daten lediglich für die Forschungszwecke von IDeA, für die Behandlung und Unterstützung des Trägers sowie für die Wartung und Verbesserung der Funktionen der Datenbrille verwendet, wird sich dies zugunsten des Verantwortlichen auswirken.

Besteht hingegen die Gefahr, dass der Träger durch eine externe Verwendung (z.B. Veröffentlichung oder Weitergabe an andere Verantwortliche), die Informationen einer mitunter nicht vorhersehbaren Vielzahl an Personen zugänglich macht, ist dies eingriffserhöhend zu berücksichtigen. Eine solche Verwendung ist eingriffsintensiver als die bloß interne Verwendung. Nicht zuletzt durch das grenzenlose Medium des Internets ist sind die Wahrnehmbarkeit der Informationen und die Einsatzmöglichkeiten der Daten äußerst umfangreich.[90] Werden die Daten im Internet veröffentlicht sind die Verwendungsmöglichkeiten grenzenlos; der „negativen Kreativität“ sind dabei keine Grenzen gesetzt.

Eingriffsintensivierend könnte grundsätzlich der Effekt der weltweiten Verbreitung von Videodaten, die daraus entstehenden Einschüchterungseffekte der Videoüberwachung und der damit verbundene Anpassungsdruck hinzukommen.[91] Im Anwendungsfall von IDeA werden hingegen nur eine sehr begrenzte Anzahl an Datenbrillen zu ausschließlich medizinischen Zwecken genutzt. Die betroffenen Personen werden statistisch nur äußerst selten einer medizinischen Datenbrille begegnen, womit das allgegenwärtige Überwachungsgefühl nicht entstehen kann und in den wenigen Fällen des Kontakts wird die (Seh-)Beeinträchtigung des Trägers für die Umgebung trotz der Unterstützung durch die Brille in aller Regel erkennbar. Ein Einschüchterungseffekt wird mithin nicht eintreten.

#### 2.2.5.2.2.2.4 Technische und organisatorische Maßnahmen

Im Rahmen der Abwägung können technische und organisatorische Maßnahmen die Risiken der Datenverarbeitung begrenzen und insoweit eine Möglichkeit für den Verantwortlichen sein, die Abwägung zu seinen Gunsten zu beeinflussen.[92] In der Literatur finden sich zahlreiche Beispiele[93]. *Schantz* verweist in etwa auf den Katalog in § 22 Abs. 2 Satz 2 BDSG sowie auf:[94]

- ein voraussetzungsloses Widerspruchsrecht,
- eine erleichterte Ausübung der Betroffenenrechte, die über die Vorgaben des Grundsatzes des Datenschutzes durch Technik nach Art. 25 Abs. 1 DS-GVO hinausgeht

---

90 *Spiecker gen. Döhmann*, CR 2010, 311 (316).

91 *Klar* 2012, 38.

92 Gierschmann et al. -*Veil*, Art. 6 DS-GVO Rn. 143.

93 S. bspw. das Standard-Datenschutzmodell der AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf.

94 Simitis/Hornung/Spiecker gen. Döhmann-*Schantz*, Art. 6 Abs. 1 DS-GVO Rn. 114.

- zusätzliche Informationen über Art. 12 ff. DS-GVO hinaus, die die Datenverarbeitung sowie die Bedeutung der Daten für den Verantwortlichen transparenter machen,
- Pseudonymisierung, Verschlüsselung oder unverzügliche Anonymisierung nach Erhebung der Daten,
- Einschaltung eines Datentreuhänders, um die Nutzung der Daten für andere Zwecke zu verhindern
- die Möglichkeit zur Ergänzung oder Veränderung der Daten durch die betroffene Person

Als weitere Gewichtungsfaktoren werden in der Literatur genannt:[95]

- der Umfang der Datenverarbeitung einschließlich der Nutzbarkeit für die Bildung von Persönlichkeitsprofilen
- die denkbaren negativen Folgen der Datenverarbeitung, wie sie beispielsweise in EG 75 S. 1 DS-GVO spezifiziert werden
- die Betroffenheit verletzlicher betroffener Personen, neben den in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO genannten Kindern beispielsweise Ältere oder psychisch Kranke

Gerade im Kontext von Datenbrillen kommen unter anderem folgende Maßnahmen in Betracht:

- Verwischen,
- Verschlüsselung,
- Situationsbedingte Aktivierung besonderer Funktionen (Kamera-, Gesichtserkennungs- oder Übertragungsfunktion standardmäßig aus),
- Umgebungsdaten umgehend löschen (z.B. Ringpuffer nach Vorbild Dash-Cam),
- Unterscheidung zwischen Landschaft und Menschen o.ä. mit abgestuften Aufnahmefunktionen,
- Anzeige des Zwecks und der gerade genutzten Funktionen zur Transparenz (An-Aus, Aufnahmefunktion, Training, Gesichtserkennung…) oder
- Kommunikation mit anderen Geräten.

#### 2.2.5.2.3 Zwischenergebnis

Aufgrund der Nachteile einer Einwilligung für dieses Verarbeitungsszenario bietet sich für die Verarbeitung von personenbezogenen Daten von Dritten lediglich die allgemeine Norm des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Dabei lässt sich eine endgültige Aussage zur Rechtmäßigkeit lediglich bei vollständiger Kenntnis der technischen Umsetzung und der genauen Einsatzsituationen treffen. Es lassen sich dennoch grundsätzliche Aussagen für diesen Bereich treffen, anhand derer eine Orientierung der zukünftigen Ausgestaltung von Datenbrille – insbesondere für medizinische Zwecke – möglich ist.

Werden Datenbrillen zu privaten Zwecken (z.B. der Freizeitgestaltung oder modisches Accessoire) genutzt, so überwiegen die Interessen der betroffenen Personen eindeutig. Derzeit ist keine technische Ausgestaltung realisierbar, die insbesondere den Überwachungsdruck der Gesellschaft eingrenzen und eine solche Datenverarbeitung rechtfertigen könnte.

An diesem Ergebnis ändert es auch nichts, wenn ein Anbieter die Datenbrille so gestaltet, dass sie etwa Sehschwächen ausgleichen kann, jedoch überwiegend zum privaten Gebrauch

---

[95] S. Simitis/Hornung/Spiecker gen. Döhmann-*Schantz*, Art. 6 Abs. 1 DS-GVO Rn. 105 ff.; *Herfurth*, ZD 2018, 517; Auernhammer-*Kramer*, Art. 6 DS-GVO Rn 50 ff; *Wolff* in Schantz/Wolff 2017, Rn. 652 ff.

konzipiert ist. Ein solches Vorschieben von etwaigen medizinischen Gründen ist bei der datenschutzrechtlichen Betrachtung unbeachtlich; entscheidend ist die tatsächliche Nutzung.

Wird die Datenbrille zu medizinischen Zwecken genutzt, beurteilt sich die Abwägung anders. Neben das kommerzielle Interesse des Anbieters und das private Interesse des Trägers an der Freizeitgestaltung tritt das gewichtige Interesse an der körperlichen Unversehrtheit und Würde des Menschen. Insbesondere das schutzwürdige Interesse an einer würdigen und gleichwertigen Alltagsgestaltung der an AMD erkrankten Personen überwiegt – jedenfalls bei einer nur kurzzeitigen Speicherung der Daten Dritter – in diesem Fall die tangierten Interessen der betroffenen dritten Personen. Zudem wirkt erleichternd, dass nur wenige Menschen diese Brille tragen und eine allumfassende Überwachung nicht zu befürchten ist.

Ob zwischen einzelnen Graden an medizinischer Indikation zu unterscheiden ist, ist in der juristischen Literatur bisher noch ungeklärt. Ist die altersbedingte Makuladegeneration noch nicht so weit fortgeschritten, dass eine Assistenzfunktion in der Außenwelt erforderlich wäre und die Datenbrille zwar – auch für gesunde Menschen – nützliche Funktionen (wie das Vergrößern von Texten oder Sprachassistenten) bereithält, ist die Funktion der Brille auf die Behandlungs- und Trainingsfunktion zu beschränken. Jedenfalls ab Krankheitsgraden, in denen der Träger bei der Verrichtung seiner Alltagshandlungen eingeschränkt ist, kann von einem Überwiegen seiner Interessen ausgegangen werden. Aufgrund der geplanten Einbindung von ärztlicher Kompetenz könnten eine solche Aktivierung bzw. Einschränkung von manchen Funktionen der Brille als technische Maßnahme implementiert werden. Die technische Maßnahme der Ringspeicherung ermöglicht dabei den Betrieb der Datenbrille in der Öffentlichkeit, ohne in die Rechte der betroffenen Personen unzulässig einzugreifen.

#### 2.2.5.3 Träger – Dritte

Eine weitere Verarbeitungskonstellation besteht zwischen dem Träger und dem Dritten. Auch der Träger der Datenbrille verarbeitet personenbezogene Daten von Dritten. Dabei wird er sich in aller Regel nicht auf die Haushaltsausnahme berufen können, weshalb die DS-GVO anwendbar ist und ihre Anforderungen einzuhalten sind.[96]

Eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO ist zumindest im Verhältnis zu unbekannten Dritten aus denselben Gründen wie im Verhältnis der Anbieter zu Dritten nicht möglich.[97] Denkbar erschiene hingegen eine Einwilligung in abgeschlossenen Räumen zu bekannten Personen (z.B. Familienmitglieder oder enge Bekannte), die insbesondere über die genaue Nutzung informiert wurden.[98]

Letztlich wird sich der Träger der Brille auch auf berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO stützen (müssen). Hierbei sind dieselben Erwägungen wie im Verhältnis des Anbieters zu den Dritten maßgeblich. Eine Nutzung bei – insbesondere fortgeschrittener – AMD-Erkrankung erscheint je nach konkreter Ausgestaltung der Anwendung grundsätzlich als möglich.

## 2.3 Annex: Ausgewählte haftungsrechtliche Fragestellungen

Im Folgenden sollen als Annex zur datenschutzrechtlichen Prüfung ausgewählte haftungsrechtliche Herausforderungen betrachtet werden. Dabei sollen aufgrund der datenschutzrechtlichen Schwerpunktsetzung der Untersuchung lediglich ausgewählte Datenbrillen-spezifische haftungsrechtliche Problemstellungen betrachtet werden. Auf allgemeine haftungsrechtliche Fragestellungen (z.B. Lieferung einer fehlerhaften Hardware) wird in diesem Gutachten verzichtet.

---

96 S. hierzu Kap. 2.2.1.

97 S. hierzu Kap. 2.2.5.2.1.

98 Zu den genauen Voraussetzungen einer Einwilligung s. Kap. 3.5.

Auch die fehlerhafte Anwendung des technisch ordnungsgemäßen Produkts sowie eine Haftung des Trägers der Datenbrille bleiben außer Betracht.

Vorab ist zu klären, ob die Datenbrille als Medizinprodukt einzustufen und damit das Medizinproduktegesetz anwendbar ist. Nach § 3 Nr. 1 Medizinproduktegesetz (MPG) sind Medizinprodukte u.a. Gegenstände, die der Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten zu dienen bestimmt sind und weder pharmakologisch noch immunologisch wirken. Die Definition des Medizinprodukts wird dabei weit ausgelegt und umfasst auch Software, wenn sie spezifisch vom Hersteller für einen der in der Definition für Medizinprodukte genannten medizinischen Zwecke bestimmt ist.[99] Eine Datenbrille, auf der unter anderem Gesundheits-Apps betrieben werden können, ist noch kein Medizinprodukt i.S.d. § 3 Nr. 1 MPG.[100] Die Gesundheits-Apps der Datenbrille können hingegen als Medizinprodukt eingestuft werden, sofern diese spezifische diagnostische oder therapeutische Funktionen (z.B. Bildauswertungsprogramme und Therapieplanungsprogramme) haben und nicht nur allgemeine Funktionen, die lediglich in einem medizinischen Zusammenhang genutzt werden (z.B. Textverarbeitungsprogramme und Betriebssysteme).[101] Die Anwendungen der Diagnose, Trainings- und Assistenzfunktion, die für die genannten notwendigen Schnittstellen zu den Dritten (z.B. Ärzte und Optiker) sowie die Infrastruktur zur Verknüpfung dieser Funktionen in IDeA dienen der Behandlung und Unterstützung von AMD-kranken Personen und sind damit Medizinprodukte gem. § 3 Nr. 1 MPG.

Mangels spezialgesetzlicher Regelung der zivilrechtlichen Haftung der Betreiber und Anwender im MPG und dem Medizinproduktebetreiberverordnung (MPBetreibV) bestimmen sich die Haftungsfragen von Medizinprodukten nach den allgemeinen Haftungsregeln.[102] Dabei kommen insbesondere vertragliche und deliktische Haftungsansprüche sowie Ansprüche aus dem verschuldensunabhängigen Produkthaftungsgesetz (ProdHaftG) in Betracht.

Bei einer Haftungsprüfung im Medizinbereich ist grundsätzlich zwischen der Haftung in der Erprobungsphase und der Haftung in der Nutzungsphase zu unterscheiden.[103] Die Erprobungsphase umfasst die Entwicklung bis zum Inverkehrbringen des Produkts. Die Nutzungsphase beginnt ab Inverkehrbringen des Produkts.

### 2.3.1 Vertragliche Mängelhaftung

Eine vertragliche Mängelhaftung nach den §§ 280 ff. BGB erfolgt in aller Regel lediglich inter partes, also nur zwischen den Vertragspartnern. Der Träger der Datenbrille wird in aller Regel einen Vertrag über die Nutzung oder den Erwerb der Datenbrillen in der Entwicklungsphase mit einer juristischen Person des Forschungsprojekts und in der Nutzungsphase mit dem jeweiligen Betreiber der Datenbrille schließen. Je nach Ausgestaltung der Rechtsform des Forschungsprojekts und der Vertragsart, die sich letztlich nach der konkreten Nutzungsart richtet, bestimmen sich die Möglichkeiten eines Regresses des geschädigten Trägers.

Typischerweise wird sich die Hauptfrage darum drehen, ob der Verkäufer einen möglichst umfassenden Haftungsausschluss in den Vertrag integrieren kann. Dieser muss sich jedoch an die Grenzen des allgemeinen AGB-Rechts halten. Dabei stehen einem Haftungsausschluss insbesondere die Klauselverbote ohne Wertungsvorbehalt nach § 309 Nr. 7 lit. a und b BGB entgegen. Demnach darf ein Ausschluss oder eine Begrenzung der Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen

---

99 Rehmann/Wagner-*Rehmann*, § 3 MPG Rn. 1.

100 So auch *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2919).

101 Bergmann/Pauge/Steinmeyer-*Webel*, § 3 MPG Rn. 12.

102 *Weimer*, MPR 2007, 119 (120); *Koyuncu/Müller*, MPR 2012, 158 (158).

103 *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2921).

Pflichtverletzung des Verwenders oder einer vorsätzlichen oder fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen des Verwenders beruhen, nicht ausgeschlossen werden (§ 309 Nr. 7a BGB). Zudem ist ein Ausschluss oder eine Begrenzung der Haftung für sonstige Schäden, die auf einer grob fahrlässigen Pflichtverletzung des Verwenders oder auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder Erfüllungsgehilfen des Verwenders beruhen, unzulässig (§ 309 Nr. 7b BGB). Bei der Beurteilung des Vorsatzes und der Fahrlässigkeit sind die Umstände des Einzelfalls zu berücksichtigen.

### 2.3.2 Beschränkte Haftung in der Erprobungsphase

#### 2.3.2.1 Haftung nach dem ProdHaftG

Eine weitere Haftungsmöglichkeit besteht in der Produkthaftung nach dem Produkthaftungsgesetz (ProdHaftG). Hierunter fällt die Haftung des Herstellers für Folgeschäden aus der Benutzung seiner Produkte für Personen- als auch für Sachschäden, mit Ausnahme der Schäden an dem Produkt selbst.[104] Es handelt sich dabei um eine sogenannte Gefährdungshaftung, nach der der Hersteller allein für das Inverkehrbringen eines fehlerhaften Produkts haftet, unabhängig davon, ob er den Schadensfall verschuldet hat oder nicht.

Grundsätzlich haftet nach § 1 Abs. 1 ProdHaftG jeder Hersteller für das Produkt. Die Haftung ist jedoch nach § 1 Abs. 2 Nr. 1 ProdHaftG ausgeschlossen, wenn der Hersteller das Produkt nicht in Verkehr gebracht hat.

Ein Inverkehrbringen in der Erprobungsphase ist allerdings bereits abzulehnen, sofern auf das Verständnis des Inverkehrbringens eines Medizinproduktes (§ 3 Nr. 1 MPG) nach dem MPG abgestellt wird. Nach § 3 Nr. 11 Satz 1 MPG ist erst die entgeltliche oder unentgeltliche Abgabe eines fertigen Medizinprodukts an andere als Inverkehrbringen zu verstehen.[105] Vor- und Zwischenprodukte fallen nicht unter diese Definition. Freilich lässt sich vertreten, dass der Begriff des Inverkehrbringens im ProdHaftG ein anderer als der des MPG sei.[106]

Selbst wenn dieser Auffassung nicht gefolgt und ein Inverkehrbringen bereits in der Erprobungsphase bejaht wird bzw. auf das Inverkehrbringen nach dem ProdHaftG abstellt, scheitert eine Haftung nach dem ProdHaftG an § 1 Abs. 2 Nr. 5 ProdHaftG. Hiernach lösen Fehler keine Ersatzpflicht aus, die „nach aktuellem Stand von Wissenschaft und Technik zum Zeitpunkt des Inverkehrbringens nicht erkannt werden konnten".[107] Die Erprobungsphase dient gerade dazu, den Stand von Wissenschaft und Technik fortzuentwickeln.

#### 2.3.2.2 Deliktische Haftung

Die Haftung nach dem Deliktsrecht in den § 823 ff. BGB bedarf keiner Sonderbeziehungen zwischen den Beteiligten, sondern schützt alle betroffenen Personen. Im Gegensatz zur vertraglichen Mängelhaftung schützt das Deliktsrecht das Integritätsinteresse, also das Interesse an Unversehrtheit, der Rechtsgüter einer Person. Im Wesentlichen kommen zwei Haftungstatbestände in Betracht. Zum einen ist gem. § 823 Abs. 1 BGB derjenige schadensersatzpflichtig, der vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt. An den Tatbestandsmerkmalen der Vorsätzlichkeit oder Fahrlässigkeit, die ein persönlich vorwerfbares Verhalten voraussetzen, wird der Charakter des § 823 BGB als eine Verschuldenshaftung deutlich. Zum anderen ist derjenige in derselben Weise schadensersatzpflichtig, der gegen ein den Schutz

---

104 *Kanz/von Coelln* 2012, 58.

105 Spickhoff-*Lücker*, § 3 MPG Rn. 15.

106 So *Koyuncu*, MPR 2006, 29 (34).

107 So auch *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2921 ff.).

eines anderen bezweckendes Gesetz verstößt. Für die Qualifikation als Schutzgesetz ist maßgebend, ob die verletzte Vorschrift dem Schutz von Individualinteressen zu dienen bestimmt ist.[108]

Zu beachten ist ein entscheidender Unterschied zum ProdHaftG. Im Deliktsrecht bestehen i.R.d. § 823 BGB auch Produktbeobachtungspflichten, während es beim ProdHaftG nur auf den Zeitpunkt des Inverkehrbringens ankommt.[109]

Eine deliktische Haftung in der Erprobungsphase von Datenbrillen im medizinischen Kontext wird in aller Regel an mangelndem Verschulden scheitern.[110] Ein denkbarer Vorwurf könnte nur darin bestehen, dass der Hersteller das realisierte Risiko in fahrlässiger Weise übersehen hat. Nach den Wertungen des allgemeinen Zivilrechts ist bei neuartigen Produkten hingegen stets die „Zumutbarkeit der Erkenntnisgewinnung“[111] zu berücksichtigen.[112]

In diesem Zusammenhang ist zu beachten, dass eine Haftung auch bezüglich „Kombinationsgefahren durch gleichzeitigen Einsatz mit einem fremden Produkt (Honda-Urteil des BGH[113]) in Betracht kommen kann.[114] Ist also eine Nutzung im Automobilbereich geplant oder ist mit einer solchen Nutzung erwartungsgemäß durch die Nutzer der Brille zu rechnen, sind die Wechselwirkungen zu beachten. Gerade in dieser Kombination muss eine mögliche Haftbarkeit genau zu prüfen. Es erscheint deshalb empfehlenswert, entweder klare Hinweispflichten bezüglich eines etwaigen Verbots des Gebrauchs der Brille beim Führen eines Kfz im Straßenverkehr zu implementieren oder gar eine technische Maßnahme zur Verhinderung der Nutzung in einer solchen Umgebung. So könnte die Datenbrille eine Fahrumgebung erkennen und sich das Gerät selbständig abschalten oder zumindest eine Warnung anzeigen. Auf jeden Fall bedarf es einer genauen straßenverkehrsrechtlichen und haftungsrechtlichen Untersuchung bezüglich der Nutzung im Straßenverkehr. Bis dato mangelt es diesbezüglich an juristischer Literatur. Dieses Nutzungsszenario erscheint jedoch nach erster Einschätzung als juristisch äußerst herausfordernd.

Darüber hinaus misst auch § 20 Abs. 1 Satz 4 Nr. 1 MPG die Risiken, die im Rahmen einer klinischen Studie für die Person auftreten können, an der voraussichtlichen Bedeutung des Medizinprodukts für die Heilkunde. Diese müssen ärztlich vertretbar sein. Es werden mithin gewisse Risiken für den zukünftigen Nutzen des Medizinprodukts in Kauf genommen. Diese Wertungen erscheinen auch für den Bereich von Datenbrillen im medizinischen Kontext anwendbar.[115]

### 2.3.3 Mögliche Haftung in der Nutzungsphase

#### 2.3.3.1 Haftung nach dem ProdHaftG

Eine Haftung des Herstellers eines Produkts besteht nach § 1 Abs. 1 Satz 1 ProdHaftG, sofern durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt wird.

Zunächst ist festzuhalten, dass sowohl das gesamte Produkt der fertigen Datenbrille als auch deren einzelne Komponenten der Hard- und Software[116] im Zweifel Produkte i.S.d. § 2

---

108 MüKoBGB-*Wagner*, § 823 BGB Rn. 498.

109 *Ebers* 2017, 101.

110 So auch *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2922 ff.).

111 Palandt-*Sprau*, BGB, § 823, Rn. 173.

112 *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2922).

113 BGHZ 99, 167.

114 *Kanz/von Coelln*, 2012, 73.

115 So auch *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2922).

116 *Ebers* 2017, 102.

ProdHaftG sein können.[117] So sind beispielsweise auch die Fahrerassistenzsysteme in einem Kraftfahrzeug Produkte i.S.d. § 2 ProdHaftG.[118] Dabei können auch die Hersteller von Teilprodukten als Anspruchsgegner in Frage kommen, sofern der Schaden durch dieses Teilprodukt verursacht wurde. Der Hersteller und der Teilehersteller haften dann im Außenverhältnis als Gesamtschuldner und können im Innenverhältnis gegenseitig je nach Schadensverursachungsanteil Regress nehmen.[119]

Ferner muss eine Rechtsgutverletzung i.S.d. § 1 Abs. 1 Satz 1 ProdHaftG, also eine Verletzung der körperlichen Integrität, der Gesundheit oder des Eigentums einer Person, eingetreten sein. Diese Rechtsgutsverletzung muss durch einen Fehler des Produkts nach § 3 ProdHaftG bewirkt worden sein. Hierbei kommen Konstruktions-, Fabrikationsfehler sowie Instruktionsfehler in Betracht.[120] Der Maßstab der Beurteilung eines Fehlers richtet sich nach der berechtigten Erwartung bezüglich aller Umstände, zu denen insbesondere die Darbietung, der Gebrauch, mit dem billigerweise gerechnet werden kann, und der Zeitpunkt des Inverkehrbringens zählen (§ 3 Abs. 1 ProdHaftG).

Bezüglich Medizinprodukten hat der EuGH entschieden, dass bei Herzschrittmachern ein Ausfallrisiko von 0,31-0,88 % für die Bejahung eines Fehlers ausreicht, ohne, dass es tatsächlich zu einem Fehler gekommen ist.[121] Die Sicherheitsanforderungen, die an ein Medizinprodukt gestellt werden können, ergeben sich dabei aus dem Verwendungszweck und den Besonderheiten der Benutzergruppe. Die Verletzlichkeit der Betroffenen und die gravierenden Konsequenzen, die bei Ausfall eines Herzschrittmachers entstehen, begründen diese strenge Sichtweise. Letztlich sei die Qualifizierung eines Fehlers eine Abwägungsfrage. Die berechtigten Interessen des Verbrauchers und der sonstigen Betroffenen sind mit dem Interesse des Produzenten an einer Haftungsbefreiung abzuwägen. Diese Entscheidung ist übertragbar auf andere Anwendungsfälle. So ist der Ausfall einer den Blutzucker anzeigenden Kontaktlinse sehr hoch, da eine Fehlinformation auch zum Tod führen kann. Dementsprechend sind auch in diesem Fall an die Fehlerbeurteilung hohe Anforderungen zu stellen.

Die Datenbrille soll Menschen unterstützen, die aufgrund einer AMD-Erkrankung mitunter Alltagshandlungen nur schwierig oder gar nicht mehr selbstständig vornehmen können. Sie verlassen sich deshalb auf die Unterstützungsfunktionen der Datenbrille. Wird diese etwa im Straßenverkehr getragen und es tritt ein Fehler auf, so können erhebliche Schäden für den Träger der Brille und auch die anderen Teilnehmer des Straßenverkehrs entstehen. Die Software könnte beispielsweise eine Ampelanzeige nicht richtig erkennen und fälschlicherweise die auditive Empfehlung zur Überquerung einer Straße geben. Nach den obigen Wertungen wird aufgrund des hohen Schadensrisikos auch in diesem Fall ein entsprechend strenger Maßstab bezüglich der Fehlerbeurteilung anzulegen sein.

Mangels einschlägiger höchstrichterlicher Entscheidungen und juristischer Literatur zu neuen AR-Assistenzsystemen im Gesundheitsbereich muss auf Erwägungen anderer, aber dennoch ähnlicher Situationen zurückgegriffen werden. Aufgrund des ebenfalls sehr hohen

---

117 *Palandt/Sprau*, § 2 ProdHaftG Rn. 1 differenziert zwischen Standardsoftware und Individualsoftware, wobei nur ersteres erfasst sein soll; BeckOK BGB-*Förster* § 2 ProdHaftG, Rn. 22 ff. lehnt eine solche Unterscheidung ab und stellt auf eine Verkörperung ab, was dazu führt, dass eine Software nicht erfasst ist, außer sie wird gespeichert und verkörpert sich auf der Festplatte; MüKoBGB-*Wagner*, § 2 ProdHaftG, Rn. 13 ff. bemängelt die Unterscheidung nach der Verkörperung und will die Informationen einheitlich und unabhängig von einer Verkörperung aus dem Anwendungsbereich des ProdHaftG ausnehmen.

118 *Kanz/von Coelln* 2012, 59.

119 *Fleck/Thomas*, NJOZ 2015, 1393 (1396).

120 *Fleck/Thomas*, NJOZ 2015, 1393 (1398).

121 EuGH, NJW 2015, 1163.

Risikopotenzials und dem Abtreten der Entscheidung über Handlungen an ein Assistenzsystem bietet sich ein Vergleich mit den rechtlichen Herausforderungen des automatisierten Fahrens an.

Bei hoch- bzw. vollautomatisierten Systemen, wie dem automatisierten Fahren, sind die Erwartungen an die Fehlerfreiheit des Systems ebenfalls hoch. Der mögliche eintretende Schaden ist in diesem Bereich sehr groß. Würde der Maßstab nicht dementsprechend hoch angelegt werden, dürfte dem Fahrzeugführer nicht gestattet bzw. ermöglicht werden, seine Aufmerksamkeit vom Straßenverkehr abzuwenden.[122] Das hochautomatisierte System müsste in der Lage sein, während des Automatikbetriebs alle auftretenden Situationen zu bewältigen. Tritt dennoch ein Schaden ein, deutet dies stark auf einen Produktfehler hin.[123]

Wendet man diese Erwägungen auf Datenbrillen an, könnte zwischen unterschiedlichen Sehstufen abzugrenzen sein. Soll die Datenbrille eine Person mit weit fortgeschrittener AMD-Erkrankung unterstützen, die ohne die Unterstützung durch die Datenbrille nicht in der Lage wäre, selbstständig am Straßenverkehr teilzunehmen, so wird sich diese Person erwartungsgemäß völlig auf die Unterstützung der Brille verlassen. In diesem Fall erscheint ein Vergleich und damit eine ähnliche Bewertung wie beim automatisierten Fahren angebracht. Dementsprechend wären an die Datenbrille auch ähnlich hohe Anforderungen zu stellen. Ist die Krankheit hingegen noch nicht so weit fortgeschritten, ist der Träger der Datenbrille auch nicht in dem gleichen Maße auf eine Unterstützung angewiesen. Fraglich ist, ob sich der Träger nicht dennoch nur auf die Unterstützungshandlung – sei es nur aus Bequemlichkeit – verlassen wird. In diesem Fall ist aus haftungsrechtlicher Sicht ebenfalls von hohen Anforderungen auszugehen, da es nach § 3 ProdHaftG auf den Gebrauch ankommt, mit dem billigerweise gerechnet werden kann.

Im Bereich des automatisierten Fahrens wird darauf abgestellt, dass das Fahrzeug erkennen solle, worauf die Aufmerksamkeit des Fahrers gerichtet ist.[124] Eine Mensch-Maschine-Schnittstelle soll sicherstellen, dass der Fahrer jederzeit weiß, welche Funktion gerade aktiv ist, ob sie ihre Regelaufgabe erfüllt und wie sie diese erfüllt. Diese Erwägung könnte ebenfalls auf Datenbrillen übertragen werden. Erkennt die Datenbrille, dass der Träger im Straßenverkehr ausschließlich Unterstützung durch die Software und nicht mehr – auch – den Straßenverkehr betrachtet, könnte eine Warnung erfolgen. Wird zudem aufgrund der Umgebungsaufnahme erkannt, dass sich der Träger im Straßenverkehr befindet, könnte zudem eine Warnung zur erhöhten Vorsicht und – gerade ab einem fortgeschrittenen Krankheitsgrad – eine mögliche Nutzung von anderweitigen Hilfsmitteln (z.B. Blindenhilfe bei Ampeln) empfohlen werden.

Auf der anderen Seite wird beim autonomen Fahren vertreten, dass von Verbrauchern als Nutzern von Warn- und Informationssystemen verlangt werden darf, dass diese nicht von eigenem sorgfältigen Verhalten im Straßenverkehr entbunden werden, auch wenn sie nicht selbst fahren.[125] Auf den Bereich von Datenbrillen angewandt, bedeutet dies, dass vom Träger der Datenbrille erwartet werden darf, dass er die erforderliche Sorgfalt im Straßenverkehr an den Tag legt und sich nicht nur auf die Unterstützungsanzeige der Datenbrille verlässt.

Nicht zuletzt aufgrund der fehlenden Rechtsprechung zu AR-basierten Assistenzsystemen lässt sich keine verlässliche Aussage zu einer möglichen Haftung treffen. Die rege Diskussion zu den haftungsrechtlichen Fragestellungen im Bereich des autonomen Fahrens verdeutlicht jedoch, dass die Rechtslage ungeklärt ist und ein Risiko der Haftung durchaus bestehen kann.

---

122 *Fleck/Thomas*, NJOZ 2015, 1393 (1397).

123 *Fleck/Thomas*, NJOZ 2015, 1393 (1397).

124 *Jourdan/Matschi*, NZV 2015, 26 (28 ff.).

125 *Kanz/von Coelln*, 2012, 81.

#### 2.3.3.2 Deliktische Haftung nach § 823 Abs. 1 BGB

In der Nutzungsphase könnte ein Verstoß des Herstellers gegen Verkehrssicherungspflichten in Betracht kommen.[126] Hiernach hat er etwa offenkundige Fehler zu kontrollieren oder in anlassbezogenen Ausnahmefällen (z.B. Häufung von Beschwerden) die Kunden zu warnen.

Konkrete Vorgaben zu Meldepflichten enthält die MPSV, die Meldepflichten an die zuständige Bundesoberbehörde für diejenigen vorsieht, die Medizinprodukte (§ 3 Nr. 1 MPG) herstellen bzw. beruflich oder gewerblich betreiben oder anwenden (§ 3 MPSV). § 2 Nr. 1 MSPV besagt, dass ein meldepflichtiges Vorkommnis eine Funktionsstörung, ein Ausfall, eine Änderung der Merkmale oder der Leistung oder eine unsachgemäße Kennzeichnung oder Gebrauchsanweisung eines Medizinproduktes ist, die oder der unmittelbar oder mittelbar zum Tod oder zu einer schwerwiegenden Verschlechterung des Gesundheitszustands eines Patienten, eines Anwenders oder einer anderen Person geführt hat, geführt haben könnte oder führen könnte. Zwar erfasst die MPSV keine Warnungen an Kunden, sondern eine behördliche Meldung. Nach der ständigen Rechtsprechung konkretisiert die MPSV jedoch auch im Bereich von § 823 Abs. 1 BGB die Beobachtungspflichten für Medizinprodukte, sodass für eine darüberhinausgehende Haftung i.R.d. § 823 Abs. 1 BGB kein Raum bleibt.[127]

#### 2.3.3.3 Deliktische Haftung nach § 823 Abs. 2 BGB i.V.m. einem Schutzgesetz

Im Bereich der Nutzung von Datenbrillen zu medizinischen Zwecken kommen diverse medizinrechtliche Normen als Schutzgesetze in Betracht, die über § 823 Abs. 2 BGB zu einer Haftung führen können. So dient das MPG nach § 1 MPG dem „erforderlichen Schutz der Patienten, Anwender und Dritter“. Die Norm ist dabei im Zusammenhang mit der Richtlinie 93/42/EWG zu lesen, deren Hauptziel der Schutz des Patienten vor gesundheitlichen Beeinträchtigungen ist. Mögliche Schutzgesetze können unter Umständen die §§ 4, 6, 9, 11, 12, 20 und 21 MPG und die MPBetreibV sein.[128] Falls die Datenbrille beim Betrieb eines Kraftfahrzeuges eingesetzt wird, könnten auch die Normen der StVO als Schutzgesetze in Betracht kommen.

Die Haftung nach diesen Vorschriften beurteilt sich nach den entsprechenden Grundsätzen wie § 823 Abs. 1 BGB und gelangt zu entsprechenden Ergebnissen.

### 2.3.4 Zwischenergebnis

Eine Haftung der Betreiber von Datenbrillen für medizinische Zwecke ist in zwei unterschiedliche Phasen zu trennen und gesondert zu bewerten. Mangels einer Regelung von Haftungstatbeständen in den medizinrechtlichen Vorschriften ist dabei auf die allgemeinen Haftungsnormen zurückzugreifen.

Eine vertragliche Mängelhaftung ist je nach Ausgestaltung des Systems und des Vertrags grundsätzlich denkbar. Sie wirkt hingegen nur inter partes, d.h. Dritte können in diesem Verhältnis keine Ansprüche geltend machen. Eine Haftung kann grundsätzlich durch einen Haftungsausschluss begrenzt werden. Dieser muss sich jedoch an die Grenzen des AGB-Rechts halten.

In der Erprobungsphase wird in der Regel keine Haftung des Betreibers bestehen. Das verschuldensunabhängige ProdHaftG ist mangels Inverkehrbringens des Produkts nicht anwendbar. Eine deliktische Haftung scheitert in aller Regel am mangelnden Verschulden des Betreibers.

In der Nutzungsphase ist eine Haftung des Betreibers in gewissen Situationen durchaus denkbar. Eine Haftung nach dem ProdHaftG erscheint je nach Auffassung hinsichtlich des

---

126 *Backmann*, MPR 2012, 73 (77).

127 *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2923).

128 *Ortner*/*Daubenbüchel*, NJW 2016, 2918 (2922).

Fehlerbegriffs i.S.d. § 3 ProdHaftG denkbar. Die diesbezügliche Rechtslage ist für AR-Assistenzsystemen noch ungeklärt und ein Vergleich mit ähnlichen Systemen lässt eine Haftung grundsätzlich zu. Zu einem ähnlichen Ergebnis gelangt eine deliktsrechtliche Haftung nach § 823 BGB.

Diverse technische Maßnahmen könnten gegebenenfalls ein Haftungsrisiko zumindest verringern.

# 3 Rechtsfragen des Projekts Hive-Lab

Der Forschungsverbund HIVE-Lab berät Forschungs- und Entwicklungsprojekte bei technischen Fragestellungen (z.B. der Auswahl geeigneter Algorithmen). Zugleich werden technische Innovationen in realen und simulierten Alltagsumgebungen evaluiert sowie methodisch und technisch unterstützt. Außerdem wird eine allgemein zugängliche Wissensbasis entwickelt. Diese Wissensbasis wird den Transfer des wissenschaftlichen Knowhows in wirtschaftliche und gesellschaftliche Bereiche befördern. Dies geschieht durch öffentliche Veranstaltungen und frei zugängliche Publikationen (Open Access). Gestalterische, ethische und soziale Beratungsleistungen für wissenschaftliche, wirtschaftliche und gesellschaftliche Kooperationspartner sind beim HIVE-Lab ebenfalls möglich. Das HIVE-Lab bietet den Forschungsverbünden aus Wissenschaft und Wirtschaft alltagszentrierte und gestaltungsorientierte Evaluierungsmöglichkeiten, mit denen die VR/AR-Technik sensibel in den Nutzeralltag eingebettet wird.

Projekte, die Mixed-Reality-Anwendungen nutzen, um die Gesundheit und das Wohlbefinden ihrer Nutzer zu steigern, sollen bei der Erprobung ihrer Technologien unterstützt werden. HIVE-Lab entwickelt selbst keine eigene Technologie, sondern begleitet den Forschungsprozess anderer Projekte. Dementsprechend ist es nicht möglich, wie bei IDeA detaillierte Funktionalitäten und verwendete Datenarten zu erläutern (s.o. 2.1), sondern es geht gerade um die Rechtsfragen der Zusammenwirkung mit unterschiedlichen Funktionalitäten und Technologien, die in anderen Projekten erforscht werden.

An dem Forschungsverbund HIVE-Lab sind Forschungseinrichtungen aus unterschiedlichen Bereichen beteiligt, die im Bereich der VR/AR-Technik forschen. Einige Forschungen liegen dabei im Gesundheitsbereich. Datenschutzrechtlich muss zwischen den einzelnen zurzeit noch nicht vollständig absehbaren Handlungen des Forschungsverbunds HIVE-Lab (im Folgenden vereinfachend „HIVE-Lab“ genannt) unterschieden werden. Mit dieser Bezeichnung ist mit anderen Worten nicht impliziert, dass dieser Forschungsverbund eine eigene Rechtspersönlichkeit (z.B. als Gesellschaft bürgerlichen Rechts hat) oder – als solcher – ein datenschutzrechtlich Verantwortlicher ist. Es kommt ebenfalls in Betracht, dass allein die jeweils handelnden Forschungseinrichtungen des Verbunds (Projektpartner) einzeln oder zu mehreren rechtlich für die jeweiligen Handlungen verantwortlich sind.

Folgende Handlungen sind im Rahmen des HIVE-Labs denkbar bzw. geplant:

- Unterstützung bei Erprobungsverfahren (z.B. Zurverfügungstellen von Örtlichkeiten für Testzwecke oder Vermittlung von Know-how)
- Beratung bei technischen Fragestellungen (z.B. der Auswahl geeigneter Algorithmen),
- Vermittlung von Projektpartnern und Studienteilnehmern und
- Zugriff auf Datenbanken („Body of Knowledge”, s.u. 3.3.3).

## 3.1 Anwendbarkeit der DS-GVO

Datenschutzrechtliche Vorgaben müssen nach Art. 2 Abs. 1 DS-GVO nur bei einer Verarbeitung von personenbezogenen Daten eingehalten werden. Werden im Rahmen der Leistungen des HIVE-Labs keine personenbezogenen Daten verarbeitet, so sind auch keine datenschutzrechtlichen Anforderungen zu beachten.

Berät das HIVE-Lab ein Forschungsprojekt beispielsweise bezüglich technischer Fragestellungen, so wird dies in vielen Fällen ohne eine Verarbeitung von personenbezogenen Daten durch das HIVE-Lab erfolgen. Werden im Rahmen dieser Hilfeleistungen hingegen in irgendeiner Weise personenbezogene Daten verarbeitet (z.B. durch Speicherung von zur Analyse zugesandten personenbezogenen Daten), sind dementsprechend auch die datenschutzrechtlichen

Anforderungen zu beachten.[129] Ob und in welchem Umfang das HIVE-Lab datenschutzrechtliche Vorgaben beachten muss, richtet sich dann nach der Frage der Verantwortlichkeitsverteilung.[130]

Unterstützt das HIVE-Lab einzelne Projekte bei Erprobungsverfahren, stellt sich ebenfalls die Frage, ob auch das HIVE-Lab personenbezogene Daten verarbeitet. Werden den einzelnen Projekten nur die Räume für Erprobungsverfahren zur Verfügung gestellt, wird in aller Regel nur eine Datenverarbeitung durch die mitgebrachte Hard- und Software der Projekte erfolgen. Stellt hingegen das HIVE-Lab den Projekten eigene Hard- oder Software zur Verfügung, ist zu prüfen, inwieweit personenbezogene Daten durch das HIVE-Lab verarbeitet werden. So könnte dieses mittels der zur Verfügung gestellten Hard- oder Software personenbezogene Daten erheben, speichern oder an Dritte übermitteln. In diesem Fall wäre das Datenschutzrecht anwendbar. In einem zweiten Schritt müsste geprüft werden, ob und wie das HIVE-Lab verantwortlich i.S.d. Datenschutzrechts wäre, also inwiefern die Verarbeitung dem HIVE-Lab zuzurechnen ist; in Betracht kommt auch eine Auftragsverarbeitung.[131]

Hilft das HIVE-Lab bei der Vermittlung von Testpersonen oder Projektpartnern, so werden in aller Regel die personenbezogenen Daten der betroffenen Personen übermittelt.

Zusammenfassend lässt sich sagen, dass sofern keine Erhebung, Speicherung oder sonstige Verarbeitungsform durch das HIVE-Lab erfolgt, auch keine datenschutzrechtlichen Normen zu beachten sind.

## 3.2 Datenschutzrechtliche Verantwortlichkeit

Ist an einem Forschungsprojekt nur eine Forschungseinrichtung beteiligt, so kann auch nur diese als (alleinige) Verantwortliche für die Verarbeitung von personenbezogenen Daten in Betracht kommen. Sind hingegen mehrere Forschungseinrichtungen an Verbundprojekten beteiligt, muss genau bestimmt werden, welche Forschungseinrichtungen des Verbundes personenbezogene Daten verarbeiten. Eine Möglichkeit ist die Gründung einer GbR oder sonstigen rechtsfähigen Personengesellschaft oder juristischen Person für das Verbundprojekt, die dann als Verantwortliche für die Verarbeitung von personenbezogenen Daten in Betracht kommen kann. Sofern keine GbR besteht, muss für jede Forschungseinrichtung des Verbundprojekts jeweils geprüft werden, ob diese über die Zwecke und Mittel der einzelnen Datenverarbeitungen tatsächlich entscheiden. Dabei ist jede Datenverarbeitung in einzelne Verarbeitungsschritte zu gliedern und für diese die jeweilige Verantwortlichkeitsverteilung genau zu prüfen.[132] Im Folgenden wird das Forschungskonsortium HIVE-Lab vereinfachend als „HIVE-Lab“ bezeichnet. Die rechtlichen Feststellungen zu den Anforderungen der DS-GVO an das „HIVE-Lab“ bzw. die zu erfüllenden Pflichten bleiben dabei gleich. Sie treffen dann entweder die Gesellschaft des HIVE-Labs oder das jeweils innerhalb des HIVE-Labs datenschutzrechtlich für die jeweilige Verarbeitung von personenbezogenen Daten verantwortliche Projektmitglied.

Werden personenbezogene Daten verarbeitet, ist im Rahmen der Verantwortlichkeitsverteilung in einem ersten Prüfungsschritt zu klären, ob eine Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO oder eine Auftragsverarbeitung nach Art. 4 Nr. 8 DS-GVO vorliegt.

In dem Szenario des Body of Knowledge werden Forschungsergebnisse und weitere forschungsrelevante Informationen gespeichert. Hinsichtlich dieser Verarbeitung entscheidet das HIVE-Lab (als juristische Person oder rechtsfähige Personengesellschaft bspw. in Form einer

---

129 S. den Fragen der Anwendbarkeit der DS-GVO Kap. 2.2.1.

130 S. Kap. 3.2.

131 S. Kap. 3.2.

132 S. zu den Bewertungskriterien Kap. 2.2.4.

GbR oder zumindest einzelne Mitglieder des Forschungskonsortiums) zum einen den Zweck der Speicherung von zukünftig möglicherweise relevanten (Forschungs-)Daten. Zum anderen bestimmt das HIVE-Lab auch die Mittel der Verarbeitung. Wollen (HIVE-Lab-)externe Forschungsprojekte personenbezogene Daten in dem Body of Knowledge speichern, käme eine Auftragsverarbeitung des HIVE-Labs in Betracht. Das externe Forschungsprojekt bestimmt dabei in aller Regel den Zweck zur Speicherung (und der weiteren Verarbeitung) der Forschungsdaten und das HIVE-Lab entscheidet lediglich über die Art und Weise der Speicherung. Dem Auftragsverarbeiter steht ein Ermessenspielraum hinsichtlich der eingesetzten Mittel zu, sodass die Entscheidung über die Art und Weise der Speicherung unschädlich ist.[133]

Sofern das HIVE-Lab (als juristische Person, rechtsfähige Personengesellschaft oder einzelne Mitglieder des Forschungskonsortiums) hingegen die Schwelle der Entscheidung über wesentliche Mittel oder den Zweck überschreitet, ist es als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO einzustufen. In diesem Fall muss in einem zweiten Schritt geprüft werden, ob eine gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 DS-GVO besteht. Beabsichtigen (HIVE-Lab-)externe Forschungseinrichtungen bspw. eine Verbesserung von bestimmten Eigenschaften von AR/VR-Technologien und nutzen hierfür die Hard- und Software von HIVE-Lab, so könnte an diesen Erkenntnissen auch das HIVE-Lab ein Interesse haben. Dementsprechend mag es sein, dass hierbei die Zwecke der Forschung gemeinsam entschieden werden und ggf. auch die Mittel gemeinsam festgelegt werden.

## 3.3 Rechtfertigung der Datenverarbeitung(en)

In der (medizinischen) Forschung können personenbezogene Daten einen Grundpfeiler des medizinischen Erkenntnisgewinns und damit des Erfolgs bilden.[134] Je größer die Zahl an aussagekräftigen und validen personenbezogenen Daten, je besser die Verknüpfungsmöglichkeiten von Datenquellen und je besser die Fortentwicklung der Forschungsmethoden durch neue Technologien vorangetrieben werden kann, desto mehr Innovationen und Erkenntnisse werden ermöglicht.[135] Langfristige Datenspeicherungen sind in der medizinischen Forschung für den Forschungserfolg, der typischerweise auch langfristige Auswirkungen beachten muss, unerlässlich.[136] Um diese zu gewährleisten, gesteht die DS-GVO der Forschung einige Privilegien gegenüber anderen Zwecken der Datenverarbeitung.[137] Die Kehrseite dieser oftmals datenintensiven Verarbeitung ist ein in der Regel sehr tiefer Einblick in sensitive Merkmale der Betroffenen. Um die Betroffenen nicht schutzlos zu lassen, verlangt die DS-GVO als Ausgleich für diese Privilegien einige „Garantien" für die Grundrechte und Freiheiten der Betroffenen (Art. 89 DS-GVO).[138] Festzuhalten ist, dass der Forschungsfreiheit von Forschungsprojekten und der informationellen Selbstbestimmung der betroffenen Personen ein innerer Konflikt innewohnt, den es möglichst schonend auszugleichen gilt. Auf Grundrechtsebene sind dabei auf der einen Seite die Wissenschaftsfreiheit nach Art. 13 GRCh und auf der anderen Seite die informationelle Selbstbestimmung nach Art. 7 GRCh gegeneinander abzuwägen.

Die medizinische Forschung verfolgt dabei zwei Ziele. Zum einen dient sie dem unmittelbaren Wohl des Patienten und zum anderen auch dem Wohl von zukünftigen Patienten, die von den

---

133 *Kremer*, CR 2019, 225 (229).

134 *Roßnagel*, ZD 2019, 157 (158).

135 *RAT FÜR INFORMATIONSINFRASTRUKTUREN* 2017, 3 ff.

136 *Pommerening*/*Müller* 2014, 19.

137 S. z.B. die Ausnahme von der Zweckbindung bei der Weiterverarbeitung für Forschungszwecke in Art. 5 Abs. 1 lit. b DS-GVO oder die Ausnahme von der Speicherbegrenzung in Art. 5 Abs. 1 lit. e DS-GVO.

138 *Roßnagel*, ZD 2019, 157 (157).

Ergebnissen der Testpersonen profitieren. In beiden Fällen ist die Bereitschaft der Patienten – etwa zur Erteilung einer datenschutzrechtlichen Einwilligung – regelmäßig sehr hoch.[139]

Dementsprechend müssen medizinische Forschungsprojekte datenschutzrechtlich nach dem jeweils verfolgten Zweck gesondert betrachtet werden. Die Datenverarbeitung im Rahmen eines medizinischen Forschungsprojekts kann dabei in einem direkten Behandlungszusammenhang stehen. So verfolgt die Datenverarbeitung der Datenbrille aus dem Forschungsprojekt IDeA unter anderem das Ziel der Behandlung der Augenkrankheit AMD und daneben – als sekundären Zweck – Forschungsinteressen wie die Verbesserung der dabei eingesetzten Technologien und Analysealgorithmen. Ferner können auch klinische Studien oder langfristige medizinische Forschungsprojekte durchgeführt werden, die aufgrund der erst später eintretenden Erkenntnisse für den Patienten, dessen personenbezogene Daten verarbeitet werden, keinen Behandlungserfolg generieren.[140] Je nach Zweck sind unterschiedliche rechtliche Anforderungen zu beachten. Oftmals werden in Forschungsprojekten beide Zielrichtungen verfolgt. Dies hat zur Folge, dass zum einen für jede Datenverarbeitung für einen bestimmten Zweck, stets auch eine gesonderte Rechtsgrundlage gefunden werden muss und zum anderen die sich jeweils ergebenden unterschiedlichen datenschutzrechtlichen Anforderungen eingehalten werden müssen.

In einem ersten Schritt hat also der Verantwortliche für jede Datenverarbeitung eine Rechtfertigung – also eine taugliche Rechtsgrundlage – zu finden.

### 3.3.1 Datenverarbeitungen der an HIVE-Lab beteiligten Forschungsprojekte (z.B. IDeA)

Die Frage der Rechtfertigung der Datenverarbeitungen der an HIVE-Lab beteiligten Forschungsprojekte muss primär von den Forschungsprojekten als Verantwortliche geklärt werden. So sind beispielsweise die Verantwortlichen in IDeA bei ihren Datenverarbeitungen im Zusammenhang mit der Datenbrillen-Anwendung verantwortlich und müssen sich dementsprechend um eine Rechtfertigung kümmern. Sofern das HIVE-Lab als (auch datenschutzrechtlich) verantwortliche Gesellschaft oder ein weiteres an HIVE-Lab beteiligtes Forschungsprojekt für ein Projekt als – zumindest gemeinsam – Verantwortlicher zu qualifizieren sind, müssen sie (nur) für die Verarbeitungsschritte eine Rechtfertigung aufweisen, über die sie tatsächlich über Mittel und Zwecke entscheiden. In aller Regel wird sich die Leistung des HIVE-Labs jedoch nur auf unterstützende Handlungen beschränken. Wenn diese keinerlei Bezug zu personenbezogenen Daten aufweisen, ergeben sich keine datenschutzrechtlichen Pflichten. Erstreckt sich die Unterstützung jedoch auf die Verarbeitung personenbezogener Daten, wird typischerweise eine Auftragsverarbeitung vorliegen wird. Für diese muss dann jeweils ein Vertrag nach Art. 28 DSGVO geschlossen werden. Die Rechtfertigung der einzelnen Projekte kann jedoch nur unter Kenntnis der genauen Anwendung und der datenschutzrechtlichen Verantwortlichkeit geprüft werden. Für die datenschutzrechtliche Herausforderungen im Bereich von AR-Brillen in der Öffentlichkeit kann exemplarisch auf die Ausführungen zu IDeA verwiesen werden.[141] Sofern eine Auftragsverarbeitung für die Verantwortlichen des konkreten Forschungsprojekts in Betracht kommt, ist keine eigene Rechtsgrundlage des HIVE-Labs erforderlich. In diesem Fall ist aber auf die Einhaltung von Art. 28 DSGVO zu achten und insbesondere ein entsprechender Vertrag abzuschließen.

### 3.3.2 Unterstützung der einzelnen Projekte

Das HIVE-Lab bietet eine Reihe an Unterstützungshandlungen für diverse Forschungsprojekte an, die jeweils unterschiedliche Datenverarbeitungen voraussetzen. Für den Fall, dass die

---

139 *Pommerening*/*Müller* 2014, 19.

140 *Pommerening*/*Müller* 2014, 61 f.

141 S. Kap. 2.2.5.

datenschutzrechtlichen Normen Anwendung finden[142] und das HIVE-Lab Verantwortlicher i.S.d. DS-GVO ist[143], muss jede Datenverarbeitung auf eine Rechtsgrundlage gestützt werden können.

Die erste Weichenstellung ist dabei die Frage, ob besondere Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DS-GVO (insb. Gesundheitsdaten) verarbeitet werden.

Gesundheitsdaten sind nach Art. 4 Nr. 12 DS-GVO personenbezogene 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. Dazu gehören nach EG 35 Satz 2 DS-GVO unter anderem Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen.

Gesundheitsdaten und sonstige sensible Daten i.S.d. Art. 9 Abs. 1 DS-GVO dürfen nur verarbeitet werden, sofern sie den Voraussetzungen eines der speziellen in Art. 9 Abs. 2 DS-GVO genannten Tatbestände genügen.[144] Hierbei kommen insbesondere die Erforderlichkeit für wissenschaftliche Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz) oder eine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) in Betracht. Für sonstige personenbezogene Daten kommen bei HIVE-Labs eine Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO) sowie die Erforderlichkeit für legitime Interessen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO) in Frage.[145]

Die Prüfung der Rechtmäßigkeit einer Datenverarbeitung lässt sich nur bei Kenntnis des Anwendungsszenarios klären. Im Bereich des – zumindest teilweise – medizinischen Forschungsprojekts HIVE-Lab mit der Verarbeitung von sensiblen Daten, wird in vielen Fällen die Einholung von (ausdrücklichen) Einwilligungen erforderlich, jedenfalls aber zu empfehlen sein. Im Folgenden soll das Body of Knowledge als bereits feststehende Anwendung des HIVE-Labs herausgegriffen und hinsichtlich der datenschutzrechtlichen Rechtfertigung genauer untersucht werden.

### 3.3.3 Body of Knowledge

Das Body of Knowledge ist eine Datenbank, in der eine Vielzahl an Forschungsdaten gespeichert werden sollen, die für zukünftige Forschungen nützlich sein könnten. In dieser Datenbank werden einerseits viele Daten gespeichert, die – zumindest zunächst – keinen Personenbezug aufweisen und für die demensprechend die datenschutzrechtlichen Normen nicht beachtet werden müssen (z.B. Computer-Codes). Nicht zuletzt aufgrund des Gesundheitskontextes werden andererseits auch viele personenbezogene Daten gespeichert (z.B. Gesundheitsdaten der Teilnehmer an Forschungsprojekten).

Zu beachten ist dabei, dass ein Personenbezug, insbesondere bei einer Zugänglichmachung für die Öffentlichkeit, nachträglich entstehen kann – ohne dass dies dem Verantwortlichen bekannt

---

142 S. hierzu Kap. 3.1.

143 S. hierzu Kap. 3.2.

144 S. hierzu Kap. 2.2.3.

145 Zu den genauen Anforderungen dieser Normen s. Kap. 2.2.5.1.

ist. So ist ein dynamischen „Hineinwachsens“ in den Personenbezug während der Speicherdauer gerade bei Datenbanken denkbar, die von mehreren Verarbeitern bespeist werden. Durch eine Verknüpfung von an sich nicht-personenbezogenen Daten kann aufgrund der Kumulierung genügender Merkmale ein Personenbezug entstehen. Je größer die Datenmenge und je mehr Verknüpfungsmöglichkeiten bestehen, desto wahrscheinlicher wird es, eine Person identifizieren zu können – selbst, wenn dies nicht beabsichtigt ist.[146]

Liegt ein Personenbezug vor, bedarf es für die Datenverarbeitungen des Body of Knowledge einer datenschutzrechtlichen Rechtfertigung. Aufgrund der Verarbeitung von Gesundheitsdaten, muss einer der in Art. 9 Abs. 2 DS-GVO genannten Tatbestände erfüllt sein. Die Beurteilung der Rechtfertigung richtet sich dabei nach der konkreten Ausgestaltung und genauen Art der Verwendung des Body of Knowledge.

Im Bereich der (medizinischen) Forschung ist zwischen verschiedenen Stufen der Datenverarbeitung zu unterscheiden:[147]

- Erhebung der (Primär-)Daten
- Datenverarbeitung im Sinne einer Auswertung und Analyse
- Weiterverarbeitung von (Sekundär-)Daten
- Zugänglichmachung und Publikation
- Übertragung in Drittländer.

Jeder der genannten Schritte enthält einen gesonderten Eingriff in die Rechte und Freiheiten der Betroffenen.

Im Folgenden soll auch bei der Body of Knowledge eine gesonderte Betrachtung der möglichen Nutzungen der Datenbank erfolgen. Dabei muss bereits bei der Analyse der ersten (Erhebung) und auch der zweiten Verarbeitung (z.B. Speicherung) die weitere Verwendungsabsicht berücksichtigt werden, da die originäre Datenerhebung nicht singulär steht, sondern eben für die weitere Verwendung erfolgt. Es wäre mithin praxisfern, wenn man eine möglicherweise beabsichtigte Veröffentlichung der Daten bei der Abwägung auf Erhebungsebene völlig ausklammern würde. Zudem würde dies auch dem datenschutzrechtlichen Vorsorgegedanken widersprechen. Dennoch ist eine Aufteilung in die einzelnen Verarbeitungsstufen zur Sortierung der Abwägung hilfreich. Hierdurch kann die für die Abwägung entscheidende unterschiedliche Eingriffsqualität verdeutlicht werden.

#### 3.3.3.1 Erhebung der (Primär-)Daten und Speicherung

Durch das Anlegen der Body of Knowledge und das Einspeisen der Daten werden auch personenbezogene Daten erhoben und gespeichert. So könnten Daten gespeichert werden, die auf die Gesundheit einer konkreten Person schließen lassen; etwa die Perimetrie-Daten der Träger der IDeA-Brillen. Durch die Erhebung und Speicherung wird das Recht auf informationelle Selbstbestimmung der Betroffenen beeinträchtigt.

Eine mögliche Rechtfertigung wäre die Erforderlichkeit für wissenschaftliche Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz).[148] Nach § 27 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich

146 *Hornung*/*Wagner*, CR 2019, 565 (568).

147 *Roßnagel*, ZD 2019, 157 (160).

148 S. zu den genauen Voraussetzungen Kap. 2.2.5.1.2.

überwiegen. Das Forschungsprojekt HIVE-Lab verfolgt ebenso wie das Forschungsprojekt IDeA wissenschaftliche Forschungszwecke im Bereich der Gesundheitsforschung.

Die Verarbeitung muss dabei insbesondere dem Erforderlichkeits- und dem Angemessenheitsprinzip genügen. Die Verarbeitung ist erforderlich, sofern kein gleich geeignetes, weniger belastendes Mittel zur Erreichung des konkreten Forschungszwecks besteht. Der Zweck des Body of Knowledge ist die Schaffung eines digitalen Orts zur Speicherung von Forschungsergebnissen, der für die übrigen Mitglieder des HIVE-Labs zur Verfügung gestellt werden soll.

Ein milderes Mittel kann u.a. eine Verarbeitung von anonymisierten oder pseudonymisierten Daten sein. Die zu klärende Frage ist, ob für die jeweilige Anwendung die Identität der betroffenen Personen erforderlich ist. Je nach genauem Forschungsgebiet kann jedoch – insbesondere im medizinischen Beriech – eine Identifikation des Betroffenen für den Forschungserfolg notwendig sein, weshalb zumindest anonyme Daten in einigen Fällen kein gleich geeignetes Mittel darstellen werden. Eine Pseudonymisierung wird jedoch in den meisten Forschungsprojekten – ohne größere Schwierigkeiten – durchführbar sein. Eine vollständige Speicherung der Daten wird oftmals nicht erforderlich und damit rechtswidrig sein.

Ein weiteres milderes Mittel ist die Implementierung eines Identitätsmanagementkonzepts, das etwa zwischen einzelnen Verwendungszwecken, den jeweils Zugreifenden und Datenkategorien unterscheidet. Einem Forschungsprojekt, das keine Gesundheitsdaten eines Teilnehmers für seine Forschung benötigt, Zugriff auf sensible Daten zu geben, ist nicht erforderlich. Bei anderen Projekten kann womöglich nicht ausgeschlossen werden, dass sie vollen Zugriff – auch auf identifizierende Merkmale und sensible Daten – benötigen, um ihr Forschungsziel zu erreichen. Insbesondere im Bereich der medizinischen Forschung ist im Rahmen des Identitätsmanagementkonzepts die Trennung von identifizierenden Daten und nichtidentifizierenden Gesundheitsdaten empfehlenswert.[149] So kann durch ein Rollenkonzept zum einen dem medizinischen Fachpersonal ein umfassender Zugriff ermöglicht werden und den nicht-medizinischen Projektmitgliedern, das andere Funktionalitäten einer Anwendung untersucht, dementsprechend auch nur ein eingeschränkter – für diesen Arbeitsschritt erforderlicher – Zugriff gewährt werden.

Im Rahmen der Abwägung der Interessen ist unter anderem zu beachten, dass bei HIVE-Lab oftmals kein unmittelbarer Behandlungszusammenhang der betroffenen Person besteht. Darüber hinaus ist oft unklar, welche Sekundärnutzung der Daten und durch welche Personen (z.B. neue möglicherweise fachfremde Forschungsprojekte oder Unternehmen) erfolgt. Bereits bei diesem ersten Verarbeitungsschritt sind zukünftig wahrscheinliche Nutzungen zu berücksichtigen. Ebenso ist das Risiko für Zweckentfremdungen zu beachten. Die genannten Risiken werden durch die mitunter hohe Lebensdauer der Daten noch gesteigert.[150]

Im Ergebnis ist der Weg über Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz deshalb mit deutlichen Rechtsunsicherheiten verbunden. Die sicherste und einfachste Möglichkeit ist folglich die Einholung einer ausdrücklichen Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) unter der genauen Angabe der jeweiligen Zwecke.[151] Der Nachteil der Einwilligung ist unter anderem ihre jederzeitige Widerruflichkeit.

Nach Art. 7 Abs. 3 Satz 2 DS-GVO wird durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

---

149 *Pommerening*/*Müller* 2014, 64 f.

150 *Pommerening*/*Müller* 2014, 89.

151 Zu den Anforderungen einer Einwilligung s. Kap. 3.5.

Es entsteht hingegen ein unmittelbarer Anspruch des Betroffenen auf Löschung der erhobenen personenbezogenen Daten (Art. 17 Abs. 1 lit. b DS-GVO) und auf zukünftige Unterlassung.[152]

#### 3.3.3.2 Anpassung und Veränderung

Eine mögliche weitere Verarbeitung wäre die Anpassung und Veränderung der Daten durch das HIVE-Lab. Aktualisiert das HIVE-Lab personenbezogene Daten (z.B. Wohnanschrift der Teilnehmer), so erfolgt eine (datenschutzrechtliche) Anpassung der Daten. Werden die Daten etwa mit Kommentaren versehen oder zumindest die Funktion implementiert, sodass andere die Daten kommentieren können, wird eine Veränderung der Daten vorgenommen. Die Daten werden umgestaltet, sodass sich ihr Informationsgehalt ändert.[153] Dies kann mitunter eine zusätzliche Eingriffsqualität darstellen.

Nichtsdestotrotz dürfte auch diese Verwendung unter denselben Prämissen für wissenschaftliche Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz) erforderlich sein, sofern diese Rechtsgrundlagen die grundsätzliche Verarbeitung tragen. Aufgrund der weiteren Eingriffsdimension muss hingegen gewährleistet sein, dass insbesondere die Anpassungen und Veränderungen sachlich richtig sind. Dies wird auch vom Grundsatz der Richtigkeit nach Art. 5 Abs. 1 lit. d DS-GVO gefordert. Ein fehlerhaft verändertes Datum könnte insbesondere im Verlauf der Zeit durch einen Kontextverlust falsch sein bzw. werden. Bei einer Anpassung und Veränderung ist es im Sinne der Nachvollziehbarkeit empfehlenswert, die Änderungen in Form einer Versionierung oder mit Hilfe eines Audit-Trails nachvollziehbar zu machen.[154]

Die ausdrückliche Einwilligung zur Erhebung und Speicherung könnte auch auf diese weiteren Verarbeitungsschritte erstreckt werden.

#### 3.3.3.3 HIVE-Lab-interne Nutzung

Die gespeicherten Daten könnten ausschließlich von den Mitgliedern des Forschungsprojekts HIVE-Lab (intern) genutzt werden. Die teilnehmenden Projekte könnten auf die Daten zugreifen und diese ggf. auch verändern, anpassen oder in sonstiger Weise verarbeiten. Werden die gespeicherten Informationen für die (internen) (Forschungs-)Zwecke der HIVE-Lab-Forschungsprojekte genutzt, liegt eine (datenschutzrechtliche) Verwendung vor, die ebenfalls eine Verarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO ist.[155] Diese Verwendung kann je nach Forschungsgruppe und -zweck unterschiedlich sein. Der Zweck der internen Nutzung muss jedoch nach dem Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DS-GVO klar festgelegt werden. Der Zweck der Body of Knowledge ist die Zurverfügungstellung von möglichen forschungsrelevanten Daten für die Mitglieder der HIVE-Lab-Forschungsgruppe. Je weiter der Zweck gefasst wird, desto größer ist der Eingriff in die Rechte und Freiheiten der betroffenen Personen. Je genauer der Zweck eingegrenzt wird, desto einfacher wird eine Erforderlichkeit anzunehmen sein.

Eine denkbare interne Nutzung ist die Vermittlung von Testpersonen. So könnten HIVE-Lab-intern die Kontaktdaten von beispielsweise älteren Testpersonen vermittelt werden, die für ein anderes Forschungsprojekt von HIVE-Lab interessant sind. Betrachtet man diesen Zweck, so wäre die Übermittlung der (personenbezogenen) Kontaktdaten erforderlich. Die Übermittlung

---

[152] Der Verantwortliche hat nach Art. 17 Abs. 2 DS-GVO auch Dritte, die diese Daten erhalten haben, über diese Ansprüche zu unterrichten. Die Ansprüche richten sich auch gegen diese Dritte.

[153] Kühling/Buchner-*Herbst*, Art. 4 Rn. 25.

[154] *Pommerening*/*Müller* 2014, 95.

[155] Sofern das HIVE-Lab keine eigene Gesellschaft ist, stellt jede Verwendung der Daten durch nicht an der Erhebung und Speicherung beteiligten HIVE-Lab-Mitglieder auch eine Übermittlung i.S.d. Art. 4 Nr. 2 DS-GVO dar.

von Gesundheitsdaten über die Sehfähigkeit von älteren Menschen wäre hingegen für ein Projekt, das Rückenbeschwerden von älteren Menschen behandeln will, nicht erforderlich. Durch ein Identitätsmanagementsystem könnte jedoch ein Zugriff auf die gewünschten Daten beschränkt werden.

Erhobene und bereits verarbeitete (z.B. für die interne Nutzung) Forschungsdaten sind nach dem Grundsatz der Speicherbegrenzung des Art. 5 lit. e HS. 1 DS-GVO grundsätzlich zu löschen. Gerade im Forschungsbereich widerspräche dies allerdings häufig dem berechtigten Interesse der Nachprüfung von Forschungsergebnissen oder der weiteren Nutzung für weitere Forschungsprojekte oder langfristige Studien.[156] Würden die Forschungsprojekte gezwungen werden, dieselben Daten für einen anderen Zweck nochmals zu erheben, könnte argumentiert werden, dass dies sogar dem Grundsatz der Datenminimierung widerspräche.[157] Aus diesen Gründen eröffnet Art. 5 lit. e HS. 2 DS-GVO eine Ausnahme von dem Prinzip der Speicherbegrenzung. Die Daten dürfen länger gespeichert werden als dies für den ursprünglichen Zweck erforderlich ist. Diese Speicherung darf hingegen nicht zu einer unbegrenzten Vorratsdatenspeicherung führen. Vielmehr muss der sekundäre künftige wissenschaftliche Zweck, nach der jeweiligen Wissenschaftsdisziplin und dem konkreten Forschungskontext absehbar sein.[158]

Sollen Forschungsdaten langfristig gespeichert und genutzt werden, sind sie zuvor zu anonymisieren oder zu pseudonymisieren. Eine originale Speicherung ist nur dann zulässig, wenn nur in dieser Form die Zwecke der wissenschaftlichen Funktionen des Body of Knowledge erfüllt werden können. Als Richtwert für die Speicherdauer im Forschungsbereich zur Überprüfbarkeit der Forschungsdaten sieht *Roßnagel* zehn Jahre an.[159] Entscheidend ist damit, ob für den jeweiligen Forschungserfolg ein Personenbezug notwendig ist oder auch eine pseudonymisierte oder anonymisierte Form der Daten genügt.

Art. 89 Abs. 1 Satz 4 DS-GVO fordert dabei für Weiterverarbeitungen von Daten für Forschungszwecke ausdrücklich eine anonyme Verarbeitung. Nur wenn die Zwecke der wissenschaftlichen Forschung nicht erfüllt werden können, soll eine Ausnahme von diesem Grundsatz möglich sein. Diese Sekundärnutzung stellt eine Zweckänderung bezüglich der Primärnutzung dar. Diese ist jedoch nach Art. 5 Abs. 1 lit. b DS-GVO für wissenschaftliche Forschungszwecke „nicht als unvereinbar mit den ursprünglichen Zwecken“ anzusehen. Der Verantwortliche darf mithin in der Regel davon ausgehen, dass eine Vereinbarkeit der beiden Zwecke vorliegt und eine Weiterverarbeitung ohne gesonderte Rechtsgrundlage möglich ist.[160] Es kann hingegen auch im Forschungsbereich vorkommen, dass die Risiken für die Rechte der betroffenen Person aufgrund der Weiterverarbeitung erheblich zunehmen. In diesem Fall sind für die Abwägung die Garantien des Art. 6 Abs. 4 DS-GVO maßgeblich. An dieser Stelle ist es erneut von Vorteil, wenn technische und organisatorische Maßnahmen ergriffen wurden (z.B. Pseudonymisierung und Sicherung der Zuordnungsregel der Pseudonymisierung), da hierdurch die Eingriffsintensität für die betroffenen Personen geringer ist und sich dies positiv auf die Abwägung auswirkt.[161]

Je nach Anwendungsfall könnten also Verarbeitungen zur internen Nutzung auch auf die Erforderlichkeit für wissenschaftliche Forschungszwecke (Art. 9 Abs. 2 lit. j DS-GVO i.V.m dem jeweiligen Landes- oder Bundesgesetz) gestützt werden. Ebenso ist eine Rechtfertigung nach

156 *Roßnagel*, ZD 2019, 157 (162).
157 *Roßnagel*, ZD 2019, 157 (162).
158 *Roßnagel*, ZD 2019, 157 (162).
159 *Roßnagel*, ZD 2019, 157 (162).
160 S. hierzu Kap. 2.2.2.
161 *Roßnagel*, ZD 2019, 157 (162).

Art. 9 Abs. 2 lit. a DS-GVO durch eine ausdrückliche Einwilligung unter Nennung des jeweiligen Verarbeitungszwecks möglich.

#### 3.3.3.4 Externe Nutzung

Die Daten des Body of Knowledge könnten auch Personen außerhalb des Forschungsprojekts HIVE-Lab zur Verfügung gestellt werden. Dabei könnten die Daten einem abgrenzbaren Personenkreis (z.B. dem BMBF), einem nichtabgrenzbaren Personenkreis (z.B. externen Forschungsprojekten oder Unternehmen) oder der Öffentlichkeit (z.B. durch Veröffentlichung im Internet) zur Verfügung gestellt werden. Sofern die Daten der Body of Knowledge weiteren Personen zugänglich gemacht werden, liegt eine Übermittlung, Verbreitung oder eine andere Form der Bereitstellung i.S.d. Art. 4 Nr. 2 DS-GVO vor. Fraglich ist, ob eine Übermittlung an Dritte oder eine Veröffentlichung erforderlich nach Art. 9 Abs. 2 lit. j DS-GVO i.V.m. dem jeweiligen Landes- oder Bundesgesetz sind.

Je mehr Akteure an der Datenverarbeitung involviert sind, desto mehr Einblicke in die Privatsphäre der Betroffenen werden ermöglicht und umso mehr potenzielle Risikoquellen bestehen für eine Verletzung des Schutzes personenbezogener Daten. Eine Veröffentlichung im Internet ist für die betroffenen Personen besonders eingriffsintensiv, da die Daten einer unüberschaubaren Anzahl an Personen zugänglich gemacht werden und diese nun unkontrollierbar weitere Verarbeitungen vornehmen können.[162]

Wollen externe Forschungsprojekte oder Unternehmen auf personenbezogene Daten zugreifen, sind diese vor dem externen Zugriff zu anonymisieren.[163] Eine datenschutzfreundliche Möglichkeit für externe Zugriffe besteht in der Zurverfügungstellung von Dummy-Dateien, die in Aufbau und Merkmalsausprägungen den Originaldaten gleichen. Der externe Forscher stellt für seine jeweilige Forschungsfrage spezielle Abfragen. Diese Abfragen werden an die Verantwortlichen des Body of Knowledge weitergeleitet, woraufhin diese die Abfragen auf die Originaldaten anwenden. Die Ergebnisse dieser Auswertung werden wieder an die externen Forscher geleitet, sodass diese den Erkenntnisgewinn ohne Kenntnis der Identität der betroffenen Personen erlangen.[164] Anonymisierungsmaßnahmen sollten zudem mit vertraglichen Vereinbarungen zur Nutzung und (Nicht-)Weitergabe der Daten flankiert werden.[165]

Eine Veröffentlichung von Forschungsergebnissen darf in den hier relevanten Szenarien[166] ausschließlich in anonymisierter Form erfolgen. Dies verlangen sowohl die Regelung des § 27 Abs. 4 BDSG als auch die entsprechenden landesdatenschutzrechtlichen Normen (z.B. § 24 Abs. 4 HDSIG). Diese Regelungen basieren auf den Gefahren der Re-Identifizierbarkeit durch die Öffentlichkeit und des tiefen Eingriffs im Bereich der medizinischen Forschungen bei Gesundheitsdaten.[167]

Zusammenfassend lässt sich sagen, dass eine externe Nutzung von sensiblen Daten (hier vor allem Gesundheitsdaten) umso schwieriger wird, je mehr Personen Zugriff erhalten und je entfernter der Personenkreis von dem Forschungsprojekt HIVE-Lab ist.

---

162 *Herfurth*, ZD 2018, 514 (517).

163 *Pommerening*/*Müller* 2014, 92.

164 *Pommerening*/*Müller* 2014, 93.

165 *Pommerening*/*Müller* 2014, 93.

166 Die gesetzlichen Ausnahmen betreffen Forschungsergebnisse über Ereignisse der Zeitgeschichte, bei denen eine Anonymisierung regelmäßig unmöglich ist. Dies ist weder in IDeA noch in HIVE-Lab relevant.

167 *Roßnagel*, ZD 2019, 157 (163).

## 3.4 Technische und organisatorische Maßnahmen

Selbst wenn die Datenverarbeitung grundsätzlich zulässig ist, enthält das Datenschutzrecht weitere Anforderungen an ihre Durchführung. Das Prinzip des Datenschutzes durch Systemgestaltung (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) gem. Art. 25 DS-GVO sowie technische und organisatorische Sicherungsmaßnahmen gem. Art. 32 DS-GVO fordern jeweils Maßnahmen entsprechend dem Risiko für die Rechte und Freiheiten natürlicher Personen.

Wird eine Datenverarbeitung auf Art. 9 Abs. 2 lit. j DS-GVO (i.V.m. dem jeweiligen Landes- oder Bundesgesetz) gestützt, verlangt Art. 89 Abs. 1 DS-GVO (ebenso wie die deutschen Gesetze, z.B. § 27 Abs. 1 Satz 2 BDSG, § 24 Abs. 1 Satz 2 HDSIG) besondere Garantien zum Ausgleich für die Privilegierung der Forschung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen.

Das Bundesdatenschutzgesetz nennt in § 22 Abs. 2 Satz 2 BDSG ebenso wie das Hessische Datenschutzgesetz in § 20 Abs. 2 Satz 2 HDSIG neun Beispiele für die von Art. 89 Abs. 1 DS-GVO geforderten Garantien:

1. technische und organisatorische Maßnahmen, um die Konformität mit der DS-GVO sicherzustellen,

2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,

3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,

5. Pseudonymisierung personenbezogener Daten,

6. Verschlüsselung personenbezogener Daten,

7. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

8. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder

9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben des BDSG bzw. des HDSIG sowie der DS-GVO sicherstellen.

Zwei mögliche technische und organisatorische Maßnahmen sind die Anonymisierung und die Pseudonymisierung. Sie bieten sich auch für den Bereich der wissenschaftlichen Forschung im medizinischen Bereich an. Im Wesentlichen werden die ursprünglich personenbezogenen Daten von den betroffenen Personen in einer jeweils unterschiedlichen Ausprägung entkoppelt.[168] Wird der Personenbezug vollständig entfernt, liegen anonymisierte Daten vor. Wenn der Personenbezug nicht irreversibel entfernt wird, sondern lediglich in der Weise verändert, dass die

[168] Simitis/Hornung/Spiecker Döhmann-*Hansen*, Art. 4 Nr. 5 DS-GVO Rn. 1.

zugehörigen betroffenen Personen zwar entkoppelt, aber mithilfe einer Zusatzinformation re-identifizierbar sind, spricht man von pseudonymisierten Daten.[169] Beide Verfahren eignen sich zur Minimierung der Risiken für die personenbezogenen Daten.

### 3.4.1 Anonymisierung

Eine Anonymisierung ist das Verändern von personenbezogenen Daten, sodass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht bzw. nicht mehr identifiziert werden kann.[170] Anonymisierte Daten weisen mithin keinen Personenbezug auf, womit auch die Vorgaben des Datenschutzrechts nicht mehr anzuwenden sind.

Aufgrund des oftmals nachträglich eintretenden (plötzlich oder „schleichend" auftretenden) Personenbezugs kann sich die Einordnung und Wertung eines Datums als anonym im Laufe der Zeit ändern.[171] So könnte durch Kombination der medizinischen personenbezogenen Daten, die an sich keinen Rückschluss auf die Identität des Betroffenen erlauben, mit anderen Daten eine Identifizierung ermöglicht werden. Wenn die Kombinationsmöglichkeiten nach und nach größer werden, kann dieser Prozess graduell ablaufen. Die Schwierigkeit an einem solchen schleichenden Personenbezug ist, dass er sich nur sehr schwer bis gar nicht voraussagen lässt.

Gerade im medizinischen Bereich mit vielen sensiblen Daten ist deshalb zu empfehlen, bereits prophylaktisch durch technische und organisatorische Maßnahmen abzusichern, dass Datenübermittlungen nur zweckbezogen und an einen bekannten bzw. zumindest bestimmbaren Nutzerkreis erfolgen..

Ein Hindernis für Anonymisierungen im medizinischen Forschungsbereich kann der Umstand darstellen, dass viele Anwendungen nicht durch anonymisierte Daten durchgeführt werden können, da Krankheitsverläufe (bzw. der oftmals langwierige Genesungsprozess) nur mit Hilfe von Follow-Ups im langfristigen Verlauf (durch individuelle Feedbacks z.B. über neue Therapiemöglichkeiten, Risiken oder Zufallsbefunde) möglich sind.[172]

### 3.4.2 Pseudonymisierung

Im Gegensatz zur Anonymisierung ist die Pseudonymisierung in der DSGVO legaldefiniert. Gemäß Art. 4 Nr. 5 DSGVO ist sie 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. Anders als bei der Anonymisierung besteht bei der Pseudonymisierung also eine Zuordnungsregel, die die Identifizierung der betroffenen Person ermöglicht. Diese Zuordnungsregel ist dabei einer – in aller Regel größeren – Gruppe (z.B. Forschungsprojekte, die an HIVE-Lab teilnehmen) nicht bekannt und einer – meist kleinen – Gruppe bekannt; für Letztere handelt es sich um personenbezogene Daten.[173]

Der Grad zur Pseudonymität ist erreicht, sofern ein Kennzeichen benutzt wird, durch das die Wahrscheinlichkeit, dass Daten einer konkreten Person zugeordnet werden können, so gering ist, dass sie ohne Kenntnis der passenden Zuordnungsregel zwischen Kennzeichen und Person

---

169 Simitis/Hornung/Spiecker Döhmann-*Hansen,* Art. 4 Nr. 5 DS-GVO Rn. 13 f.

170 Paal/Pauly-*Ernst,* Art. 4 Rn. 48.

171 S. hierzu umfassend *Hornung*/*Wagner*, CR 2019, 565.

172 *Pommerening*/*Müller* 2014, 44.

173 BeckOK Datenschutzrecht-*Schild,* Art. 4 Rn. 72.

nach allgemeiner Lebenserfahrung und dem aktuellen Stand der Wissenschaft praktisch ausscheidet.[174]

Bietet man pseudonymisierte Daten der Öffentlichkeit an, steigt die Wahrscheinlichkeit, dass eine Gruppe Kenntnis von Kennzeichen erhält, die eine Identifizierung ermöglichen. Eine Pseudonymität der Daten entfällt damit in aller Regel.[175]

## 3.5 Gestaltung einer Einwilligungserklärung

Die Einwilligung als Rechtsgrundlage bietet eine sichere Möglichkeit, um Datenverarbeitungen im medizinischen Forschungskontext zu legitimieren. Die Erklärungen müssen hierfür jedoch rechtskonform gestaltet sein. Eine rechtmäßige Einwilligung muss für jede Datenverarbeitung gesondert eingeholt werden, um so alle Umstände des jeweiligen Einzelfalls zu erfassen. Im Folgenden sollen zunächst rechtliche Anforderungen an eine wirksame Einwilligungserklärung speziell für den medizinischen Bereich dargestellt werden. Zudem sind Quellen für Mustereinwilligungen genannt. Diese Muster können dann mithilfe des Anforderungskatalogs bearbeitet werden und sodann im jeweiligen Einzelfall unter Berücksichtigung der konkreten Umstände zu einer Einwilligung zusammengeführt werden.

### 3.5.1 Rechtliche Anforderungen im medizinischen Kontext

Die DS-GVO stellt an eine Einwilligung einige Anforderungen. Die Erklärung muss unter anderem:

- für einen oder mehrere bestimmte Zwecke (Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO),
- freiwillig (Art. 4 Nr. 11 DS-GVO),
- vor der Verarbeitung informiert (Art. 4 Nr. 11 DS-GVO) und
- ausdrücklich (Art. 9 Abs. 2 lit. a DS-GVO)

abgegeben werden. Im Folgenden sollen die Eckpunkte einer Einwilligungserklärung – insbesondere für den Forschungsbereich – dargestellt werden. Wie für viele rechtliche Texte wie Verträge, AGBs oder Betriebsvereinbarungen gilt auch für Einwilligungserklärungen, dass diese kein „Einheitsanzug“ sind, sondern individuell „maßgeschneidert“ werden müssen. Eine passgenaue und wirksame Erklärung erweist sich mangels Kenntnis der genauen Umstände des Einzelfalls als unmöglich. Durch Berücksichtigung der folgenden Eckpunkte, kann jedoch für alle Einzelfälle eine jeweils individuelle, die unterschiedlichen Umstände berücksichtigende, Erklärung formuliert werden.

#### 3.5.1.1 (Konkreter) Zweck

Die Einwilligung muss für einen oder mehrere bestimmte Zwecke gegeben werden (Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO). Diese Zwecke müssen dem Betroffenen zum Zeitpunkt der Abgabe so deutlich vorhersehbar sein, dass er sich ein Bild von den für ihn bestehenden Chancen und Risiken machen kann. Bloße Blanko-Einwilligungen sind rechtswidrig. Es reicht mithin nicht aus, dass in eine Datenweitergabe an nicht bestimmbare Dritte eingewilligt wird.[176] Vielmehr wäre zumindest der Kreis der Personen (z.B. behandelnder Augenoptiker oder das Unternehmen, das die Augmentierung weiterentwickelt) anzugeben.

Freilich ist insbesondere für die medizinische Forschung ein möglichst weiter Zweck förderlich und unter Umständen auch notwendig. Hierdurch können die Daten länger gespeichert und

---

174 BeckOK Datenschutzrecht-*Schild*, Art. 4 Rn. 71.

175 *Pommerening*/*Müller* 2014, 43, m.w.N.

176 Simitis/Hornung/Spiecker Döhmann-*Klement*, Art. 7 Rn. 69.

genutzt werden sowie einem größeren Verarbeiterkreis zugänglich gemacht werden. Gerade im medizinischen Forschungsbereich kann es auch durchaus im Interesse des Patienten sein, dass nicht nur eine Forschungsgruppe mit ihren speziellen Interessen, Fähigkeiten und Forschungsansätzen mit den Daten forscht, sondern diese auch mit unterschiedlichen Betrachtungsweisen genutzt werden.[177] Eine längere Speicherung kann gerade im medizinischen Bereich zur Erstellung von neuen Hypothesen dienlich sein.

Diese Umstände vor Augen, erlaubt die Verordnung in EG 33 DS-GVO eine Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu erteilen, sofern dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die Anforderungen für die Einwilligung im Forschungsbereich sind bezüglich ihrer Bestimmtheit also geringer.

Werden hingegen sensible Daten i.S.d. Art. 9 Abs. 1 DS-GVO verarbeitet, müssen trotz dieser Privilegierung die betroffenen Kategorien der Daten, die Umstände und die möglichen Zweckänderungen angegeben werden.[178] Abstriche hiervon dürfen nur erfolgen, sofern dies aus wissenschaftlichen Gründen unmöglich ist.

Nichtsdestotrotz gilt, dass eine allgemeine Zweckbestimmung einer Einwilligung nur rechtmäßig sein kann, solange eine theoretische spätere Einholung zusätzlicher Einwilligungen aus technischen und organisatorischen Gründen unmöglich ist.[179]

Ist also eine spätere Sekundärverarbeitung durch weitere Projekte beabsichtigt, so ist dieser Zweck in der Einwilligungserklärung mit aufzunehmen.

#### 3.5.1.2 Freiwillig

Die Einwilligung muss ferner gem. Art. 4 Nr. 11 DS-GVO freiwillig erteilt worden sein. Es muss eine echte Wahl zwischen Zustimmung und Ablehnung bestehen, ohne dabei Nachteile zu erleiden (EG 42 Satz 5 DS-GVO).

Gerade im medizinischen Bereich können sich Patienten aufgrund ihrer Erkrankung von dem behandelnden oder Hilfe leistenden Personal abhängig fühlen. Dementsprechend sollte der Aufklärungs- und Einwilligungsprozess möglichst ergebnisoffen gestaltet werden, um eine wirklich freiwillige Einwilligung zu garantieren.[180]

#### 3.5.1.3 Informiert

Die Einwilligung hat nach Art. 4 Nr. 11 DS-GVO in einer informierten Weise zu erfolgen. Sie muss alle erforderlichen Informationen erhalten, um die Vor- und Nachteile einer Einwilligung bewerten zu können.

Kernelemente einer Einwilligung sind:

- Verantwortliche (EG 42 Satz 4 DS-GVO)
- Zwecke (EG 42 Satz 4 DS-GVO)
- Mögliche Übermittlung an Dritte (dies bestimmt maßgeblich den „Umfang“ der Einwilligung nach EG 42 Satz 2 DS-GVO)[181]
- Art der verarbeiteten Daten[182]

---

177 *Pommerening*/*Müller* 2014, 39.

178 *Roßnagel*, ZD 2019, 157 (161).

179 *Pommerening*/*Müller* 2014, 41.

180 *Pommerening*/*Müller* 2014, 38.

181 *Bergt* in Koreng/Lachenmann 2018, 937 (941).

182 Simitis/Hornung/Spiecker Döhmann-*Klement*, Art. 7 Rn. 72.

- Speicherdauer[183]
- Belehrung über die Möglichkeit eines Widerrufs (Art. 7 Abs. 3 Satz 3 DS-GVO)
- Ggf. Absicht einer ausschließlich automatisierten Entscheidung (Art. 22 Abs. 2 lit. c DS-GVO)
- Ggf. Datenübermittlung in ein Drittland (Art. 49 Abs. 1 Satz 1 lit. a DS-GVO)

Darüber hinaus postulieren Art. 13 f. DS-GVO weitere Informationspflichten des Verantwortlichen bei der Datenerhebung. Diese Informationspflichten sind letztlich auch Teil der Informiertheit der Einwilligung. Fehlen diese, wird die Einwilligung nicht per se unwirksam; es liegt jedoch ein Verstoß gegen Art. 13 f. DS-GVO vor.[184]

#### 3.5.1.4 Sprache, Transparenz, Hervorhebung

Art. 7 Abs. 2 Satz 1 DS-GVO fordert eine verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache. Sofern die Einwilligung zusammen mit anderen Erklärungen abgegeben wird, muss sichergestellt werden, dass (nur) sie besonders hervorgehoben ist (z.B. durch Fettdruck, Umrandung oder Farbe.[185]

Zwischen der Verständlichkeit auf der einen und der Vollständigkeit (Informiertheit) auf der anderen Seite besteht seit jeher ein Spannungsfeld. Wird die Einwilligung zu detailliert gestaltet, kann dies auf Kosten der Verständlichkeit gehen. Verzichtet man dagegen auf Informationen, kann es wiederum an der Vollständigkeit mangeln. Eine mögliche Lösung ist das Zwei-Stufen-Modell, in dem Betroffenen zunächst eine kürzere Information über die groben Züge der Verarbeitung gegeben und gleichzeitig eine Möglichkeit geboten wird, vollständige Informationen einzuholen.[186] Der Zugang zu dieser zweiten Stufe muss dabei ebenfalls so einfach wie möglich sein. Dieser Weg ist auch bei komplizierten medizinischen Verarbeitungen denkbar. So könnte zunächst eine grobe Information über die Datenverarbeitung gegeben und anschließend auf einer Website noch zusätzlich genaue Informationen über die einzelnen Datenverarbeitungen bereitgestellt werden.

#### 3.5.1.5 Widerruflichkeit

Die betroffene Person hat nach Art. 7 Abs. 3 Satz 1 DS-GVO jederzeit das Recht, ihre Einwilligung zu widerrufen. Hiervon ist sie nach Art. 7 Abs. 3 Satz 3 DS-GVO vor Abgabe der Einwilligung in Kenntnis zu setzen. Der Widerruf der Einwilligung muss dabei nach Art. 7 Abs. 3 Satz 4 DS-GVO so einfach wie die Erteilung der Einwilligung sein. Es ist umstritten, ob ein fehlender Hinweis auf die Widerruflichkeit, die Rechtswidrigkeit der Einwilligung bewirkt.[187] Außer wegen der expliziten Vorgabe in Art. 7 Abs. 3 Satz 3 DS-GVO ist dem Verantwortlichen also auch aus diesem Grund zu raten, dies in die Einwilligungserklärung aufzunehmen.

#### 3.5.1.6 Sensible Daten

Werden sensible Daten nach Art. 9 DS-GVO verarbeitet, so muss die Einwilligung ausdrücklich erteilt werden. Konkludente Erteilungen sind deshalb nicht möglich, in den hier relevanten Szenarien aber auch nicht erforderlich. Die besonderen Kategorien personenbezogener Daten müssen ausdrücklich, zumindest durch Nennung von Oberbegriffen wie „Gesundheitsdaten“ genannt werden. [188]

---

183 *Bergt* in Koreng/Lachenmann 2018, 937 (941).

184 *Bergt* in Koreng/Lachenmann 2018, 937 (942); Gola et al.-*Schulz*, Art. 7 Rn. 36.

185 *Bergt* in Koreng/Lachenmann 2018, 937 (938).

186 Simitis/Hornung/Spiecker Döhmann-*Klement*, Art. 7 Rn. 74.

187 *Bergt* in Koreng/Lachenmann 2018, 937 (939).

188 *Bergt* in Koreng/Lachenmann 2018, 937 (939).

### 3.5.2 Mustereinwilligungen

Es gibt einige Mustereinwilligungserklärungen, die an den konkreten Einzelfall anzupassen sind. Mustereinwilligungserklärungen eigenen sich jedoch als Ausgangspunkt für eine eigene Erklärung.

- Der Arbeitskreis Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland e.V. hat unter anderem speziell für medizinische Forschungen Mustereinwilligungserklärungen bereitgestellt. [189]
- Das Fraunhofer IOSB und die Fachhochschule Bielefeld haben einen Leitfaden zum Umgang mit dem Datenschutz in Projekten mit Mensch-Technik-Interaktion herausgegeben, in dem unter anderem eine Mustereinwilligung zu finden ist.[190]
- Eine ausführliche allgemeine rechtliche Mustereinwilligungserklärung findet sich zudem in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht.[191]

Mithilfe der Mustereinwilligungen und dem obigen Anforderungskatalog können die einzelnen Einwilligungserklärungen rechtssicher erstellt werden. Hierfür sollten die Mustereinwilligungen durch den Anforderungskatalog geändert bzw. erweitert werden.

## 3.6 Annex: Ausgewählte haftungsrechtliche Fragestellungen

Im Folgenden sollen als Annex zur datenschutzrechtlichen Prüfung ausgewählte haftungsrechtliche Herausforderungen betrachtet werden. Dabei sollen aufgrund der datenschutzrechtlichen Schwerpunktsetzung der Untersuchung lediglich ausgewählte Datenbrillen-spezifische haftungsrechtliche Problemstellungen betrachtet werden. Auf allgemeine haftungsrechtliche Fragestellungen (z.B. Lieferung einer fehlerhaften Hardware) wird in diesem Gutachten verzichtet. Auch die fehlerhafte Anwendung des technisch ordnungsgemäßen Produkts sowie eine Haftung des Trägers der Datenbrille bleiben außer Betracht.

Eine Haftung des HIVE-Labs (oder eines anderen Forschungsprojekts wie IDeA) kommt nur in Betracht, sofern diese rechtlich verselbständigt sind, also eine juristische Person oder rechtsfähige Personengesellschaft besteht (z.B. eine GbR). Sofern dies nicht erfolgt ist, kommt nur eine Haftung der einzelnen Forschungseinrichtungen innerhalb des Forschungsprojekts in Betracht. Im Falle einer rechtlichen Selbstständigkeit bestehen für das HIVE-Lab insbesondere zwei denkbare Haftungskonstellationen. Zum einen eine Haftung des HIVE-Labs gegenüber Dritten, die mit den Leistungen des HIVE-Labs in Berührung kommen und hierdurch geschädigt werden. Dies können bspw. Probanden, Unternehmen und externe Forschungsprojekte sein. Zum anderen könnten auch Forschungsprojekte, die Teil des HIVE-Lab-Projekts sind, haftungsrechtliche Ansprüche gegen die Gesellschaft des HIVE-Labs geltend machen. Sofern keine rechtliche Selbständigkeit vorliegt, haften die Forschungsprojekte des HIVE-Labs jeweils eigenständig. Dies gilt ebenfalls im Verhältnis zu Probanden, Unternehmen, internen und externen Forschungsprojekten. Im Folgenden soll – sofern nicht ausdrücklich ausgeführt – vereinfachend die Bezeichnung „HIVE-Lab“ stets diese beiden Möglichkeiten umfassen.

Für das Verhältnis der einzelnen HIVE-Lab-Forschungsprojekte gegenüber Dritten (z.B. Testpersonen) gelten die Ausführungen zu den haftungsrechtlichen Fragen des Projekts IDeA.[192] Die an HIVE-Lab Beteiligten können dabei je nach Konstellation Erfüllungs- oder

---

189 https://ak-med-ethik-komm.de/index.php?option=com_content&view=article&id=147&ltemid=153&lang=de.

190 https://www.iosb.fraunhofer.de/servlet/is/77819/GUIDELine.pdf, 20 ff.

191 *Bergt* in Koreng/Lachenmann 2018, 937.

192 S. Kap. 2.3.

Verrichtungsgehilfen für einen anderen Beteiligten am Forschungsprojekt sein, sodass letzterer für erstere im Außenverhältnis einzustehen hat.

Eine denkbare Haftungssituation wäre beispielsweise ein Anwendungsfall, in dem die Örtlichkeiten des HIVE-Labs einem Forschungsprojekt für Testzwecke zur Verfügung gestellt werden oder dem Forschungsprojekt in sonstiger Weise Hilfe geleistet wird und infolgedessen eine Rechtsgutsverletzung einer Testperson eintritt. Hier wird regelmäßig eine Haftung der Beteiligten des Forschungsprojekts vorliegen, während das HIVE-Lab bzw. die konkret mitwirkenden Forschungsprojekte des HIVE-Labs als Erfüllungs- oder Verrichtungsgehilfen einzuordnen sind.

Darüber hinaus wäre denkbar, dass das HIVE-Lab bzw. die jeweiligen Mitglieder des HIVE-Labs für eine Unterstützungsleistung auf die Hardware des jeweiligen Forschungsprojekts zugreifen und diese beschädigen oder fehlerhafte Daten übermitteln, aufgrund derer ein Schaden durch einen Softwarefehler eintritt. Gerade für dieses Verhältnis müsste die genaue Rechtsbeziehung zwischen den einzelnen Forschungsprojekten geklärt werden. Zudem ist fraglich, ob nur Mitglieder der HIVE-Lab-Forschungsgruppe die Leistungen des HIVE-Labs beanspruchen können oder auch externe Forschungsprojekte oder Unternehmen sich beteiligen können.

### 3.6.1 Vertragliche Mängelhaftung

Eine vertragliche Mängelhaftung nach den §§ 280 ff. BGB erfolgt in aller Regel lediglich inter partes, also nur zwischen den Vertragspartnern. Im Rahmen des HIVE-Labs kommen für das HIVE-Lab bzw. die Mitglieder des HIVE-Labs folgende Vertragsbeziehungen in Betracht:

- HIVE-Lab (verselbstständigt) – Dritte (z.B. Testpersonen oder externes Forschungsprojekt),
- HIVE-Lab (verselbstständigt) – Mitglieder des HIVE-Labs und
- Mitglieder des HIVE-Labs – Dritte (z.B. Testpersonen, interne und externe Forschungsprojekte).

Die Testperson (z.B. der Träger der Datenbrille) wird in aller Regel einen Vertrag über die Nutzung oder den Erwerb der Datenbrillen in der Entwicklungsphase mit einer juristischen Person des Forschungsprojekts schließen. Treten Mängel auf, so kann sich die Testperson im Rahmen der vertraglichen Mängelhaftung nur an die Person innerhalb des Vertragsverhältnisses halten. Das HIVE-Lab (verselbständigt) bzw. die Mitglieder des HIVE-Labs sind in diesem Fall in aller Regel Erfüllungsgehilfen.

Werden in den Vertrag auch beispielsweise Dienstleistungen des HIVE-Labs integriert, so wird typischerweise dennoch das HIVE-Lab bzw. die jeweiligen Mitglieder des HIVE-Labs nicht Vertragspartner und damit auch nicht Anspruchsgegner vertraglicher Haftungsansprüche sein. Nur dann, wenn das HIVE-Lab bzw. die jeweiligen Mitglieder des HIVE-Labs selbst Vertragspartei sind (also den Vertrag mit schließen oder sich insoweit durch einen Beteiligten des Forschungsprojekts vertreten lassen), kommt eine solche Haftung in Betracht. In diesem Fall wird es sich wiederum typischerweise darum drehen, ob der Anbieter (das Forschungsprojekt und das HIVE-Lab) einen möglichst umfassenden Haftungsausschluss in den Vertrag integrieren kann. Dieser muss sich jedoch an die Grenzen des allgemeinen AGB-Rechts halten.[193]

Übernimmt das HIVE-Lab für ein Forschungsprojekt eine vertraglich vereinbarte Dienstleistung, wie die Entwicklung einer Software für eine Anwendung oder das Zurverfügungstellen von „fehlerhaften“ Daten, die für das Training einer Software genutzt werden, könnte das Forschungsprojekt Regress bei dem HIVE-Lab bzw. dem jeweiligen Mitglied nehmen wollen. Sobald solche Leistungen des HIVE-Labs übernommen werden, ist es ratsam einen umfassenden

[193] S. Kap. 2.3.1.

Vertrag – je nach Vertragstyp, Art der Handlung und gewünschtem Verhältnis – mit einer genauen Regelung der Haftung zu schließen.

### 3.6.2 ProdHaftG

Eine Haftung für den Tod, die Verletzung des Körpers oder der Gesundheit oder einer Sache eines Dritten nach dem ProdHaftG kommt nur in Betracht, sofern das HIVE-Lab bzw. die jeweiligen Mitglieder des HIVE-Labs Hersteller i.S.d. ProdHaftG sind.

Hersteller im Sinne dieses Gesetzes ist, wer das Endprodukt, einen Grundstoff oder ein Teilprodukt hergestellt hat. Als Hersteller gilt auch jeder, der sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt (§ 4 Abs. 1 ProdHaftG).

Beschränkt sich die Leistung des HIVE-Labs auf reine Unterstützungstätigkeiten, scheidet eine Haftung nach dem ProdHaftG aus. Übernimmt das HIVE-Lab Teile der Herstellung der Software, könnte es als Hersteller eines Teilprodukts der finalen Anwendung angesehen werden.

Selbst für den Fall einer Annahme der Herstellereigenschaft, wird in der Erprobungsphase eine Haftung in aller Regel an einem mangelnden „Inverkehrbringen“ des Produkts scheitern.[194]

### 3.6.3 § 823 BGB

Nach § 823 Abs. 1 BGB ist derjenige einem anderen zum Schadensersatz verpflichtet, der vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht des anderen widerrechtlich verletzt.

Wie bereits dargestellt, wird eine deliktische Haftung für die Schäden Dritter in der Erprobungsphase von Datenbrillen im medizinischen Kontext in aller Regel an einem mangelndem Verschulden scheitern.[195] Stellt das HIVE-Lab beispielsweise die Örtlichkeiten zur Verfügung, innerhalb derer sich ein Unfall der Testperson aufgrund eines Softwarefehlers einer Datenbrille eines Forschungsprojekts ereignet, so ist das HIVE-Lab bzw. sind die Mitglieder des HIVE-Labs in aller Regel lediglich Verrichtungsgehilfen des jeweils verantwortlichen Forschungsprojekts. Wird das HIVE-Lab bzw. eines der Mitglieder des HIVE-Labs an einer Forschungstätigkeit tätig und führt diese zu einem Schaden (z.B. fehlerhafte Daten des HIVE-Labs führen zu dem Softwarefehler), so wird in der Entwicklungsphase oftmals kein Verschulden vorliegen.

Eine deliktische Haftung bezüglich der Rechtsgüter der Forschungspartner kann pauschal nicht ausgeschlossen werden. Hierbei ergeben sich jedoch keine neuen technikbedingten (AR/VR) Implikationen. Vielmehr richtet sich die Haftung nach den allgemeinen haftungsrechtlichen Regeln. Eine deliktrechtliche Haftung besteht immer dann, sobald ein vorwerfbares Handeln oder Unterlassen des HIVE-Labs vorliegt. Hierfür muss zumindest Fahrlässigkeit vorliegen.

### 3.6.4 Zwischenergebnis

Im Verhältnis zwischen einem teilnehmenden Forschungsprojekt des HIVE-Labs und einem Dritten (z.B. Testperson) gelten dieselben haftungsrechtlichen Erwägungen wie beim Forschungsprojekt IDeA. Im Stadium der Erprobung findet ein geringerer Maßstab Anwendung, sodass eine Haftung in der Regel ausscheidet. Derselbe Maßstab ist auch für das Verhältnis von HIVE-Lab zu Dritten anzuwenden, wonach ebenfalls keine Haftung bestehen wird.

Das Verhältnis zwischen HIVE-Lab und den teilnehmenden Forschungsprojekten muss durch genaue Bestimmung der Rechtsform, des Verhältnisses der Projekte bzw. Projektpartner zueinander und der Regelung eines möglichst umfassenden Haftungsausschlusses vertraglich geregelt werden. Dabei ist es im Interesse des HIVE-Labs, einen möglichst umfassenden

---

194 S. Kap. 2.3.2.1.

195 S. Kap. 2.3.2.2.

Haftungsausschluss hinsichtlich der vertraglichen und gesetzlichen Ansprüche zu erwirken. Zudem sollte sich das HIVE-Lab bei jeder Leistung vergewissern, ob es nicht in die Rolle eines Herstellers nach dem ProdHaftG wächst; in der Erprobungsphase wird dies jedoch aufgrund des mangelnden Inverkehrbringens meist nicht problematisch sein.

Besondere haftungsrechtliche Hürden sind für das HIVE-Lab, dessen Beteiligte im Gegensatz zu einem Forschungsprojekt wie IDeA, nicht für die Nutzungsphase haften, nicht ersichtlich. Es bestehen lediglich die allgemeinen und nicht technikbezogenen haftungsrechtlichen Erwägungen, die jedoch mit den vorhandenen Standardverträgen der wissenschaftlichen Forschung handhabbar sein dürften.

# 4 Literaturverzeichnis


*Albrecht, J. P./Jotzo, F.*, Das neue Datenschutzrecht der EU. Grundlagen - Gesetzgebungsverfahren - Synopse, Baden-Baden 2017.

*Artikel-29-Datenschutzgruppe*, WP 203. Opinion 03/2013 on purpose limitation, 2013.

*Artikel-29-Datenschutzgruppe*, Annex 2. Proposals for Amendments regarding exemption for personal or household activities, 2012.

*Artikel-29-Datenschutzgruppe*, WP 169. Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, 16. 2. 2010.

*Backmann, B.*, Produkthaftung bei Medizinprodukten, MPR 2012. S. 37.

*Bamberger, G./Roth, H./Hau, W./Poseck, R.*, BeckOK BGB, 53. Aufl. 2020 (zitiert als BeckOK BGB-*Bearbeiter*).

*Bergmann, K. O./Pauge, B./Steinmeyer, H.-D.*, Gesamtes Medizinrecht, 3. Auflage, Baden-Baden 2018.

*Bergt, M.*, Kundendatenschutz. Einwilligungen durch betroffene Personen, in: *Koreng, A./Lachenmann, M.* (Hrsg.), Formularhandbuch Datenschutzrecht, 2. Auflage, München 2018, S. 937.

*Britz, G.*, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, S. 1.

*Dreier, T./Spiecker gen. Döhmann, I.*, Die systematische Aufnahme des Straßenbildes, Zur rechtlichen Zulässigkeit von Online-Diensten wie ‚Google-Street View‘, Baden-Baden, 2010.

*Ebers, M.*, Autonomes Fahren: Produkt- und Produzentenhaftung, in: *Oppermann, B.H./Stender-Vorwachs, J.*, Rechtsfolgen, Rechtsprobleme, technische Grundlagen, München 2017, S. 93.

*Eßer, S./Kramer, P./v. Lewinski, K.* (Hrsg.), DSGVO/BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze. Kommentar, 6. Aufl., Köln 2018 (zitiert: Auernhammer-*Bearbeiter*).

*European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, 6.1.2020.

*European Data Protection Supervisor (EDPS)*, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7.11.2019.

*Fleck, J./Thomas, A.*, Automatisierung im Straßenverkehr – Wohin fahren wir?, NJOZ 2015, S. 1393.

*Gierschmann, S.*, Gemeinsame Verantwortlichkeit in der Praxis. Systematische Vorgehensweise zur Bewertung und Festlegung, ZD 2020, S. 69.

*Gierschmann, S./Schlender, K./Stentzel, R./Veil, W.* (Hrsg.), Kommentar EU-Datenschutz-Grundverordnung, Köln 2018 (zitiert: Gierschmann et al.-*Bearbeiter*).

*Gola, P./Eichler, C./Franck, L.*, et al. (Hrsg.), Datenschutz-Grundverordnung. VO (EU) 2016/679: Kommentar, 2. Auflage, München 2018 (zitiert: Gola et al.-*Bearbeiter*).

*Herbst, T.*, Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD 2016, *S.* 371.

*Herfurth, C.*, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Nachvollziehbare Ergebnisse anhand von 15 Kriterien mit dem sog. „3x5-Modell“, ZD 2018, S. 514.

*Hornung, G./Wagner, B.*, Der schleichende Personenbezug. Die Zwickmühle der Re-Identifizierbarkeit in Zeiten von Big Data und Ubiquitous Computing, CR 2019, S. 565.

*Jourdan, F./Matschi, H*, Automatisiertes Fahren – Wie weit kann die Technik den Fahrer ersetzen? Entwickler oder Gesetzgeber, wer gibt die Richtung vor?, NZV 2015, S. 26.

*Kanz, C./von Coelln, C.*, Haftung bei kooperativen Verkehrs- und Fahrerassistenzsystemen, 2012.

*Klar, M.*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, Münster 2012.

*Koyuncu, A./Müller, D. C.*, Medizinproduktehaftung – Auskunftsansprüche, Beweisfragen und Hinweise zur Anwenderkommunikation, MPR 2012, S. 158.

*Kremer, S.*, Gemeinsame Verantwortlichkeit: Die neue Auftrags-verarbeitung? Analyse der tatsächlichen Lebenssachverhalte zur Abgrenzung zwischen gemeinsamer Verantwortlichkeit und Auftragsverarbeitung, CR 2019, S. 225.

*Kühling, J./Buchner, B.* (Hrsg.), Datenschutz-Grundverordnung/BDSG. Kommentar, 2. Aufl., München 2018 (zitiert: Kühling/Buchner-*Bearbeiter*).

*Lang, M.*, Private Videoüberwachung im öffentlichen Raum, Hamburg 2008.

*Lindner, C.*, Persönlichkeitsrecht und Geo-Dienste im Internet – z.B. Google Street View/Google Earth, ZUM 2010, S. 292.

*Lurtz, H./Schindler, S.*, Gemeinsame Verantwortlichkeit des Websitebetreibers bei Social-Plug-Ins, VuR 2019, S. 468.

*Monreal, M.*, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, S. 507.

*Ortner, R./Daubenbüchel, F.*, Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit, NJW 2016, S. 2918.

*Paal, B. P./Pauly, D. A.* (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., München 2018 (zitiert: Paal/Pauly-*Bearbeiter*).

*Palandt, O.* (Begr.) Bürgerliches Gesetzbuch, Kommentar, bearb. v. *Brudermüller, G./Ellenberger, J./Götz,I., et al*., 78. Aufl., München 2019 (zitiert: Palandt-*Bearbeiter*).

*Plath, K.-U.* (Hrsg.), BDSG/DSGVO, Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Aufl. 2016.

*Pommerening, K./Müller, T.*, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten. Generische Lösungen der TMF 2.0, Berlin 2014.

*RAT FÜR INFORMATIONSINFRASTRUKTUREN*, Datenschutz und Forschungsdaten, 2017.

*Rehmann, W. A./Wagner, S. A.*, Medizinprodukterecht Verordnung (EU) 2017/745 über Medizinprodukte Kommentar, 3. Aufl. 2018.

*Roßnagel, A.*, Datenschutz in der Forschung. Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen, ZD 2019, S. 157.

Münchener Kommentar zum Bürgerlichen Gesetzbuch. Band 6, Schuldrecht – Besonderer Teil IV, §§ 705-853 Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, hrsg. v. *Säcker, F. J./Rixecker, R./Oetker, H./Limperg, B.*, 7. Aufl. 2017, (zitiert als MüKoBGB-*Bearbeiter*).

*Schantz, P./Wolff, H.A.*, Das neue Datenschutzrecht, Datenschutz-Grundverordnung und Bundesdatenschutzgesetz für die Praxis, München 2017.

*Schneider, J.*/Schindler, S., Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, Datenschutzrechtliche Anforderungen beim Erheben von Videodaten, ZD 2018, S. 463.

*Schreiber, K.*, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden. Anwendungsbereiche, Vertragsgestaltung und Folgen nicht gleichwertiger Verantwortung, ZD 2019, S. 55.

*Schwenke, T.*, Private Nutzung von Smartglasses im öffentlichen Raum, Edewecht 2016.

*Schwenke, T.*, Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach der DS-GVO, NJW 2018, S. 823.

*Simitis, S./Hornung, G./Spiecker Döhmann, I.* (Hrsg.), Datenschutzrecht. DSGVO mit BDSG, Baden-Baden 2019 (zitiert: Simitis/Hornung/Spiecker gen. Döhmann-*Bearbeiter*).

*Spickhoff, A.*, Medizinrecht, 3. Auflage, München 2018 (zitiert: Spickhoff-*Bearbeiter*).

*Spiecker gen. Döhmann, I.*., Datenschutzrechtliche Fragen und Antworten in Bezug auf Panorama-Abbildungen im Internet, Google Street View und die Aussichten, CR 2010, S. 311.

*Weimer, T.*, Medizinproduktehaftung. – Straf- und zivilrechtliche Haftung der Anwender und Betreiber von Medizinprodukten – Teil 3, MPR 2007, S. 119.

*Wolff, H. A/ Brink, S.* (Hrsg.), BeckOK Datenschutzrecht, 30. Aufl., München 2019 (zitiert: BeckOK Datenschutzrecht-*Bearbeiter*).