Schriftenreihe der TMF

T. Weichert

Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung

Vorgaben der EU-Datenschutz-Grundverordnung und national geltender Gesetze

Medizinisch Wissenschaftliche Verlagsgesellschaft

Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

Band 19

Medizinisch Wissenschaftliche Verlagsgesellschaft

Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

Band 19

Thilo Weichert

Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung

Vorgaben der EU-Datenschutz-Grundverordnung und national geltender Gesetze

Medizinisch Wissenschaftliche Verlagsgesellschaft

Der Autor

Dr. Thilo Weichert
Netzwerk Datenschutzexpertise
Waisenhofstraße 41
24103 Kiel
Telefon: 0431 9719742
E-Mail: weichert@netzwerk-datenschutzexpertise.de

MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG
Unterbaumstraße 4
10117 Berlin
www.mwv-berlin.de

ISBN 978-3-95466-700-0 (eBook: PDF)

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Informationen sind im Internet über http://dnb.d-nb.de abrufbar.

Produkt-/Projektmanagement: Ulrike Marquardt, Anna-Lena Spies, Berlin
Copy-Editing: Monika Laut-Zimmermann, Berlin
Layout, Satz & Herstellung: zweiband.media, Agentur für Mediengestaltung und -produktion GmbH, Berlin

Zuschriften und Kritik an:
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG, Unterbaumstr. 4, 10117 Berlin, lektorat@mwv-berlin.de

Editorial der TMF

Datenschutz in medizinischen Forschungsprojekten ist eines der Kernthemen der TMF seit ihrer Gründung 1999. Über mehr als 20 Jahre hinweg berät die TMF-Arbeitsgruppe Datenschutz mit großer Kontinuität Forschungsverbünde und -institutionen bei der Erstellung von Datenschutzkonzepten, verfasst Gutachten und entwickelt Leitfäden für Forschende. Im Juni 2021 konnte die AG ihre bereits 100. Sitzung abhalten. Im Zuge ihrer langjährigen Arbeit ist in der AG eine hohe Kompetenz entstanden, wie Datenschutz praktisch umgesetzt und medizinische Forschung datenschutzkonform betrieben werden kann. Die konkreten und praxisnahen Erkenntnisse der AG waren auch prägend für den Dialog, den die TMF seit 2001 mit den Datenschutzaufsichtsbehörden der Länder und des Bundes führt, und aus dem abgestimmte Konzepte und Leitfäden entstanden sind, die unter Federführung der TMF regelmäßig fortgeschrieben werden (zuletzt 2020 in Form des Mustertextes zum „Broad Consent" der Medizininformatik-Initiative). Aber auch auf den Reibungsfeldern zwischen Forschenden und Datenschützern hat die TMF vielfältige Erfahrungen sammeln können, insbesondere beim Umgang mit unterschiedlichen gesetzlichen Vorgaben und behördlichen Auffassungen zu standort- und bundeslandübergreifenden Forschungsvorhaben.

Die 2018 national geltendes Recht gewordene Datenschutzgrundverordnung der EU (EU-DSGVO) versprach zunächst eine Harmonisierung des rechtlichen Rahmens der Datenverarbeitung zu Forschungszwecken – und damit Abhilfe bei zumindest einigen der diesbezüglichen Probleme. Bei der konkreten Anwendung stellten sich aber rasch neue Fragen, insbesondere hinsichtlich des Zusammenspiels des neuen europäischen Rechts mit den landes- und bundesgesetzlichen Regelungen in Deutschland. Die AG Datenschutz der TMF hat sich daher bereits 2018 damit befasst, was die EU-DSGVO vor dem Hintergrund der nationalen rechtlichen Rahmenbedingungen für die medizinische Forschung bedeutet, und hat hierzu einen Fragenkatalog abgestimmt. Auf dessen Grundlage hat die TMF im Juli 2019 ein Rechtsgutachten ausgeschrieben, mit dem im Oktober 2019 Dr. Thilo Weichert, Jurist und Datenschutzbeauftragter a.D. des Landes Schleswig-Holstein, beauftragt wurde.

Eine erste Fassung des Gutachtens wurde Anfang 2020 einem Review unterzogen, das von Ronny Repp (Vorsitzender des AK der DSB außeruniversitärer Forschungseinrichtungen bei der Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V.) geleitet wurde, und an dem neben Mitgliedern der AG Datenschutz der TMF auch Sophie Rybczak, Farid Tehrani, Irene Schlünder und Dr. Johannes Drepper seitens der TMF-Geschäftsstelle beteiligt waren. Im Mittelpunkt des Prozesses stand ein fachliches Review, für das Prof. Dr. Alexander Roßnagel (Leiter des Fachgebiets Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel, mittlerweile Hessischer Landesbeauftragter für Datenschutz und Informationsfreiheit) gewonnen werden konnte. Auf der Grundlage einer zweiten Fassung des Gutachtens wurde dann im Juli 2020 ein gemeinsamer Workshop mit Dr. Thilo Weichert und den Reviewern durchgeführt, aus dem sich weitere Anregungen zum Gutachten ergaben. Es wurde im Mai 2021 vom Gutachter finalisiert.

Die vorliegende Expertise gründet auf dem als Band 17 der TMF-Schriftenreihe veröffentlichten Gutachten von Prof. Dr. Alexander Roßnagel und Prof. Dr. Dr. Christian Dierks („Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen", Medizinisch Wissenschaftliche Verlagsgesellschaft Berlin, 2019). Wir

freuen uns, dass mit Band 19 nun der datenschutzrechtliche Rahmen der medizinischen Forschung umfassend dargestellt ist. Die Bewertung der neuen Regularien durch den Gutachter wird einen wichtigen Beitrag zu künftigen Diskussionen rund um das Thema leisten. Im Vorwort wirft der Autor zudem erneut einen Blick auf das Verhältnis zwischen den datenschutzrechtlichen Anforderungen der medizinischen Forschung und den vielfältigen spezialgesetzlichen Regelungen, insbesondere jenen, die in der abgelaufenen Legislaturperiode des Bundestages für den Gesundheitsbereich eingeführt wurden, und die speziell die künftige patientennahe Forschung prägen werden. Angesichts der Ankündigung der neuen Bundesregierung, laut Koalitionsvertrag vom November 2021 in der aktuellen Legislaturperiode die Forschungsdateninfrastruktur zu stärken, Digitalisierungshindernisse abzubauen und ein „Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung" zu schaffen, kommt der vorliegende Band der TMF-Schriftenreihe genau zur richtigen Zeit.

Für dessen aufwändige Erstellung gebührt insbesondere dem Autor des Gutachtens, Dr. Thilo Weichert, großer Dank. Die TMF dankt auch der AG Datenschutz und Ronny Repp für die Initiierung des Gutachtens sowie allen Beteiligten am Review-Prozess, insbesondere Prof. Dr. Alexander Roßnagel und den bereits genannten Mitarbeiterinnen und Mitarbeitern der TMF-Geschäftsstelle.

Wir freuen uns schon jetzt auf Anregungen und Beiträge der Leser zur künftigen Debatte rund um die datenschutzkonforme Ausgestaltung der patientennahen medizinischen Forschung in Deutschland.

Für die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. im Auftrag des Vorstands

Sebastian Claudius Semler
(Geschäftsführer)

Prof. Dr. Michael Krawczak
(Vorstandsvorsitzender)

Vorwort

Medizinische Forschung und Datenschutz im Konflikt!?

Das Recht der medizinischen Forschung ist im Umbruch. Dies ist auch dringend nötig: Medizinisch Forschende beklagen zu Recht, dass die bestehenden Regelungen eine wirksame übergreifende Forschungsarbeit unter Nutzung von in Behandlungszusammenhängen generierten Gesundheitsdaten behindern und dass eine für diese Nutzung nötige einheitliche Infrastruktur fehlt. Die Rechtslage wird auch von Datenschützern beklagt. Das im Namen des Datenschutzes bestehende Regelwerk behindert eine Sekundärnutzung von Gesundheitsdaten für Forschungszwecke, obwohl dies für den Schutz des Patientengeheimnisses und des Rechts auf informationelle Selbstbestimmung überhaupt nicht nötig ist. Dies führt zu einer Diskreditierung des Datenschutzanliegens unter Forschenden und in der Öffentlichkeit sowie teilweise auch dazu, dass dringend durchzuführende medizinische Forschungsprojekte auf rechtlich unsichere Grundlagen und insbesondere auf Einwilligungen zurückgreifen müssen, bei denen die Patienten ihre medizinisch-informationelle Selbstbestimmung nicht immer wirksam wahrnehmen können.

Die rechtlichen Hindernisse bei der Durchführung medizinischer Forschung wurden in den letzten Jahren nicht nur erkannt, sondern führten auch zu ersten zielführenden rechtlichen Reformen. So ermöglichte eine Änderung der strafrechtlichen Regelung der beruflichen Schweigepflicht in § 203 StGB, mit der das Patientengeheimnis geschützt wird, dass Berufsgeheimnisträger, also auch Ärzte, beim Einsatz von Informationstechnik externe fachkundige digitale Unterstützung in Anspruch nehmen können, ohne ihr Vertraulichkeitsversprechen gegenüber ihren Patienten zu brechen. Dies wurde dadurch erreicht, dass die digitale Unterstützung von Berufsgeheimnisträgern durch „Mitwirkende" in den Schutzbereich der beruflichen Verschwiegenheit einbezogen wurde.

Die Grundlage für ein modernes Datenschutzverständnis im Bereich der Forschung wurde mit der seit Mai 2018 anzuwendenden europäischen Datenschutz-Grundverordnung (DSGVO) geschaffen. Dabei wurden die nicht nur im Grundgesetz (Art. 5 Abs. 3 GG), sondern auch in der europäischen Grundrechte-Charta (Art. 13 GRCh) garantierte Forschungsfreiheit und das Grundrecht auf Datenschutz in eine „praktische Konkordanz" gebracht. Danach müssen verfassungsrechtlich geschützte Rechtsgüter bei der Problemlösung einander so zugeordnet werden, dass jedes von ihnen Wirklichkeit gewinnt. Beiden Gütern müssen Grenzen gesetzt werden, damit beide zu optimaler Wirksamkeit gelangen können.[1] Dies gelingt dadurch, dass die Nutzung personenbezogener Daten für Forschungszwecke in der DSGVO bei Vorliegen von Schutzvorkehrungen privilegiert wird. Dies erfolgt über eine erleichterte Sekundärnutzung zweckgebundener Primärdaten (Art. 5 Abs. 1 lit. b DSGVO) sowie durch eine Modifikation der Betroffenenrechte im Bereich der Forschung (Art. 12 ff. DSGVO). Diese Privilegierung steht aber unter dem Vorbehalt, dass „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person" bestehen (Art. 89 Abs. 1 DSGVO).

1 Hesse, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage, Heidelberg 1999, Rn. 72.

Gutachtenauftrag

Diese beiden Rechtsänderungen sind der Hintergrund für das vorliegende im Auftrag der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) erstellte Gutachten, das in einer ersten Fassung Juli 2020 fertiggestellt wurde. Eine Überarbeitung und Aktualisierung des Gutachtens erfolgte im Mai 2021. Ziel des Gutachtens ist es, den neuen Rechtsrahmen für Medizinforschende ausführlich und anwendungsspezifisch darzustellen und zu erläutern und Hilfen bei der Anwendung der nicht ganz einfach zu verstehenden neuen rechtlichen Regelungen zu geben. Insofern hoffe ich, dass das Gutachten dazu beiträgt, dass Forschungsprojekte datenschutzgerecht gestaltet und umgesetzt werden und dass medizinische Forschung ermöglicht wird, ohne dass es rechtliche Hindernisse gibt, weil angemessene Datenschutzvorkehrungen getroffen werden.

Ein zweites Anliegen des Gutachtens besteht darin, nach Darstellung des neuen rechtlichen Rahmens für medizinische Forschung die weiterhin bestehende rechtliche Regelungsstruktur daraufhin zu überprüfen, ob diese den Anforderungen moderner Forschung und eines modernen Grundrechtsschutzes genügt. Die nationalen Regelungen sind von zentraler Bedeutung, da die DSGVO europarechtlich nur einen Rahmen vorgibt, der durch den nationalen Gesetzgeber konkretisiert werden muss. Das Gutachten kommt insofern zu dem Ergebnis, dass durch die in Deutschland geltenden Gesetze die DSGVO nur unzureichend umgesetzt wurde und dass die Rechtslage in Deutschland chaotisch, unübersichtlich, teilweise widersprüchlich und oft unpraktikabel ist, was u.a. auf die geteilte Gesetzgebungskompetenz zwischen Bund und Ländern im Bereich der Medizinforschung zurückzuführen ist.

Gesetzgebungsbedarf

Die Einsicht in die Notwendigkeit einer umfassenden nationalen Neuregelung zur medizinischen Forschung hat sich seit dem formellen Abschluss des vorliegenden Gutachtens weiterverbreitet und konkretisiert. Die Erfahrung, dass angesichts der Corona-Pandemie aktuelle Gesundheitsdaten für die Behandlung, die Vorsorge und den politischen Umgang dringend benötigt werden, diese Daten aber mangels Infrastruktur und gesetzlicher Grundlagen nicht zur Verfügung stehen, hat den Handlungsdruck verstärkt.

Die letzte Bundesregierung reagierte auf die gesetzgeberischen Defizite mit einigen Initiativen, mit denen Einzelfragen geregelt wurden, ohne dass ein Gesamtkonzept zur Reform der medizinischen Forschung erarbeitet, geschweige denn umgesetzt wurde. Um die Gesetzgebungskonkurrenz zwischen Bund und Ländern zu umgehen, setzte das Gesundheitsministerium mit seinen Gesetzesinitiativen auf einzelne Regelungen insbesondere im Sozialgesetzbuch (SGB) V, das systematisch nur für den Bereich der gesetzlichen Krankenversicherung gilt. Im Digitale-Versorgung-Gesetz (DVG)[2] wurde das Forschungsdatenzentrum eingeführt (§§ 303a ff. SGB V). In einem Implantateregistergesetz (IRegG) ist die Bereitstellung der dort gespeicherten Daten für die Forschung vorgesehen.[3] Im Patientendatenschutzgesetz (PDSG)[4] wird eine

2 DVG v. 09.12.2019, BGBl. I S. 2562.
3 Implantateregister-Errichtungsgesetz (mit § 31 IReG) v. 12.12.2019, BGBl. 2494.
4 PDSG v. 04.10.2020, BGBl. I S. 2115.

elektronische Patientenakte geregelt, die auf Einwilligungsbasis für Forschungszwecke zur Verfügung gestellt werden kann (sog. Datenspende).[5] Im Rahmen der Verabschiedung des Pandemieschutzgesetzes[6] wurde ein § 287a SGB V in Kraft gesetzt, der für länderübergreifende Vorhaben der Versorgungs- und Gesundheitsforschung das Bundesdatenschutzgesetz (BDSG) für anwendbar erklärt.

Die von der früheren Bundesregierung getragene Gesetzgebung zur Datenverarbeitung im Bereich medizinischer Forschung basierte auf Einzelentscheidungen, die oft ohne öffentliche Debatte und ohne die Einbindung der beteiligten Stellen erfolgten und sich an kurzfristigen Erwägungen orientierten, die nicht Teile einer umfassenden Konzeption oder Strategie waren. Dies hat zur Folge, dass zentrale Regelungen berechtigterweise kritisiert werden. So sind das bisherige Konzept und die Regelungen zu einem medizinischen Forschungsdatenzentrum (§§ 303a ff. SGB V) verfassungsrechtlich angreifbar.[7] Die Vereinheitlichung der Rechtsgrundlagen für länderübergreifende medizinische Forschung ist gesetzessystematisch und auch in Bezug auf die Gesetzgebungskompetenz zumindest fragwürdig, da in § 287a SGB V die bestehenden Landesregelungen mit dem Argument „Forschungsförderung" ausgehebelt werden (Art. 73 Abs. 1 Nr. 13 GG).[8]

Fachliche Expertise ist vorhanden

In jüngster Zeit intensivierte sich die Diskussion über die Notwendigkeit neuer gesetzlicher Regelungen und neuer Strukturen. Die TMF erarbeitete im Auftrag des Bundesgesundheitsministeriums ein umfangreiches Gutachten zur „‚Datenspende' – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen".[9] Der „Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen" veröffentlichte 2021 ein umfangreiches Gutachten, das u.a. für ein „Gesundheitsdatennutzungsgesetz" wirbt.[10] Das Netzwerk Datenschutzexpertise veröffentlichte ein „Plädoyer für ein medizinisches Forschungsgesetz".[11] Specht-Riemenschneider erarbeitete im Auftrag des Bundesministeriums für Bildung und Forschung unter anderem für den Gesundheitsbereich eine „Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln".[12]

5 § 363 SGB V.
6 G. v. 27.03.2020, BGBl. I S. 587.
7 Weichert MedR 2020, 539 ff.; vgl. aber Kühling/Schildbach NZS 2020, 41 ff.
8 Graf von Kielmansegg VerwArch 2021, 153 ff.
9 TMF, „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 30.03.2020, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf.
10 Sachverständigenrat, Digitalisierung für Gesundheit, Rn. 23, https://www.svr-gesundheit.de/gutachten/gutachten-2021/.
11 Plädoyer für ein medizinisches Forschungsgesetz, 22.02.2022, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021_02_medforschungdatens_final.pdf.
12 Specht-Riemenschneider, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, August 2021 https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf.

Im Herbst 2021 wurde ein von der TMF und der BQS im Auftrag des Bundesministeriums für Gesundheit erstelltes Gutachten zur „Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit" veröffentlicht.[13] Darin enthalten ist eine erstmalige Übersicht über die in Deutschland bestehenden medizinischen Register und deren Nutzungsmöglichkeit für Forschungszwecke. Dabei wird auch herausgearbeitet, dass eine Funktion dieser Register neben der Datensammlung für wissenschaftliche Zwecke auch darin besteht, medizinische Qualitätssicherung vorzunehmen, Patientensicherheit zu überwachen oder Wirksamkeitsuntersuchungen in Bezug auf Medizinprodukte, Arzneimittel und Versorgungsmodelle vorzunehmen. Das Gutachten schließt mit detaillierten Handlungsempfehlungen für die Politik, die sowohl gesetzliche wie auch organisatorische Maßnahmen zum Aufbau einer Register-Infrastruktur beinhalten. Die doppelte Funktion von Medizinregistern – Forschung und Qualitätskontrolle – und die rechtlichen Grundlagen werden von praktischer Seite auch beleuchtet durch eine von der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS), der Deutschen Gesellschaft für Unfallchirurgie (DGU), der Gesellschaft für Datenschutz und Datensicherheit (GDD) und dem Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD) veröffentlichte Praxishilfe, in der die bestehenden rechtlichen Voraussetzungen für den Betrieb von medizinischen Registern, insbesondere auch nach Landesrecht, beleuchtet werden.[14] Die Möglichkeiten von Treuhändermodellen zur Umsetzung des Datenschutzes wurden von verschiedenen Seiten wissenschaftlich herausgearbeitet.[15]

Koalitionsvertrag für 2021 bis 2025

Der rot-grün-gelben Koalitionsvereinbarung für die 20. Legislaturperiode[16] des Deutschen Bundestags ist zu entnehmen, dass die Bundespolitik für die Jahre bis 2025 einen Aufbruch für die medizinische Forschung plant: Es sollen „Instrumente wie Datentreuhänder, Datendrehscheiben und Datenspenden" auf den Weg gebracht werden. „Ein Dateninstitut soll Datenverfügbarkeit und -standardisierung vorantreiben, Datentreuhändermodelle und Lizenzen etablieren" (S. 17). Die Koalitionäre wollen den Zugang zu Forschungsdaten für öffentliche und private Forschung mit einem „Forschungsdatengesetz umfassend verbessern sowie vereinfachen" und „Forschungsklauseln" einführen. Die nationale Forschungsdateninfrastruktur soll weiterentwickelt und ein europäischer Forschungsdatenraum vorangebracht werden. Dabei soll „Datenteilung von vollständig anonymisierten und nicht personen-

13 TMF/BQS Institut für Qualität und Patientensicherheit, https://www.bundesgesundheitsministerium.de/ministerium/ressortforschung-1/handlungsfelder/digitalisierung/gutachten-zur-weiterentwicklung-medizinischer-register.html.

14 GMDS/DGU/GDD/BvD, Landesrechtliche Anforderungen an medizinische Register: Was zu beachten ist, 15.11.2021. https://gesundheitsdatenschutz.org/download/Praxishilfe_Anforderungen_Register.pdf

15 Z.B. Blankerz/Specht, Wie eine Regulierung für Datentreuhänder aussehen sollte, Juli 2021, https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf; Funke, Die Vereinbarkeit von Data Trust mit der Datenschutzgrundverordnung (DSGVO), November 2020, https://algorithmwatch.org/de/gutachten-data-trusts-dsgvo/.

16 Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Dezember 2021, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

bezogenen Daten für Forschung im öffentlichen Interesse" ermöglicht werden (S. 21). In der Gesundheitswirtschaft sollen die Potenziale der Digitalisierung genutzt werden, „um eine bessere Versorgungsqualität zu erreichen, aber auch Effizienzpotenziale zu heben" (S. 29). Die Stärkung der Digitalisierung im Gesundheitswesen soll u.a. über den Ausbau der gematik zu einer digitalen Gesundheitsagentur erreicht werden. Es wird versprochen:

> *„Zudem bringen wir ein Registergesetz und ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf" (S. 83).*

Um diese ehrgeizigen Ziele umzusetzen, muss umgehend mit den Vorbereitungen begonnen werden.

Beitrag für den wissenschaftlichen Diskurs, die Forschungspraxis und die Politik

Für die angekündigten politischen Maßnahmen steht die fachliche Expertise zur Verfügung, die ohne weiteres Abwarten in die Vorbereitungen und die Realisierung der gesetzgeberischen und organisatorischen Projekte einbezogen werden sollte. Eine zentrale Aufgabe ist es dabei, den aktuell bestehenden nationalen Rechtsrahmen zu berücksichtigen, insbesondere den beruflichen Geheimnisschutz sowie die DSGVO.

Das vorliegende Gutachten liefert hierzu eine Grundlage, indem es die teilweise kontrovers erörterten rechtlichen Fragestellungen darstellt und beantwortet. Mit diesem Gutachten ist die Hoffnung verbunden, dass in dieser Legislaturperiode die heute noch bestehenden Reibungsflächen zwischen medizinischer Forschung und Datenschutz beseitigt werden können.

Unabhängig davon soll das Gutachten für die Forschenden heute schon als nützliches Nachschlagewerk dienen, wenn es darum geht, offene rechtliche Fragen zum Datenschutz und zum Patientengeheimnis bei der Durchführung ihrer wissenschaftlichen Projekte zu beantworten.

Dr. Thilo Weichert
Februar 2022

Inhalt

Kurzzusammenfassung

Durch die Veränderung des datenschutzrechtlichen Rahmens seit der direkten Geltung und Anwendbarkeit der europäischen Datenschutz-Grundverordnung (DSGVO) im Mai 2018 und nach weiteren Rechtsänderungen in Deutschland haben sich die Regeln für die Verarbeitung personenbezogener Daten bei der medizinischen bzw. patientenorientierten Forschung grundlegend geändert. Der Ausgleich zwischen den sowohl im Grundgesetz (GG) wie der Europäischen Grundrechte-Charta (GRCh) garantierten Grundrechten, insbesondere dem Grundrecht auf Datenschutz und der Forschungsfreiheit, ist davon geprägt, dass die DSGVO die Weiterverarbeitung von personenbezogenen Daten **für Forschungszwecke privilegiert**, indem materiellrechtlich eine Zweckvereinbarkeit mit der Primärnutzung angenommen wird. Außerdem kann die Wahrnehmung von Betroffenenrechten eingeschränkt werden. Voraussetzung dafür ist, dass an dem Forschungsprojekt ein öffentliches Interesse besteht. Eine weitere Voraussetzung besteht darin, dass eine strenge Zweckbindung der Datenverarbeitung für Forschungszwecke erfolgt. Notwendig ist schließlich, dass über Bedingungen und Garantien die Rechte und Freiheiten der betroffenen Personen sichergestellt werden.

Die DSGVO stellt zwar europaweit verbindliche Prinzipien für die Verarbeitung von personenbezogenen Daten wie auch von besonderen Kategorien solcher Daten (sensitive Daten) auf. Zu diesen sensitiven Daten gehören insbesondere auch die für medizinische Forschungsprojekte bedeutenden Gesundheitsdaten. Doch überlässt es die DSGVO über sog. **Öffnungsklauseln** den Mitgliedstaaten, die Spezifizierung und Konkretisierung vorzunehmen und insbesondere auch den Schutz von Berufsgeheimnissen, wozu die ärztliche Schweigepflicht (das Patientengeheimnis) zu zählen ist, zu regeln.

Bei der Anpassung des nationalen Rechts an die europäischen Vorgaben bestehen insbesondere im Hinblick auf die Sekundärnutzung medizinischer Daten Umsetzungsprobleme, die dazu führen, dass die nationalen Nutzungsregelungen unanwendbar bleiben oder im Lichte der DSGVO angewendet werden müssen. Die **Rechtsgrundlagen** für die Verarbeitung personenbezogener Daten für Zwecke medizinischer Forschung finden sich durchgängig auf Bundes- und auf Landesebene. Diese müssen sich aber immer im Rahmen der Grundsätze der DSGVO (Art. 5), der dort enthaltenen allgemeinen Befugnisregelungen (Art. 6 DSGVO) sowie der spezifischen Regeln für die Verarbeitung sensitiver Daten (Art. 9 DSGVO) halten.

Die deutschen Gesetzgeber in Bund und Ländern haben es bisher unterlassen zu präzisieren, unter welchen Voraussetzungen die von der DSGVO garantierte Forschungsprivilegierung gilt. Durch die Vorrangregelungen im deutschen Recht für die Einwilligung von Betroffenen und wegen des zusätzlichen Erfordernisses der Beachtung des Patientengeheimnisses ist es Forschenden oft unklar, welchen rechtlichen Rahmen sie im Detail zu beachten haben. Diese **Rechtsunsicherheit** wird dadurch verstärkt, dass wegen der föderalen Struktur der Gesetzgebung im Rahmen eines Forschungsprojektes zugleich oft sowohl Bundes- wie auch Landesrecht und teilweise spezifisches Sozial- und Medizinrecht zu beachten sind.

Diese unklare Situation führt dazu, dass bei Forschungsprojekten Einwilligungen eingeholt werden, deren Wirksamkeit aber wegen der Breite und Unbestimmtheit fragwürdig ist. Erweist sich eine Einwilligung als unwirksam oder wird diese wider-

rufen, so stehen den Forschenden unter bestimmten Voraussetzungen gesetzliche Erlaubnistatbestände zur Verfügung. Auf diese darf aber nur im Ausnahmefall zurückgegriffen werden, wenn der **Wechsel in der Rechtsgrundlage** transparent gemacht wird und das Vertrauen der Betroffenen auf ihre Entscheidungsbefugnis über die Nutzung ihrer Daten nicht beeinträchtigt wird.

Die nationalen Regeln für die Datenverarbeitung bei **Berufsgeheimnisträgern** wurden im Jahr 2017 durch eine Änderung des § 203 Strafgesetzbuch (StGB) dahingehend modifiziert, dass die Offenbarung von Patientengeheimnissen auch gegenüber externen Mitwirkenden erlaubt ist, die in den beruflichen Geheimnisbereich mit einbezogen werden. Dies ermöglicht es, in Forschungsprojekten externe Stellen ohne eine Schweigepflichtentbindung der Betroffenen einzubeziehen, soweit diese in die ärztliche Tätigkeit im Rahmen des Erforderlichen eingebunden sind.

Ausschließlich **auf eine eigene Forschung ausgerichtete Tätigkeiten** einer externen Stelle oder Person können jedoch nicht dem ärztlichen Bereich zugeordnet werden mit der Folge, dass es für diese Datennutzung entweder einer Schweigepflichtentbindung oder einer expliziten gesetzlichen Legitimation bedarf. Auch in Bezug auf die Legitimation zur Offenbarung für Forschungszwecke weisen die geltenden Regelungen in Deutschland Defizite auf.

Der bisherige Vorrang für die Rechtfertigung medizinischer Forschung durch eine **Betroffeneneinwilligung** wird den Anforderungen an eine moderne medizinische Forschung nicht mehr gerecht. Forschungsprojekte sind oft geprägt von hoher technischer Komplexität, Arbeitsteilung, Langfristigkeit, Interdisziplinarität und Internationalität. Die dabei erfolgende Datenverarbeitung lässt sich oft mit Einwilligungen, die den datenschutzrechtlichen Anforderungen genügen, nicht mehr erfassen. Auch gestufte und dynamische Verfahren der Einwilligung können nur begrenzt einen Ausgleich zwischen Forschungsnotwendigkeiten und informationeller Selbstbestimmung der Betroffenen bewirken.

Dies macht kompensierende normative Vorgaben nötig, mit denen die Betroffeneninteressen und -rechte gesichert werden. So haben die Betroffenen Transparenzansprüche, wozu in den Art. 12ff. DSGVO weitgehende Vorgaben enthalten sind. Eine hohe **Transparenz** ermöglicht es den Betroffenen, ihre Rechte auf Widerspruch und auf Löschung in Anspruch zu nehmen.

Eine rechtliche Neuorientierung hat sich für das deutsche Datenschutzrecht dadurch ergeben, dass das bisher selten angewandte Instrument der „**gemeinsamen Verantwortlichkeit**“ durch die jüngste Rechtsprechung des Europäischen Gerichtshofes (EuGH) in der Praxis stark aufgewertet wurde. Gemeinsame Verantwortlichkeit ist bei einer arbeitsteiligen Datenverarbeitung immer dann gegeben, wenn jeder der Beteiligten im eigenen Verarbeitungsinteresse einen entscheidenden Beitrag leistet. Der Umstand einer gemeinsamen Verantwortlichkeit hat nicht zur Folge, dass zivilrechtlich eine bestimmte Rechtsform für die Zusammenarbeit besteht oder gewählt werden muss.

In Forschungsprojekten mit mehreren Beteiligten bietet sich eine Gestaltung der Datenverarbeitung in gemeinsamer Verantwortlichkeit an. Dabei können zwecks Datenminimierung und „informationeller Gewaltenteilung“ Treuhänder eingebunden werden. Voraussetzung für eine zulässige Verarbeitung in gemeinsamer Verant-

wortlichkeit ist, dass die Beteiligten in einer **Vereinbarung** ihre Ziele, ihre Verarbeitung und die Aufteilung der Aufgaben präzise festlegen und transparent machen.

Die Sicherung der Betroffenenrechte im Rahmen von medizinischen Forschungsprojekten bedarf in jedem Fall geeigneter Garantien materiell-rechtlicher, prozessualer und technisch-organisatorischer Art. Dabei kommt der Pseudonymisierung von Daten als Instrument der Datenminimierung eine wichtige Funktion zu. Die Verwaltung der Pseudonyme kann durch Treuhänder erfolgen, die aber nicht zugleich die Funktion eines Datenschutzbeauftragten wahrnehmen sollten. Die Gesamtheit der Maßnahmen mit einer Bewertung, ob und inwieweit damit den entstehenden Risiken begegnet wird, muss im Regelfall in eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) einfließen. Zwar bestehen insofern nur beschränkt gesetzliche Anforderungen, doch legen es die Regelungen nahe, die Festlegungen zur Datenverarbeitung und zum Datenschutzmanagement bei medizinischen Forschungsprojekten in einem konsistenten **Datenschutzkonzept** vorzunehmen.

Die Wahrnehmung von **Betroffenenrechten** bei privilegierten Forschungsprojekten kann, soweit hierfür erforderlich, beschränkt werden. Ein Anspruch auf Datenübertragbarkeit (Art. 20 DSGVO) besteht zumeist nicht. Demgegenüber besteht ein Auskunftsanspruch, wenn durch die Auskunft nicht die Forschungszwecke ernsthaft beeinträchtigt werden. Wegen der teilweise sehr umfassend möglichen Zweckfestlegung bei Forschungsprojekten kann die Löschung von Daten oft vermieden oder zumindest weit hinausgeschoben werden. Soweit möglich, ist eine Datenminimierung durch Pseudonymisierung vorzunehmen, die bei einer möglichen Reidentifizierung aber nicht davon befreit, Betroffenenansprüchen nachzukommen.

Der Datenaustausch von wissenschaftlichen Projektpartnern innerhalb der Europäischen Union folgt den gleichen Regeln, die auch zwischen deutschen Partnern gelten. Beim Datenaustausch mit Partnern in einem **Drittland** kommt es darauf an, ob dort ein angemessenes Datenschutzniveau sichergestellt ist. Soweit eine Verarbeitung innerhalb der Union erfolgt, gilt ausschließlich europäisches Recht, auch wenn aus dem Drittland Daten importiert werden.

Die DSGVO bietet einen validen Rechtsrahmen für medizinische Forschung. Demgegenüber bestehen bei der nationalen Umsetzung in Deutschland auf der Grundlage der Öffnungsklauseln große Defizite. Diese sollten durch eine **Harmonisierung des Rechts in Deutschland** beseitigt werden. Als Instrument hierfür käme ein Bund-Länder-Staatsvertrag in Betracht. Durch eine Änderung im GG könnte auch eine Gesetzgebungszuständigkeit des Bundes für die Datenverarbeitung bei der (medizinischen) Forschung geschaffen werden, sodass vom Bundesgesetzgeber einheitliche Regelungen erlassen werden könnten. Durch Verhaltensregeln sowie durch andere untergesetzliche Festlegungen sind Harmonisierungsmaßnahmen möglich, mit denen die bestehenden gesetzlichen Defizite teilweise gemildert, aber nicht vollständig beseitigt werden können.

Angesichts der massiv gesteigerten Relevanz unionsweiter medizinischer Forschung und angesichts international geltender gemeinsamer Standards in diesem Bereich ist eine **europaweite verbindliche Regulierung** der personenbezogenen Datenverarbeitung bei (medizinischen) Forschungsvorhaben wünschenswert. Der europäische Rechtsrahmen bedarf hierfür keiner grundlegenden Veränderung und kann an die bestehenden Regelungen der DSGVO anknüpfen.

1 Einführung

Das vorliegende Rechtsgutachten wurde von Ende 2019 bis April 2020 im Auftrag der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. – erstellt und im Mai 2021 auf den aktuellen Stand gebracht. Die vorrangige Aufgabe des Gutachtens besteht darin, die **in jüngerer Zeit erfolgten Rechtsänderungen**, insbesondere das Wirksamwerden der europäischen Datenschutz-Grundverordnung (DSGVO), darzustellen und auf seine Auswirkungen auf die medizinische wissenschaftliche Forschung hin zu untersuchen.

Der aktuelle neue Rechtsrahmen wirft eine Vielzahl von Fragen auf, die mit dem vorliegenden Gutachten erörtert und beantwortet werden. Diese Antworten zu teilweise umstrittenen und unklaren Regelungen sollen der Forschungsgemeinschaft eine **rechtssicherere Anwendung in der wissenschaftlichen Praxis** ermöglichen. Grundlage der Bearbeitung ist ein Fragenkatalog. Die Fragen sowie die Antworten darauf finden sich knapp zusammengefasst in Kapitel 15; die ausführlichen Herleitungen und Erläuterungen dazu in den jeweils angegebenen Gutachtenabschnitten. Das Gutachten beschränkt sich nicht auf die gestellten Fragen, sondern ordnet diese systematisch in einen größeren rechtlichen und tatsächlichen Zusammenhang ein.

Im Kapitel 14 erfolgt eine **kritische Bewertung des aktuellen Rechtsrahmens** im Hinblick auf die Praktikabilität für eine wirksame und rechtssichere Durchführung medizinischer Forschungsprojekte. Dabei wird eine Evaluation der neuen Regelungen der DSGVO und des nationalen Rechts vorgenommen; hieraus werden rechtliche Änderungsnotwendigkeiten abgeleitet.

Erklärte Zielsetzung des vorliegenden Gutachtens ist es, den Schutz der Grundrechte und insbesondere des Grundrechts auf Datenschutz bei der Durchführung medizini-

scher Forschung so gut wie möglich zu verwirklichen und hierbei zugleich ein Optimum für die Forschung zu erreichen im Hinblick auf den Aufwand, die organisatorische und praktische Durchführung und die mögliche wissenschaftliche Erkenntnis. Es geht also um die Herstellung einer **praktischen Konkordanz zwischen dem Schutz informationeller Grundrechte und der medizinischer Forschungsfreiheit**.[1]

Das vorliegende Gutachten beruht auf der **Auswertung der rechtswissenschaftlichen Literatur**, die insbesondere zu den aktuellen Rechtsänderungen umfangreich vorhanden ist, sowie der jüngeren Rechtsprechung. Deren Fokus liegt aber bisher nicht auf den Auswirkungen auf die medizinische Forschung. Das vorliegende Gutachten nimmt diese Schwerpunktsetzung vor. Die Ergebnisse werden im **Diskurs mit medizinischen Forschenden** mit deren praktischen Erfordernissen, die im Rahmen eines Review-Prozesses eingebracht wurden, gespiegelt. Es werden Lösungen für eine wirksame und effiziente Umsetzung der rechtlichen Anforderungen gesucht.

Ziel des Rechtsgutachtens ist es also, die wesentlichen datenschutzrechtlichen Fragestellungen zur Nutzung personenbezogener Gesundheitsdaten nach den Vorgaben der europäischen Datenschutz-Grundverordnung (DSGVO), des allgemeinen nationalen Datenschutzrechts (Bundesdatenschutzgesetz, BDSG, Landesdatenschutzgesetze, LDSG) sowie sonstiger relevanter Regelungen (Sozialgesetzbücher/SGB, Strafgesetzbuch/StGB, Ärztliche Berufsordnungen, Krankenhausgesetze und sonstige Medizinrechtsnormen) zu untersuchen und Empfehlungen für die praktische rechtssichere Anwendung zu geben. Zudem wird eine Bewertung der bestehenden Forschungsregelungen im Hinblick auf die Praktikabilität und die Zielsetzung (Ermöglichung medizinischer Forschung, Umsetzung des Persönlichkeitsschutzes) vorgenommen. Die Bewertungen können als Grundlage für einen Erfahrungsbericht der TMF bzgl. der praktischen Umsetzung der DSGVO gegenüber der EU-Kommission verwendet werden.

Die **Darstellung** beginnt mit allgemeinen Fragen des Verfassungsrechts (Kap. 2). Insbesondere werden die Zielsetzungen und Grenzen der Forschungsfreiheit unter Bezugnahme auf die informationellen Grundrechte von Patienten bzw. Probanden beleuchtet (Kap. 3). Auf dieser Grundlage sowie unter Berücksichtigung der zentralen Rechtsnormen (Kap. 4) werden dann die sich bei medizinischer Forschung stellenden spezifischen Fragen zum Datenschutz und zum Berufsrecht beantwortet. Dabei geht es zunächst um eine Klärung der datenschutzrechtlichen Verantwortlichkeit, die durch das Hervorheben gemeinsamer Verantwortlichkeit durch den europäischen Gesetzgeber und den Europäischen Gerichtshof (EuGH) einer Neubewertung zugeführt werden musste (Kap. 5). Das Verhältnis des Patientengeheimnisses als berufliche Schweigepflicht ist neu zu klären, nachdem der deutsche Gesetzgeber durch eine Änderung des § 203 StGB externe Mitwirkende in den beruflichen Geheimschutzbereich einbezogen hat (Kap. 6).

Im Folgenden werden die materiell-rechtlichen, prozeduralen und technisch-organisatorischen **Anforderungen an medizinische Forschung** dargestellt und erörtert: Dabei wird auf die Rolle der Betroffeneneinwilligung (Kap. 7) und die Zweckbindung von Forschungsdaten (Kap. 8) eingegangen. Fragen der Sicherheit der Forschungsdatenverarbeitung werden nur knapp behandelt (Kap. 9). Das Spannungsverhältnis

1 Schlüchter/Duttge JR 1997, 174.

zwischen datenschutzrechtlich geforderter Datenminimierung und einer validen Forschungsdatengrundlage kann durch Maßnahmen der Anonymisierung und Pseudonymisierung zumindest teilweise aufgelöst werden (Kap. 10). Weitere Maßnahmen zur Verwirklichung des Datenschutzes sind über ein wirksames Datenschutzmanagement möglich (Kap. 11). Zur Wahrung der Betroffenenrechte, die in der DSGVO zugunsten einer wirksamen Forschung eingeschränkt werden können, sind die Rahmenbedingungen und Ausgleichsmaßnahmen zu erörtern (Kap. 12). Weiterhin wird auf die Besonderheiten medizinischer Forschung mit ausländischen Projektpartnern (Kap. 13) eingegangen. Abschließend erfolgt eine Analyse der aktuellen Rechtslage und der praktischen Anforderungen medizinischer Forschung, woraus konkrete Verbesserungsvorschläge abgeleitet werden (Kap. 14).

2 Verfassungsrechtliche Grundlagen

Bei der Verarbeitung personenbezogener Daten für Forschungszwecke können sowohl auf nationaler wie auf europäischer Ebene gewährleistete Grundrechte miteinander in Konflikt geraten.[2] Bei Forschungsvorhaben geht es oft darum, das Verhalten und die Umstände von natürlichen Personen zu erkunden und hieraus Schlussfolgerungen zu ziehen. Dies setzt regelmäßig das Erfassen von personenbezogenen Daten voraus, auch wenn die Ergebnisse der Forschung regelmäßig nicht mehr personenbezogen sind. Es geht bei Forschung mit personenbezogenen Daten insbesondere um einen Ausgleich zwischen dem Grundrecht auf **Forschungsfreiheit** (Art. 13 S. 1 GRCh, Art. 5 Abs. 3 S. 1 GG) und dem Recht auf informationelle Selbstbestimmung[3] bzw. dem **Grundrecht auf Datenschutz** (Art. 8 GRCh).[4] In den hier relevanten Grundrechtsbereichen ist auf Unionsebene ein wirksamer Grundrechtsschutz vorgesehen, sodass das Unionsrecht einen Anwendungsvorrang hat.[5] Dies tangiert aber nicht die innerstaatliche Verteilung der Gesetzgebungskompetenzen (s.u. Kap. 2.4).[6]

2 Zum Verhältnis des GG zur GRCh sowie zur Prüfkompetenz des BVerfG bzw. des EuGH vgl. BVerfG 6.11.2019 – 1 BvR 16/13, DuD 2020, 199f. sowie BVerfG 6.11.2019 – 1 BvR 276/17, DuD 2020, 206ff.

3 Erstmals BVerfG 15.12.1983 – 1 BvR 209/83 u.a., LS 1, NJW 1984, 419.

4 Roßnagel, ZD 2019, 158; zur Geschichte des Grundrechtskonflikts Bizer, 25ff. m.w.N.

5 Ausführlich BVerfG 06.11.2019 – 1 BvR 16/13 (Recht auf Vergessen I), Rn. 41ff.; BVerfG 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 32ff.

6 Dierks 2019, 33.

2.1 Grundrecht auf Datenschutz

Das **Recht auf informationelle Selbstbestimmung** wurde vom BVerfG 1983 wie folgt beschrieben:

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[7]

In Art. 8 Abs. 1, 2 S. 1 GRCh wird nun seit 2009 verbindlich für die Europäische Union[8] eine **ausdrückliche Normierung** vorgenommen:

> *„Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden."*

Der Inhalt des verfassungsrechtlich abgeleiteten „Rechts auf informationelle Selbstbestimmung" und des in Art. 8 GRCh gewährleisteten Grundrechts auf Datenschutz kann, auch wenn es unterschiedliche Auslegungskompetenzen gibt, als deckungsgleich angesehen werden.[9] Es ist allgemein anerkannt, dass das Grundrecht auf Datenschutz nicht schrankenlos gewährleistet werden kann. Der Einzelne muss **Einschränkungen** seines Rechts im überwiegenden Allgemeininteresse hinnehmen. Diese Einschränkungen bedürfen einer gesetzlichen Grundlage, die den Wesensgehalt des Grundrechts wahrt und aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben (rechtsstaatliches Gebot der Normenklarheit). Beim Erlass dieser Regelungen sowie bei deren Anwendung ist der Grundsatz der Verhältnismäßigkeit zu beachten. Angesichts der Risiken bei der Nutzung der automatischen Datenverarbeitung sind zusätzliche organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr der Verletzung des Persönlichkeitsrechts entgegenwirken.[10]

Ein **Ausgleich zwischen den Grundrechten** ist also nötig und normativ vorzugeben.[11] Dies gilt insbesondere für Forschungsvorhaben, für deren Durchführung auf sensitive personenbezogene Daten zurückgegriffen wird, wodurch das Grundrecht auf Datenschutz und die Forschungsfreiheit in Kollision geraten können.[12]

---

7 BVerfG 15.12.1983 – 1 BvR 209/83 u.a. (Volkszählung), NJW 1984, 419; zur ethischen Dimension der Selbstbestimmung bei der medizinischen Forschung Strech in TMF, 60ff.

8 Für Polen und das Vereinigte Königreich ist bzw. war die Verbindlichkeit ausgeschlossen gemäß Protokoll über die Anwendung der Charta der Grundrechte der Europäischen Union auf Polen und das Vereinigte Königreich, ABl. EU 2007, C 306/156.

9 Bretthauer in Specht/Mantz, Rn. 66; Kühling/Raab in Kühling/Buchner, Einführung Rn. 31–41; vgl. aber Augsberg in von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. Bd. 1 2015, Art. 8 GRC Rn. 5, der auf den Subsidiaritätsaspekt hinweist.

10 BVerfG 15.12.1983 – 1 BvR 209/83 u.a. (Volkszählung), NJW 1984, 419, 422; 94/12, EuGH 08.04.2014 – C-293/12 u. C-594/12 (Vorratsdatenspeicherung), Rn. 38; NJW 2014, 2171.

11 Geminn, DuD 2018, 640.

12 Roßnagel/Geminn in Dierks/Roßnagel, 196.

2.2 Sonstige Grundrechte

Durch Forschungsprojekte mit personenbezogenen Daten können zusätzlich zu dem Grundrecht auf Datenschutz **weitere Grundrechte** tangiert sein. Dies sind u.a. das in Art. 7 GRCh bzw. in Art. 10 GG gewährleistete Telekommunikationsgeheimnis, der auch in Art. 7 GRCh sowie in Art. 13 GG gewährleistete Schutz der Wohnung sowie generell die Achtung des privaten Lebens. Weiteren Grundrechten kommt eine informationelle Komponente zu.[13] Bei medizinischen Forschungsprojekten kann das Recht auf körperliche Unversehrtheit (Art. 2 Abs. 2 S. 1 GG, Art. 3 Abs. 1 GRCh) tangiert sein. Dabei kommt der freien *„Einwilligung des Betroffenen nach vorheriger Aufklärung entsprechend den gesetzlich festgelegten Modalitäten"* eine wichtige Rolle zu (Art. 3 Abs. 2 lit. a GRCh). Gemäß Art. 35 S. 1 GRCh hat jeder Mensch *„das Recht auf Zugang zur Gesundheitsvorsorge und auf ärztliche Versorgung"*. Dies kann für die Umsetzung medizinischer Forschungsergebnisse bedeutend sein, etwa wenn diese in die individuelle Behandlung einfließen. Bei derartigen Fallkonstellationen können auch die Gleichheit vor dem Gesetz (Art. 3 Abs. 1 GG, Art. 20 GRCh) sowie Diskriminierungsverbote (Art. 3 Abs. 3 GG, Art. 21 GRCh) Bedeutung erlangen.[14] Patienten sind zugleich „Verbraucher" im Bereich der Gesundheitsversorgung. Insofern ist Art. 38 GRCh zu beachten, wonach die Politik der Union ein hohes Verbraucherschutzniveau sicherstellt. Schließlich ist darauf hinzuweisen, dass das Bundesverfassungsgericht (BVerfG) aus dem allgemeinen Persönlichkeitsrecht und in Gesamtsicht weiterer Grundrechte ein „IT-Grundrecht" bzw. „Computergrundrecht" mit dem etwas sperrigen Namen „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" abgeleitet hat. Dabei geht es um die Schaffung eines persönlichen speziellen digitalen Vertraulichkeitsraums, in den auch medizinische Sachverhalte einbezogen sein können, in den Dritte nur unter hohen Voraussetzungen einzudringen befugt sind.[15]

Private forschende Stellen können zusätzlich zur Forschungsfreiheit (s.u. Kap. 3) für ihre wissenschaftliche Tätigkeit auch ihre **unternehmerische Freiheit** geltend machen.[16] Diese findet nach der deutschen Verfassungsrechtsprechung als Konkretisierung der allgemeinen Handlungsfreiheit Anerkennung und wird nun in Art. 16 GRCh ausdrücklich anerkannt. Zudem können sich Personen, soweit sie beruflich forschend tätig sind, auf ihre **Berufsfreiheit** berufen (Art. 12 GG, Art. 15 GRCh). Es ist aber nicht erkennbar, dass datenschutzrechtliche Regelungen, die eine Privilegierung der Forschung vorsehen, den Schutz dieser wirtschaftlichen Freiheiten zum Ziel haben, so auch nicht die sehr weit gehenden Privilegierungen der DSGVO. Diese sollen vorrangig die Forschungsfreiheit und im wissenschaftlichen Rahmen die Meinungs- und Informationsfreiheit zur Geltung bringen. Mit diesen Grundrechten werden auch gemeinschaftsförderliche Ziele verfolgt. Privilegierte Eingriffe in das Grundrecht auf Datenschutz, also über die generell geltenden Verarbeitungsbefugnisse zwischen Privaten hinausgehende Rechte, lassen sich nur mit Allgemeinwohl-

13 Roßnagel, ZD 2019, 108; Weichert, KJ 2014, 125ff.; Weichert in DWWS, Einl. DSGVO Rn. 11–15, 17; Hoffmann/Luch/Schulz/Borchers, Die digitale Dimension der Grundrechte, 2015; Heberlein DVBl 2020, 1225ff.

14 Weichert 2018, Kap. 6.13 u. Kap. 14; Graf von Kielmansegg in TMF, 87f.

15 BVerfG 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = NJW 2008, 822 = MMR 2008, 315 = DVBl 2008, 582; dazu Dochow, 537ff.; zu allem oben genannten: Weichert 2018, Kap. 6.

16 BVerfG 6.11.2019 – 1 BvR 276,17, Rn. 103; DuD 2020, 207; Krohm in Gola/Heckmann, § 27 Rn. 24.

erwägungen rechtfertigen (s.u. Kap. 8.1). Schließlich genießen die Forschenden als wissenschaftlich tätige natürliche Personen selbst ein **Grundrecht auf Datenschutz**.[17]

2.3 Europäische Regelungskompetenz

Die Europäische Union (EU) hat im Hinblick auf **Forschung** keine eigenständige Normsetzungskompetenz. Art. 3 Abs. 3 UAbs. 1 S. 3 EUV nennt den wissenschaftlichen Fortschritt neben nachhaltigem wirtschaftlichem Wachstum und sozialem Fortschritt als Zielbestimmung der EU. Art. 179 Abs. 1 AEUV gibt als Ziel die Stärkung der wissenschaftlichen und technologischen Grundlagen vor, wodurch *„ein europäischer Raum der Forschung geschaffen wird, in dem Freizügigkeit für Forscher herrscht und wissenschaftliche Erkenntnisse und Technologien frei ausgetauscht werden."* Die Wettbewerbsfähigkeit auch der Industrie soll und Forschungsmaßnahmen sollen gefördert werden. Dies gilt besonders für „Zusammenarbeitsbestrebungen" (Art. 179 Abs. 2 AEUV).[18]

Hinsichtlich des **Gesundheitswesens** hat die Europäische Union (EU) gemäß Art. 168 AEUV – ebenso wie im Bereich der Forschung – weitgehend nur eine Kompetenz zur Koordinierung, zur Förderung und zur Ergänzung der nationalen Maßnahmen. Gesetzgeberische Aufgaben liegen bei der EU nur bei der Festlegung von Qualitäts- und Sicherheitsstandards sowie zum grenzüberschreitenden Schutz der Bevölkerung. Die Mitgliedstaaten bleiben die „Herren der Gesundheitspolitik".[19]

Hinsichtlich des **Datenschutzes** wird in Art. 16 Abs. 2 AEUV eine umfassende Normsetzungskompetenz der EU festgelegt in Bezug auf „den Anwendungsbereich des Unionsrechts" und den „freien Datenverkehr". Zum Anwendungsbereich des Unionsrechts gehören auch die Regelungen der Art. 179–188 AEUV; vom freien Datenverkehr wird also der Austausch personenbezogener Daten im Bereich der Gesundheit und für Forschungszwecke erfasst. Insofern besteht für die EU eine umfassende Regelungskompetenz hinsichtlich des Datenschutzes für Forschungszwecke, also auch für medizinische Forschungszwecke.[20]

2.4 Kompetenzrechtliche nationale Vorgaben

Für das deutsche Datenschutzrecht gibt es im GG keine ausdrücklich geregelte **Gesetzgebungszuordnung**. Vielmehr wird das Datenschutzrecht als Kompetenz kraft Sachzusammenhangs bzw. als Annexkompetenz dem Gesetzgeber zugewiesen, der für die jeweilige Hauptmaterie zuständig ist. Dies führt zu einem Nebeneinander von Zuständigkeiten für die Länder (Art. 70 GG) und des Bundes, wenn bestimmte Sachverhalte der ausschließlichen (Art. 71, 73 GG) oder der konkurrierenden Gesetzgebung (Art. 72, 74 GG) zugewiesen sind. Hinzu kommen Regelungsbefugnisse der Kirchen in Bezug auf ihre eigenen Angelegenheiten.[21] Dies hat zur Folge, dass der Bund zuständig ist für die Bundesverwaltung (Art. 87 GG), das Post- und Fernmelde-

17 Johannes DuD 2012, 817.
18 Dierks 2020, 5.
19 Berg/Augsberg in Schwarze, Art. 168 AEUV, Rn. 15f.; Sachverständigenrat, 40f.
20 Dierks 2019, 13.
21 Dierks 2019, 77–85; Dierks in Dierks/Roßnagel, 10.

wesen (Art. 73 Nr. 7 GG), die Statistik für Bundeszwecke (Art. 73 Nr. 11 GG), das bürgerliche Recht und das Strafrecht (Art. 74 Nr. 1 GG), die öffentliche Fürsorge (Art. 74 Nr. 7 GG), das Recht der Wirtschaft (Art. 74 Nr. 11 GG), die Förderung der wissenschaftlichen Forschung (Art. 74 Nr. 13 GG)[22], die medizinisch unterstützte Erzeugung menschlichen Lebens, die Untersuchung und die künstliche Veränderung von Erbinformationen sowie Regelungen zur Transplantation von Organen, Geweben und Zellen (Art. 74 Nr. 26 GG). Die Länder sind in den nicht ausdrücklich dem Bund zugewiesenen Bereichen für die Gesetzgebung zuständig, also u.a. für die zu ihrer Verwaltung, einschließlich der Gesundheitsverwaltung, und zu den Hochschulen.[23]

Für die Datenverarbeitung im **Bereich der Forschung** oder für Forschung generell gibt es keine gesonderten Zuständigkeiten. Auch insofern bestehen lediglich Annexkompetenzen. Dies hat zur Folge, dass Forschung an Bundesuniversitäten und an Bundesforschungseinrichtungen sich nach Bundesrecht richtet, die von Hochschulen der Länder nach Landesrecht. Die Forschung durch private Einrichtungen fällt unter den Bereich der Wirtschaft in der Gesetzgebungszuständigkeit des Bundes. Unter den Begriff Fürsorge (Bund) fällt die abschließend vom Bund in den Sozialgesetzbüchern (SGB) geregelte Aufgabenerledigung der Sozialleistungsträger, einschließlich deren Forschungsdatenverarbeitung.[24]

22 Für eine extensive Auslegung Graf von Kielmansegg in TMF, 122.
23 Dierks 2019, 8f., 34–36.
24 Dierks in Dierks/Roßnagel, 12; Engelke/Kipker/Voskamp, 34ff.; vgl. Graf von Kielmansegg in TMF, 122f.

3 Insbesondere Forschungsfreiheit

Forschung ist die Basis nahezu aller unserer **technischen Errungenschaften**. Durch die Digitalisierung aller Lebensbereiche kommt datenbasierter Forschung eine herausragende und zunehmende Bedeutung zu.

Damit steigt auch die Relevanz der **verfassungsrechtlichen Grundlagen** für die Forschung:

- Art. 5 Abs. 3 S. 1 GG: „*Kunst und Wissenschaft, Forschung und Lehre sind frei.*"
- Art. 13 S. 1 GRCh: „*Kunst und Forschung sind frei.*"

Das Grundrecht auf Forschungsfreiheit beinhaltet zunächst einen subjektiv-rechtlichen **Abwehranspruch**.[25] Die im Grundgesetz gewährleistete Forschungsfreiheit entspricht weitgehend der der GRCh (s.u. Kap. 3.2).

Daneben hat die Forschungsfreiheit auch einen institutionellen und einen **objektivrechtlichen Gehalt**. Grundrechte entfalten ihre Wirkkraft in der gesamten Rechtsordnung und als Wertentscheidungen bei der Auslegung und Anwendung des einfachen Rechts. Daraus können sich Leistungsansprüche und Schutzpflichten ableiten.[26] Diese bestehen u.a. in der staatlichen Verpflichtung, für die Forschung funktionsfähige institutionelle Voraussetzungen zu schaffen.[27] Dazu gehört eine finanzielle, personelle und sachliche Mindestausstattung. Bisher nicht anerkannt ist, dass der Staat darüber hinausgehend den Forschenden Informationsansprüche

25 Bizer, 44, mit Hinweisen darauf, wie aus dem Abwehranspruch Informationsansprüche abgeleitet werden.
26 Britz in Dreier, Art. 5 III, Rn. 58–62.
27 Britz in Dreier, Art. 5 III, Rn. 58f.; ausführlich Bizer, 56ff.

gewähren muss.[28] Angesichts beschränkter Ressourcen ist ein Anspruch auf Datenbeschaffung nur in einem sehr begrenzten Rahmen begründbar. Etwas anderes kann aber für die Bereitstellung vorhandener Informationsressourcen gelten.[29] Soweit von einer solchen Datenbeschaffung Dritte, etwa in ihrem Recht auf informationelle Selbstbestimmung, betroffen sind, müssen die damit verbundenen Eingriffe für diese Dritten zumutbar sein.[30] Über eine mittelbare Drittwirkung können sich selbst für Private aus dem Forschungsgrundrecht Verpflichtungen ergeben.[31]

Bei der Auslegung und Anwendung von Grundrechten sind die sich ändernden gesellschaftlichen und sonstigen Rahmenbedingungen zu berücksichtigen. Neben sozialen und ökonomischen Rahmenbedingungen spielen zunehmend **technische Gegebenheiten** eine bestimmende Rolle. Diese Änderungen veranlassen die Verfassungsrechtsprechung zu einer laufenden Hinterfragung und Weiterentwicklung ihrer bisherigen Rechtsprechung. Mit der modernen Informations- und Kommunikationstechnik sowie der Biotechnik haben sich neue Möglichkeiten und neue Risiken im Bereich der Forschung generell wie insbesondere auch im Bereich der Medizinforschung ergeben. Die ökologischen, ökonomischen und sozialen Herausforderungen in unserer globalisierten Gesellschaft können nur mithilfe einer freien Wissenschaft bewältigt werden. Wissenschaft wird teilweise schon als „fünfte Gewalt" zu einem Pfeiler des Machtgefüges in unserer modernen demokratischen Gesellschaft aufgewertet.[32] Dies wirkt sich letztlich auf die Interpretation der Grundrechte und des Rechts auf Forschungsfreiheit sowie des diese Rechte umsetzenden einfachen Rechts aus.[33]

Angesichts der modernen Herausforderungen durch Klimaveränderung, Pandemien, Umweltverschmutzung und Wachstum einer immer älter werdenden Bevölkerung kommt der datenbasierten Forschung mit genetischen, biometrischen oder sonstigen **Gesundheitsdaten** für Zwecke der Prävention, der Diagnostik und der Therapie eine signifikante Bedeutung zu.[34] Evidenz- und damit datenbasierte Forschung im Gesundheitsbereich ist zumeist die Arbeit mit personenbezogenen Daten von Patienten und Probanden, denen individuelle Grundrechte und insbesondere das Recht auf Datenschutz zustehen. Notwendig ist daher das Herstellen einer praktischen Konkordanz und eines Ausgleichs zwischen einer präzise zu definierenden Forschungsfreiheit und den tangierten individuellen Grundrechten.[35]

28 Bizer, 411ff., in Thesen sowie ausführlich in der gesamten Arbeit.

29 Peglau, Neue Justiz 1993, 440ff.; zur Ableitung generell aus Art. 5 GG Wegener, Der geheime Staat, 2006, 480ff.; ausführlich, aber ablehnend Bizer, 39ff.

30 Tinnefeld RDV 1995, 25; in der Vergangenheit wurde bei der Abwägung mit der Forschungsfreiheit immer wieder die „Hypertrophie des Datenschutzes" beklagt, so z.B. Duttge NJW 1998, 1615; zur Zumutbarkeit BVerfG 09.03.1988 – 1 BvL 49/86, BVerfGE 78, 77 (85, 87) = NJW 1988, 890, BVerfG 01.10.1987 – 2 BvR 1434/86, BVerfGE 77, 1 (47); BVerfG 19.11.1985 – 1 BvR 38/78, BVerfGE 71, 183 (196f.); Bizer, 209.

31 Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 62.

32 Illinger, Was Wissen schafft, SZ 26.03.2020, 4.

33 Bizer, 49f.

34 Datenethikkommission, 124.

35 Datenethikkommission, 124; Sachverständigenrat, 4ff.; Heberlein DVBl 2020, 1227.

3.1 Forschungsfreiheit allgemein

Das Grundrecht auf Forschungsfreiheit aus Art. 13 GRCh hat bisher auf **Unionsebene** nur eine begrenzte praktische Relevanz, da die Europäische Union (EU) über keine Eingriffsbefugnisse in den Bereichen Kultur (vgl. Art. 167 AEUV), Bildung (vgl. Art. 165f. AEUV) und Forschung (vgl. Art. 179ff. AEUV) verfügt.[36] Wohl aber hat die EU Gestaltungsmöglichkeiten im Bereich der Forschung. Dies gilt für den Bereich der Forschungsförderung, die Durchführung gemeinsamer Forschungsvorhaben wie auch für die datenschutzrechtliche Regulierung von Forschungsprojekten (s.o. Kap. 2.3).[37]

Die Forschungsfreiheit hat zunächst eine individualrechtliche Dimension. Sie soll das Streben des Einzelnen nach Erkenntnis und damit dessen freie Entfaltung ermöglichen. Daneben kommt der Forschungsfreiheit auch eine **gesamtgesellschaftliche Bedeutung** zu. Sie sichert den offenen Austausch in einer modernen Kulturgesellschaft.[38] Die freie wissenschaftliche Betätigung ist eine Grundbedingung für den Fortschritt in der Wirtschaft, im sozialen Leben, beim Schutz von Gesundheit, Natur und Umwelt und für die demokratische Meinungsbildung. An Forschung – mit oder ohne personenbezogene Daten – besteht grundsätzlich ein besonderes öffentliches Interesse.[39] Der Forschungsfreiheit kommt eine „Schlüsselfunktion" für eine *„Selbstverwirklichung des Einzelnen als auch für die gesamtgesellschaftliche Entwicklung"*[40] zu.

Der Begriff der Forschung wird in seiner grundrechtlichen Dimension[41] und bei der Auslegung der DSGVO[42] **weit verstanden**. Das europäische Grundrecht umfasst nicht nur die akademische Forschung und Grundlagenforschung, sondern auch die privatwirtschaftliche Forschung der Industrie sowie die Anwendungsforschung.[43] Grundsätzlich kann sich jeder auf das Grundrecht berufen, der zum Zweck des Erkenntnisgewinns unabhängig nach wissenschaftlichen Methoden tätig ist.[44]

Anders als das deutsche Verfassungsrecht, das keine explizite Schranke der Forschungsfreiheit enthält, gilt auf europäischer Ebene die allgemeine **Schrankenregelung** des Art. 52 Abs. 1 GRCh.[45] Aus diesem Unterschied ergeben sich aber keine praktischen Konsequenzen, da auch nach deutschem Verfassungsrecht anerkannt ist, dass die Forschungsfreiheit verfassungsimmanenten Schranken unterliegt, die per Gesetz konkretisiert werden können. Die Grenzen der Forschungsfreiheit sind in jedem Fall aus den Grundrechten und der Verfassung herzuleiten. Ein die Forschungs-

36 Sparr in Schwarze, Art. 13 GRCh Rn. 1.
37 Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 6f.
38 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72 Rn. 131, BVerfGE 35, 113.
39 Golla in Specht/Mantz, § 23 Rn. 3; Caspar in SHS, Art. 89 Rn. 13.
40 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 131, BVerfGE 35, 79 = NJW 1973, 1176; BVerfG 01.03.1978 – 1 BvR 333/75, Rn. 149; Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 17.
41 Bernsdorff in Meyer/Hölscheidt, Art. 13 Rn. 14; Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 63; Roßnagel/Geminn in Dierks/Roßnagel, 196.
42 ErwGr 159, 2; EDPS, 11; Johannes in Roßnagel 2017, § 7 Rn. 246; Geminn DuD 2018, 643; Buchner/Tinnefeld in Kühling/Buchner, Art. 89 Rn. 13; Roßnagel/Geminn in Dierks/Roßnagel, 207.
43 Johannes/Richter, DuD 2017, 300; Sparr in Schwarze, Art. 13 GRCh Rn. 3; Bernsdorff in Meyer/Hölscheidt, Art. 13 Rn. 15; Golla in Specht/Mantz, § 23 Rn. 14.
44 Ruffert in Callies/Ruffert, Art. 13 Rn. 8.
45 Ruffert in Callies/Ruffert, Art. 13 Rn. 11; Bernsdorff in Meyer/Hölscheidt, Art. 13 Rn. 12; Sparr in Schwarze, Art. 13 GRCh Rn. 5; Stern/Sachs, Art. 13 Rn. 22f.; BVerfG 01.03.1978 – 1 BvR 333/75, Rn. 154; BVerfGE 47, 327 = NJW 1978, 1621.

freiheit beschränkender Konflikt kann sich ergeben bei dem Schutz der Menschenwürde, von Leib und Leben anderer, des Rechts der Persönlichkeit, insbesondere beim Datenschutz.[46] Während die Wahrung der Menschenwürde (Art. 1 GRCh, Art. 1 Abs. 1 GG) zwingend ist, ist bei weiteren Grundrechten ein Ausgleich möglich und notwendig.[47]

3.2 Begriff der Forschung

Auf europäischer Ebene gibt es keine rechtsverbindliche **Definition** des Begriffs „Forschung".[48] In der Rechtsprechung des Europäischen Gerichtshofs (EuGH) spielte die Wissenschaftsfreiheit bisher nur eine untergeordnete Rolle.[49] Der Regelungsgehalt der GRCh entspricht aber insofern weitgehend dem des GG und ist durch dieses inspiriert.[50] Es gibt keine Gründe, hier hinsichtlich des Grundrechtsschutzes auf europäischer und auf deutscher Regelungsebene inhaltliche Differenzierungen vorzunehmen.[51]

Zu Art. 5 Abs. 3 GG besteht eine umfangreiche Rechtsprechung und juristische Literatur. Danach ist **wissenschaftliche Forschung**[52] ein auf wissenschaftlicher Eigengesetzlichkeit (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionsbereitschaft) beruhender Prozess zum Auffinden von Erkenntnissen, ihrer Deutung und ihrer Weitergabe. Wissenschaftliche Forschung ist *„alles, was nach Inhalt und Form als ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist"*.[53] Begriffsbestimmend für die Forschung ist also, dass **zielgerichtet neuartige Erkenntnisse** gewonnen werden sollen.[54] Es geht um das *„Bemühen nach Wahrheit als ‚etwas noch nicht ganz Gefundenes'"*.[55] Es genügt der ernsthafte Versuch; ein Erkenntniserfolg kann nicht gefordert werden.[56]

46 Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 41; Bizer, Forschungsfreiheit und informationelle Selbstbestimmung, 1992; Roßnagel/Geminn in Dierks/Roßnagel, 195; Graf von Kielmansegg in TMF, 87f.

47 Martini/Hohmann NJW 2020, 3577f.

48 Geminn, DuD 2018, 640f.; Roßnagel, ZD 2019, 158; zur EU-weiten Verwendung des Begriffs Stern/Sachs, Art. 13 Rn. 15.

49 Johannes in Roßnagel 2017, § 4 Rn. 56; EuGH 10.03.2005 – C-39/04, Rn. 23, Laboratories Fournier; EuGH 18.12.2007 – C-281/16, Rn. 59, Jundt.

50 Ruffert in Callies/Ruffert, Art. 13 GRCh Rn. 1; Roßnagel, ZD 2019, 158; Geminn, DuD 2018, 640; Roßnagel/Geminn in Dierks/Roßnagel, 197.

51 So im Ergebnis auch Geminn, DuD 2018, 640f.; anders wohl Ruffert in Callies/Ruffert, Art. 13 Rn. 6, in Bezug auf die „Wahrheitssuche".

52 Zur Differenzierung zwischen „wissenschaftlicher Forschung" und „Wissenschaft" Geminn, DuD 2018, 645f., Roßnagel/Geminn in Dierks/Roßnagel, 196ff.

53 BVerfGE 35, 112f. = NJW 1978, 1176; Werkmeister/Schwaab CR 2019, 85; Roßnagel, ZD 2019, 158f.; Stern/Sachs, Art. 13 Rn. 15; Johannes DuD 2012, 821; Weichert in HHJ, 422f.; BKL-R, 17; ähnlich Art. 2 lit. b Richtlinie 2005/71/EG des Rates über ein besonderes Zulassungsverfahren für Drittstaatsangehörige zum Zweck der wissenschaftlichen Forschung v. 12.10.2005, zur Erfordernis der Staatsferne Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, 231f.; Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 74f.

54 EDPS, 9f.; Schneider 2015, 97; Golla in Specht/Mantz, § 23 Rn. 15.

55 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 128, BVerfGE 35, 79 = NJW 1973; OLG Hamm 28.11.1995 – 1 VAs 38/94, NJW 1996, 941 = JR 1997, 172.

56 Werkmeister/Schwaab CR 2019, 86.

Forschung hat eine zentrale Grundlage im **wissenschaftlichen Diskurs** und setzt Pluralität der Methoden und der Ergebnisse voraus. Geschützt wird nicht *„eine bestimmte Auffassung von der Wissenschaft oder eine bestimmte Wissenschaftstheorie"*, sondern *„jede wissenschaftliche Tätigkeit"*.[57] Der Fortschritt der Wissenschaft bedingt den Austausch und das *„wissenschaftliche Gespräch"*.[58] Die Teilhabe an diesem Gespräch ist eine Grundbedingung des Wissenschaftsbetriebs; der Staat ist verpflichtet, organisatorische Maßnahmen für diese Teilhabe zu ergreifen.[59] Über die leistungsrechtliche Komponente der Forschungsfreiheit müssen staatlicherseits normative Rahmenbedingungen geschaffen werden, die Forschenden ihre Grundrechtsausübung erst ermöglicht (s.o. Kap. 3).

Forschung ist nicht dadurch ausgeschlossen, dass das Vorhaben auch Ausbildungs- und Prüfungszwecken dient. Dissertations- und Habilitationsvorhaben sind regelmäßig als Forschungsvorhaben anzusehen,[60] nicht aber eine vorrangig der Ausbildung dienende Studienarbeit. Nicht erfasst von dem gegenüber dem Begriff „Wissenschaft" engeren Begriff der „Forschung" ist die **wissenschaftliche Lehre**.[61] Etwas anderes kann gelten, wenn die Lehrtätigkeit zugleich von der den Forschungsbegriff prägenden Erkenntnissuche getragen wird.[62]

Forschung erstreckt sich auch auf vorbereitende und unterstützende Aktivitäten sowie die Publikation. Vom **Schutzbereich** der Forschung nicht mit umfasst ist die **Anwendung und Umsetzung** von über die Forschung gewonnenen Erkenntnissen (ErwGr 159 DSGVO).[63]

Hinsichtlich der durch die Forschungsfreiheit Begünstigten macht das Grundrecht zunächst keinerlei Einschränkungen; *„jeder wissenschaftlich Tätige"* kann sich hierauf berufen.[64] **Grundrechtsträger** sind nicht nur Universitäten und Forschungsgesellschaften; jede natürliche oder juristische Person kann sich auf die Forschungsfreiheit berufen.[65]

Die Forschungsfreiheit hat auch einen **informationellen Bestandteil**. Der Forschende genießt eine individuelle wissenschaftliche Handlungsfreiheit. Zur Freiheit des Forschenden gehört auch, nicht durch Überwachung und Kontrolle in seiner Autonomie grundlos und unverhältnismäßig eingeschränkt zu werden. Die in der Forschung tätigen Personen, seien es juristische Personen und Institutionen oder natürliche Personen, sind in ihrer wissenschaftlichen Entfaltung grundsätzlich frei. Ein-

57 BVerfG 01.03.1978 – 1 BvR 333/75, Rn. 151; BVerfGE 47, 327 = NJW 1978, 1621; BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 128, BVerfGE 35, 79 = NJW 1973; Johannes in Roßnagel 2017, § 4 Rn. 57f.

58 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 129, BVerfGE 35, 79 = NJW 1973.

59 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 133f., BVerfGE 35, 79 = NJW 1973; Weichert ZD 2020, 19.

60 OLG Hamm 28.11.1995 – 1 VAs 38/94, NJW 1996, 941 = JR 1997, 172; Kühling, 67f., a.A. offenbar der BfDI gemäß der gleichen Quelle.

61 Caspar in SHS, Art. 89 Rn. 11f.; Johannes in Roßnagel 2017, § 4 Rn. 59; Bernsdorff in Meyer/Hölscheidt, Art. 13 Rn. 14.

62 Weichert in DWWS, Art. 89 Rn. 11.

63 Roßnagel, ZD 2019, 159; Roßnagel in SHS, Art. 5 Rn. 106; Johannes in Roßnagel 2018, § 7 Rn. 247; Geminn, DuD 2018, 644; Bernsdorff in Meyer/Hölscheidt, Art. 13 Rn. 14.

64 Roßnagel/Geminn in Dierks/Roßnagel, 197; Ruffert in Callies/Ruffert, Art. 13 GRCh Rn. 8.

65 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 128; NJW 1973, 1176; BVerfG 03.03.1993 – 1 BvR 757/88 u. 1 BvR 1551/88, Rn. 41 = BVerfGE 88, 136; Johannes DuD 2012, 821f.

schränkungen bedürfen einer Legitimation.[66] Soweit die Forschenden in einem Beschäftigungsverhältnis tätig sind, gelten die Regelungen des Beschäftigtendatenschutzes (Art. 88 DSGVO, § 26 BDSG sowie viele weitere spezifische Regelungen).[67]

3.3 Unabhängigkeit der Forschung

Selbst wenn man Unabhängigkeit nicht als Definitionsmerkmal der Forschungsfreiheit ansieht, so wird diese bestimmend, wenn damit gesellschaftliche oder individuelle Beschränkungen verbunden sind.[68] Ohne diese Unabhängigkeit ist nicht gewährleistet, dass das Erkenntnisinteresse bei der forschenden Tätigkeit im Vordergrund steht. Nur unabhängige Forschung ist „frei" und damit Motor für gemeinnützige Innovation.[69] Daher ist **unabhängige Forschung** Voraussetzung für eine rechtliche Privilegierung.[70]

Der weit auszulegende Begriff der Forschung schließt grundsätzlich **privat finanzierte Forschung** mit ein (ErwGr 159 S. 1 DSGVO).[71] Eine externe Einflussnahme auf den wissenschaftlichen Erkenntnisprozess oder eine Unterordnung unter wirtschaftliche oder sonstige Interessen muss aber ausgeschlossen sein.[72] Dies gilt insbesondere für jede Art von externen Weisungen.[73]

Wissenschaftliche Untersuchungen, die zu **Organisations-, Aufsichts- und Kontrollzwecken** vorgenommen werden, verfolgen vorrangig keine wissenschaftliche Zielsetzung.[74] Wird z.B. eine Auswertung der Gesundheitsdaten von Beschäftigten durchgeführt, um die Leistungsfähigkeiten und Störungen in verschiedenen Abteilungen eines Unternehmens zu analysieren, so kann die Forschungsfreiheit nicht in Anspruch genommen werden. Untersucht dagegen ein außenstehender Forscher die Bedingungen in mehreren Unternehmen und erhalten diese Unternehmen aggregierte, verallgemeinerungsfähige Ergebnisse, so handelt es sich um Forschung.

Einen gesteigerten Grundrechtsschutz kann auch Werbeforschung nicht in Anspruch nehmen.[75] Auf die Entwicklung neuer Produkte ausgerichtete Forschung (z.B. der Pharmaindustrie) und **rein oder vorrangig kommerzielle** Absatz- oder Markt- und Meinungsforschung kommen auch nicht in den Genuss der Privilegierung nach den datenschutzrechtlichen Forschungsregelungen.[76] Entsprechendes gilt für die Spei-

66 Johannes DuD 2012, 821.
67 Johannes DuD 2012, 819f.; einen Überblick über die neuen Landesgesetze geben Weichert CuA 2018, 26ff.; Gola in Gola/Heckmann, § 26 Rn. 187–192,
68 Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 20; Schäfer in Kipker/Voskamp, 331.
69 Ruffert in Callies/Ruffert, Art. 13 Rn. 7.
70 Roßnagel/Geminn in Dierks/Roßnagel, 207; Ruffert in Callies/Ruffert, Art. 13 GRCh Rn. 7; Schneider 2015, 97f.; Martini/Hohmann NJW 2020, 3576; Weichert 2018, Kap. 6.12; ders. in HHJ, 424f.; BfDI, TB 2020, Kap. 7.3 (S. 68); deskriptiv Dierks 2020, 8.
71 Geminn, DuD 2018, 643; Caspar in SHS, Art. 89 Rn. 12.
72 Geminn, DuD 2018, 643.
73 Metschke/Wellbrock, Datenschutz in Wissenschaft und Forschung, 2000, 35.
74 Geminn, DuD 2018, 644; Johannes in Roßnagel 2018, § 7 Rn. 247.
75 Werkmeister/Schwaab CR 2019, 87; Johannes in Roßnagel 2017, § 4 Rn. 104.
76 Caspar in SHS, Art. 89, Rn. 16, 18; Greve in Auernhammer, Art. 89 Rn. 4; Werkmeister/Schwaab, CR 2019, 86; Schantz/Wolff-Wolff, Rn. 415; Johannes in Roßnagel 2017, § 4 Rn. 117; Jaspers/Schwartmann/Mühlenbeck in SJTK Art. 9 Rn. 197; so schon Simon/Vesting, CR 1992, 307; Simitis in Simitis, § 40 Rn. 43; a.A. Krohm in Gola/

cherung und Bereitstellung genetischer Daten durch Unternehmen, denen Betroffene ihre Daten und Gewebeproben mit einem genealogischen oder Lifestyle-Interesse zur Verfügung gestellt haben.[77]

Etwas anderes gilt, wenn vorrangig mit kommerziellem Interesse erhobene Daten von Forschenden erhoben und weiterverarbeitet werden, wenn diese mit ihren pharmakologischen, genetischen oder Markt- und Meinungs-Untersuchungen den Anforderungen an **wissenschaftliche Unabhängigkeit und Erkenntnisgetriebenheit** genügen.[78] Die Unabhängigkeit der Forschung ist nicht schon dadurch beeinträchtigt, dass der Auftrag hierfür durch eine dritte Stelle erteilt wird und/oder die Finanzierung des Forschungsvorhabens durch diese oder durch eine weitere Stelle erfolgt und dass eine Fragestellung vorgegeben wird. Dies gilt, selbst wenn diese Stellen ein Interesse an den (unabhängig erlangten) Erkenntnissen haben. Wichtig ist, dass auf den Erkenntnisprozess selbst kein Einfluss genommen wird.[79] Die Art der Finanzierung durch Drittmittel muss also nicht, kann aber die Unabhängigkeit beeinträchtigen.[80]

Die Aussage, dass der Begriff der Forschungszwecke weit auszulegen ist, bezieht sich auf die **inhaltlichen Fragestellungen** der Forschung, nicht auf die **Methoden** und die damit verfolgten Zwecke. Zwar haben die Forschenden das Recht, ihre Methoden selbst zu wählen, um der „Wahrheit" möglichst nahe zu kommen.[81] Eine *„scheinwissenschaftliche Begründung vorgegebener Ergebnisse"* kann aber rechtlich nicht privilegiert werden.[82] Entsprechendes gilt für falsches Zitieren oder für Plagiate.[83] Fehlt es an der wissenschaftlichen Methode oder werden andere Zwecke als das Streben nach Erkenntnis verfolgt (Art. 89 Abs. 4 DSGVO), so ist eine Privilegierung nicht gerechtfertigt.

3.4 Transparenz

Zu den Charakteristika wissenschaftlicher Forschung gehört, dass sie offen für Hinterfragung und Kritik ist. Dies setzt eine grundsätzliche Offenheit und Transparenz voraus.[84] Die Veröffentlichung der Erkenntnisse ist ein zentraler Bestandteil des wissenschaftlichen Dialogs.[85] Die wissenschaftliche Gemeinschaft soll die Möglichkeit haben, diese Ergebnisse auf ihre Richtigkeit hin zu überprüfen.[86] Auch soll sie die

Heckmann, § 27 Rn. 15–19, 24; Hornung/Hofmann, ZD-Beilage 4/2017, 5; zu wenig differenziert Johannes/Richter, DuD 2017, 302.

77 EDPS, 7f.; Weichert DuD 2019, 152.

78 Hornung/Hofmann, ZD-Beilage 4/2017, 5; Caspar in SHS, Art. 89, Rn. 12, 16; Golla in Specht/Mantz, § 23 Rn. 15; Krohm in Gola/Heckmann, § 27 Rn. 14.

79 Geminn, DuD 2018, 643f.; Schneider 2015, 98; Hornung/Hofmann, ZD-Beilage 4/2017, 4f.; Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 20.

80 EDPS, 10; Caspar in SHS, Art. 89 Rn. 17; Weichert ZD 2020, 19f.; Platzer NZS 2020, 293f.; kritischer Simitis in Simitis, § 40 Rn. 36; aufschlussreich das Interview mit Kreiß, Buchwald, „Da fällt die Wahrheit manchmal unter den Tisch", SZ 28.11.2019, 36.

81 Dreier-Britz, Art. 5 III (Wissenschaft), Rn. 24; GMDS, 6; Schlüchter/Duttge JR 1997, 173f.; Weichert ZD 2020, 20.

82 EDPS, 11f.; Geminn, DuD 2018, 643; Schneider 2015, 97f.

83 Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 7. Aufl. 2020, Rn. 512.

84 EDPS, 10; Weichert in HHJ, 426f.; zur ethischen Dimension Streck in TMF, 55, 58.

85 Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 26; dies ist nicht gleichzusetzen mit der kommerziellen Verwertung.

86 Schneider 2015, 98; so auch Roßnagel/Geminn in Dierks/Roßnagel, 209; a.A. Geminn, DuD 2018, 644.

Möglichkeit haben, auf den Ergebnissen aufbauend weitere Erkenntnisse zu suchen. Forschung ist „letztlich auf **Kommunikation und Publikation** ausgerichtet" (vgl. Art. 179 Abs. 1 AEUV).[87] Die kommunikative Rolle der Forschung spiegelt sich in der Regelung des Art. 85 DSGVO wider, der die wissenschaftlichen Zwecke in den Regelungsbereich „Meinungsäußerung und Informationsfreiheit" einordnet.[88]

Vom Schutzbereich der Forschungsfreiheit mit umfasst ist grundsätzlich die Wahl des Ortes, des Zeitpunktes und der Modalitäten der Publikation der wissenschaftlichen Ergebnisse. Die Entscheidung, auf eine **Veröffentlichung zu verzichten**, ist grundrechtlich geschützt, ja selbst die von Anfang an bestehende Absicht, die Ergebnisse nicht mit anderen zu teilen.[89]

Dagegen bedarf Forschung mit personenbezogenen Daten, die für sich eine rechtliche Privilegierung, also die teilweise Freistellung von Datenschutzprinzipien, in Anspruch nimmt, einer besonderen Legitimation. Diese begründet eine **Transparenzpflicht**, also die Bereitschaft, gegenüber der Gemeinschaft die Nutzung der Daten aus der Gemeinschaft zu begründen und zu rechtfertigen. Die Rechtfertigung liegt in der gemeinschaftsnützlichen „Suche nach der Wahrheit" und der engen Zweckbindung daran. Die Veröffentlichung der Ergebnisse ist Voraussetzung dafür, dass die Gemeinschaft aus einem Projekt einen Nutzen ziehen kann. Rechtlich privilegiertes wissenschaftliches Arbeiten setzt daher eine dahingehende Absicht voraus.[90] Dass eine solche Zielrichtung verfolgt wurde, kann nur festgestellt werden, wenn nach Beendigung einer Forschungsarbeit die wesentlichen Ergebnisse in einer bestimmten Form öffentlich zugänglich gemacht werden.[91] Der Zugriff auf personenbezogene Daten für Zwecke der Forschung und die damit verbundene begrenzte Aufhebung der Zweckbindung lassen sich nur legitimieren, wenn die Allgemeinheit hiervon zumindest potenziell einen Nutzen hat und eine gewisse Kontrolle stattfindet. Diese Gemeinwohlorientierung beschränkt sich nicht auf die Forschung an Hochschulen.[92]

Neben den Forschungserkenntnissen sind auch die **Forschungsmethoden** in einer nachvollziehbaren Weise offenzulegen. Auch diese müssen einem fachlichen Diskurs unterworfen werden können. Erweist sich eine Methode als unwissenschaftlich, so kann sie schon begrifflich nicht in den Genuss der Forschungsfreiheit gelangen. Unseriöse Methoden können zu Falscherkenntnissen führen. Gerade zu Zeiten, in denen wissenschaftliche Erkenntnisse für viele Fragen des gesellschaftlichen Lebens von höchster Relevanz sind, muss verhindert werden, dass Fake News als scheinbar wissenschaftliche Fakten gesellschaftliche Anerkennung finden und Schaden anrichten. Es ist eine zentrale Funktion von wissenschaftlicher Forschung, derartige Fake News als solche zu identifizieren. Bei der Offenlegung der Methoden geht es darum, die Plausibilität des Forschungsansatzes zu beurteilen. Hierfür ist es regelmäßig nicht nötig, Betriebs- und Geschäftsgeheimnisse zu offenbaren (s.u.).

87 BVerfG 01.03.1978 – 1 BvR 333/75, Rn. 180, BVerfE 47, 327 = NJW 1978, 1621; so letztlich auch Geminn, DuD 2018, 645.
88 EDPS, 10; Hornung/Hofmann, ZD-Beilage 4/2017, 12.
89 Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 26 m.w.N.; zur Veröffentlichungspflicht durch Hochschule BKL-R, 18f.
90 Schneider 2015, 98; a.A. Roßnagel/Geminn in Dierks/Roßnagel, 209.
91 Roßnagel/Geminn in Dierks/Roßnagel, 131.
92 BVerfG 01.03.1978 – 1 BvR 333/75, Rn. 180, BVerfGE 47, 327 = NJW 1978, 1621.

Diese Transparenzpflichten lassen sich **verfassungsrechtlich begründen**: Eingriffe in das Recht auf informationelle Selbstbestimmung müssen von Betroffenen hinreichend überprüfbar sein. Entsprechende Transparenzpflichten ergeben sich in Umsetzung des Verfassungsrechts gesetzlich zumindest indirekt aus Art. 5 Abs. 1 lit. a DSGVO sowie aus Art. 89 Abs. 1 S. 1, 2 DSGVO.[93] Durch entsprechende organisatorische Vorgaben werden Garantien für die Wahrung der Betroffenenrechte geschaffen. Eine spezifischere gesetzliche Grundlage hierfür besteht derzeit nicht. Im Interesse der Rechtssicherheit für Forschende wie sonstige Beteiligte sollten insofern **normative Konkretisierungen** erfolgen (s.u. Kap. 14.2).

Der Offenlegungspflicht kann nicht entgegengehalten werden, dass **Forschung ergebnisoffen** ausgerichtet ist und daher scheitern kann.[94] Auch das Scheitern eines Forschungsprojektes kann zum Erkenntnisgewinn zumindest insofern beitragen, als eine These nicht bestätigt wurde oder eine Methode sich nicht als valide erwiesen hat. Der Umstand, dass viele Forschungsprojekte, insbesondere gescheiterte, unveröffentlicht bleiben, hat auch negative Folgen für den gesamtgesellschaftlichen Erkenntnisprozess: Es besteht das Risiko, dass die fehlende Öffentlichkeit dazu führt, dass als nicht valide erwiesene Forschungsansätze wiederholt verfolgt werden und dadurch wertvolle Ressourcen unnötig verschwendet werden. Zudem entsteht ein „Publication Bias" bei Meta-Forschungsanalysen durch eine Verzerrung des Gesamtblicks auf Forschungsergebnisse in einem bestimmten Bereich. Schließlich können sich aufgrund fehlender Transparenz unseriöse Forschende leichter und langfristiger im öffentlichen Diskurs positiv darstellen.[95]

Zudem wird vorgetragen, dass eine Veröffentlichungspflicht zur Folge hätte, dass *„ein großer Teil der Forschung im Bereich der Landesverteidigung von einer Sonderbehandlung ausgeschlossen"* würde. Auch die kommerzielle Forschung werde oftmals an einer **Geheimhaltung** von Forschungsergebnissen interessiert sein.[96] Zweifellos gibt es Forschungsergebnisse, die wegen ihrer Brisanz geheim gehalten werden sollten. Die Forschungsgeschichte zeigt, dass entsprechende Geheimhaltungsversuche allenfalls mittelfristig Erfolg zeigten. Auch besteht ein öffentliches Geheimhaltungsinteresse etwa im Militärbereich eher im Bereich der Umsetzung der Forschungsergebnisse als in deren inhaltlichen Ergebnissen. Es kann jedenfalls nicht angehen, dass Eingriffe in die Rechtssphäre von Forschungsprobanden unkontrolliert zugelassen werden. Dies verstieße generell gegen die verfassungsrechtlichen Garantien der Grundrechte und des Rechtsschutzes. Wird eine Veröffentlichung der Ergebnisse aus Gründen eines im öffentlichen Interesse liegenden Geheimschutzes unterlassen, so bedarf es ausdrücklicher gesetzlicher Ausnahmevorschriften, die an die Stelle der öffentlichen Kontrolle eine vertrauenswürdige und unabhängige anderweitige Kontrolle gewährleisten und die sicherstellen, dass eine valide Abwägung zwischen den konfligierenden Grundrechten erfolgt.

Der Transparenzpflicht wird nicht dadurch hinreichend genügt, dass den **Datenschutzaufsichtsbehörden** im Fall einer Datenschutzkontrolle gemäß Art. 58 Abs. 1

93 Roßnagel, Review des Entwurfs zum vorliegenden Gutachten v. 02.02.2020, 6.
94 So Geminn, DuD 2018, 644; Roßnagel/Geminn in Dierks/Roßnagel, 208f.; Schneider 2015, 98.
95 Herrmann, Puzzle mit fehlenden Teilen – Psychologen ermitteln die Auswirkung unveröffentlichter Studien, SZ 13.01.2020, 14.
96 Roßnagel/Geminn in Dierks/Roßnagel, 209f.

DSGVO weitgehende Untersuchungsbefugnisse eingeräumt sind.[97] Zwar obliegt diesen umfassend gemäß Art. 1 Abs. 2 DSGVO der Schutz aller Grundrechte natürlicher Personen. Hierzu gehören auch der Schutz der Forschungsfreiheit sowie die Abwägung der Forschungsfreiheit mit dem Grundrecht auf Datenschutz. Für eine solche umfassende Grundrechtsabwägung fehlen den Datenschutzaufsichtsbehörden aber derzeit die notwendigen Ressourcen. Unabhängig davon sind die Datenschutzaufsichtsbehörden auch nicht strukturell darauf angelegt, das nötige öffentliche Interesse an Datenschutzeingriffen abschließend zu bewerten.

Aus diesem Grund sprechen einige Forschungsregelungen **weiteren Stellen** Genehmigungs- und Kontrollzuständigkeiten zu.[98] Diese Regeln gelten aber nicht für sämtliche datenschutzrechtlich privilegierten (medizinischen) Forschungsvorhaben. Zudem bestehen etwa bei obersten Bundes- oder Landesbehörden Zweifel, ob in der Praxis die Unabhängigkeit, Prüftiefe und Kompetenz gewährleistet ist, die im Interesse des Schutzes des Forschungsfreiheit und des Datenschutzes nötig ist.

Die Festlegung des Umfangs der Transparenzpflicht bei privilegierter Forschung obliegt dem Gesetzgeber. Bisher gibt es nur sehr eingeschränkt Veröffentlichungspflichten.[99] Insofern besteht ein **gesetzgeberisches Defizit**, das eine Änderung der rechtlichen Rahmenbedingungen nötig macht (dazu Kap. 14.2). Solange dieses Defizit nicht behoben ist, liegt es an den Genehmigungs- und Kontrollinstanzen, im Rahmen ihrer Befugnisse die Transparenz einzufordern, die notwendig ist, um das öffentliche Interesse an dem Projekt zu begründen und die Grundrechtseingriffe zu rechtfertigen.

Hinsichtlich des **Zeitpunkts der Veröffentlichung** von Forschungsergebnissen ist grundsätzlich anerkannt, dass dieser vom Wissenschaftler selbst bestimmt werden kann.[100] Dieses Bestimmungsrecht ist aber eingeschränkt, soweit dem die Interessen Drittbetroffener entgegenstehen. Zweifellos besteht für den Forschenden auch bei personenbezogener Forschung ein großer Beurteilungsspielraum.[101] Dabei können Aspekte medialer Aufmerksamkeit oder des Patentschutzes eine Rolle spielen.[102] Auch die Vermarktung der Ergebnisse sowie Wünsche eines Mittelgebers können von Relevanz sein. Doch darf dieser Zeitpunkt nicht so weit vom Abschluss eines Forschungsprojektes entfernt sein, dass dadurch die Aufmerksamkeit hierfür nicht mehr hergestellt werden kann und damit der Diskurs hierüber nicht mehr stattfindet. Die Fragen des Umfangs und Zeitpunktes der Veröffentlichung oder der sonstigen Offenlegung der Ergebnisse kann zumindest bei personenbezogener Forschung, die eine rechtliche Privilegierung für sich in Anspruch nimmt, einer normativen Festlegung zugeführt werden, da unzulässige Datennutzungen unter den Vorzeichen der Forschung zu einem bestimmten Zeitpunkt einer Prüfung und einer möglichen Sanktionierung unterworfen werden können müssen.[103]

97 So Roßnagel, Review des Entwurfs zum vorliegenden Gutachten v. 02.02.2020, 6.
98 Ministerien, Ethik-Kommissionen, vgl. § 75 Abs. 5 SGB V, § 15 MBO-Ä.
99 Im Bereich der Medizinforschung z.B. § 303d Abs. 1 lit. d SGB V.
100 BVerfG 01.03.1978 – 1 BvR 333/75, BVerfGE 47, 327 (393); Roßnagel/Geminn in Dierks/Roßnagel, 209;
101 Schneider 2015, 98.
102 Schneider 2015, 98.
103 Vgl. Geminn, DuD 2018, 645.

Die Offenlegung der wesentlichen Merkmale der **wissenschaftlichen Fragestellung und Methodik** von Forschungsprojekten mit personenbezogenen Daten muss zumindest im Hinblick auf deren Zulassung vor der Nutzung der Daten erfolgen. Adressat der Offenlegung muss nicht die Öffentlichkeit oder die wissenschaftliche Gemeinschaft allgemein sein; eine Vorabbewertung der Wissenschaftlichkeit der Methoden und der Grundrechtskonformität kann auch durch ein insofern qualifiziertes Gremium wie etwa eine Ethikkommission oder ein Use-and Access-Committee (UAC, s.u. Kap. 14.2) erfolgen.[104]

104 Zum Transparenzerfordernis s.a. Weichert ZD 2020, 20.

4 Rechtsgrundlagen

Die Feststellung der Rechtsgrundlagen für eine forschende Datenverarbeitung ist für deren Zulässigkeit grundlegend: Zwar muss bei der Auslegung gesetzlicher Regelungen immer der verfassungsrechtliche Rahmen beachtet werden. Für die konkrete Anwendung ist aber vorrangig der **Wortlaut** der Rechtsgrundlagen bestimmend. Dieser ist auch der Bezugspunkt für die Transparenz für die Betroffenen, für die Wahrnehmung der Betroffenenrechte, für die Verarbeitungsprozesse beim Verantwortlichen und das zu implementierende Datenschutzmanagement sowie für die stelleninterne, aufsichtliche und gerichtliche Kontrolle.

4.1 Europäisches und nationales Recht

Die EU hat ihre Regelungskompetenzen (s.o. Kap. 2.3) mit der **Datenschutz-Grundverordnung** (DSGVO) wahrgenommen (Verordnung [EU] 2016/679). Die DSGVO ist – anders als deren Vorgängerregelung, die europäische Datenschutzrichtlinie 95/46/EG (EG-DSRl) – als Verordnung i.S.v. Art. 288 Abs. 2 AEUV europaweit direkt anwendbar und in allen Teilen verbindlich.[105]

Neben der DSGVO gibt es weitere **spezielle europäische Regelungen**, die eine Relevanz für die medizinische Forschung und die hierbei stattfindende Datenverarbeitung

105 Albrecht/Jotzo, Teil 1 Rn. 25; Kühling/Raab in Kühling/Buchner, Einführung Rn. 73–76, Selmayr/Ehmann in Ehmann/Selmayr, Einführung Rn. 43; Dierks in Dierks/Roßnagel, 9.

haben. Diese sollen vorliegend nur aufgeführt werden:[106] die Verordnung über klinische Prüfungen[107], die Richtlinie menschliches Gewebe und Zellen[108], die Datenbank-Richtlinie[109] und die Patientenrechte-Richtlinie[110].

Die DSGVO enthält eine Vielzahl von für die Forschung relevanten **Öffnungsklauseln**.[111] Teilweise wird der Begriff „Öffnungsklausel" abgelehnt, da damit suggeriert werde, dass von den inhaltlichen Vorgaben der DSGVO abgewichen werden könne. Dies ist nicht der Fall. Alternativ wird der Begriff „Spezifizierungsklausel" verwendet.[112] Missverständnisse bei Verwendung des inzwischen etablierten Begriffs sind nicht zwingend und in der Praxis auch nicht erkennbar. Deshalb wird dieser Begriff verwendet. Auf der Basis von Öffnungsklauseln erlassene nationale Gesetze dürfen der DSGVO nicht widersprechen, sondern sollen die Vorgaben der DSGVO präzisieren oder konkretisieren.[113]

Bei den Öffnungsklauseln wird unterschieden zwischen solchen, bei denen den Nationalstaaten die Gesetzgebung freigestellt wird (**fakultative Öffnungsklauseln**), und solchen, bei denen eine Pflicht zur Gesetzgebung besteht (**obligatorische Öffnungsklauseln**).[114]

Art. 6 Abs. 2, 3 i.V.m. Art. 6 Abs. 1 lit. e DSGVO erlaubt den Mitgliedstaaten die Schaffung von Rechtsgrundlagen für die Ausübung der öffentlichen Gewalt und die Wahrnehmung von **Aufgaben im öffentlichen Interesse**. Hierzu gehört in jedem Fall die Wahrnehmung der Forschung durch staatliche Hochschulen sowie Maßnahmen von Ministerien und anderen öffentlichen Stellen.[115] ErwGr. 45 S. 6 stellt zudem klar, dass auch natürliche oder juristische Personen des Privatrechts im öffentlichen Interesse tätig sein können. Als ein Beispiel nennt der Gesetzgeber *„gesundheitliche Zwecke, wie die öffentliche Gesundheit oder die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge"*.[116] Genannt werden als weitere öffentliche Interessen *„die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen"* (ErwGr 46 S. 3) sowie sogar *„wichtige wirtschaftliche oder finanzielle Interessen"* (ErwGr 73 S. 1 am Ende). Das öffentliche Interesse muss ein solches Gewicht haben, dass die Beschränkung des Grundrechts auf Datenschutz verhältnismäßig ist.[117] Inwieweit Forschung, die im öffentlichen Interesse durchgeführt wird, von dieser Öffnungsklausel erfasst sein soll, ist normativ nicht festgelegt.

106 Ausführlicher Health Ethics Policy Lab, 36ff.
107 Verordnung (EU) Nr. 536/2014 v. 16.04.2014, ABl. EU L 158/1 v. 27.05.2014.
108 Richtlinie 2004/23/EF v. 31.03.2004, ABl. L 102/48 v. 07.04.2004.
109 Richtlinie 96/9/EG v. 11.03.1996, ABl. L 77 20, zuletzt geändert durch Art. 24 ÄndRL (EU) 2019/790 v. 17.04.2019, ABl. L 130 92.
110 Richtlinie 2011/24/EU v. 09.03.2011, ABl. L 88/45, betrifft nur die grenzüberschreitende Gesundheitsversorgung; Schneider 2016, 425ff.
111 Roßnagel, ZD 2019, 159; Johannes in Roßnagel 2017, § 4 Rn. 83–89.
112 Selmayr/Ehmann in Ehmann/Selmayr, Einführung Rn. 89.
113 Roßnagel in SHS, Art. 6 Rn. 22.
114 Hornung/Spiecker in SHS Einl Rn. 228; Dierks in Dierks/Roßnagel, 9f.
115 BKL-R, 220ff.
116 Dierks 2019, 24.
117 Roßnagel in SHS, Art. 6 Abs. 1 Rn. 71.

Privat finanzierte und **von der Wirtschaft ausgeübte Forschung** wird nur erfasst, soweit damit konkret eine Aufgabenwahrnehmung im „öffentlichen Interesse" erfolgt.[118] Art. 6 Abs. 2 DSGVO sieht im letzten Halbsatz vor, dass die Öffnungsklausel *„einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX gilt"*. Kapitel IX umfasst die Art. 85 bis 91, also auch Art. 89 DSGVO. Daraus wird der Schluss gezogen, dass Art. 6 Abs. 2 DSGVO der Öffnungsklausel des Art. 89 Abs. 2 DSGVO vorgehe.[119] Darauf kommt es aber nicht an, da sich bzgl. des Umfangs die Regelungsrahmen von Art. 6 Abs. 2 und Art. 89 DSGVO nicht unterscheiden. Auch die Regulierung privilegierter Forschung setzt ein „öffentliches Interesse" hieran voraus (s.u. Kap. 8.1).

Gemäß Art. 6 Abs. 3 S. 3 DSGVO wird bei einer Verarbeitung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt die Befugnis eingeräumt, ***„spezifische Bestimmungen zur Anpassung** der Anwendung"* der DSGVO zu erlassen. Diese sollen sich darauf beziehen, *„welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen und welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung"*.

Diese Öffnungsklausel erweitert die Regelungsmöglichkeiten der Mitgliedstaaten.[120] Sie geht weiter als Abs. 2, bezieht sich aber, anders als Art. 6 Abs. 2 DSGVO, nicht auf sämtliche DSGVO-Regelungen, sondern nur auf die Rechtsgrundlagen.[121] Über Art. 6 Abs. 3 DSGVO wird zwar ein Regelungsspielraum geschaffen, doch muss sich dieser im Rahmen der Erlaubnistatbestände der DSGVO halten. Die Regelung präzisiert die inhaltlichen Anforderungen an das **spezifizierende nationale Recht**.[122] Die in Art. 89 Abs. 2 BDSG vorgesehenen Privilegierungen in Bezug auf Betroffenenbefugnisse werden von Art. 6 Abs. 3 DSGVO nicht mit umfasst.

Hinsichtlich der Verarbeitung **besonderer Datenkategorien** (sog. sensitive Daten)[123] sowie von Berufsgeheimnissen enthält Art. 9 Abs. 2, 3 DSGVO Öffnungsklauseln.[124] Die Öffnungsklausel in Art. 9 Abs. 2 lit. j DSGVO zur forschenden Verarbeitung von sensitiven Daten verlangt zusätzlich, dass das spezifizierende Recht *„den Wesensgehalt des Rechts auf Datenschutz wahrt"*. Damit wird auf Art. 52 Abs. 1 S. 1 GRCh Bezug genommen, der die Wesensgehaltsgarantie grundrechtlich absichert. Dabei handelt es sich letztlich um eine besondere Betonung und äußere Grenzziehung des Verhältnismäßigkeitsgrundsatzes.[125]

118 Johannes in Roßnagel 2017, § 4 Rn. 83, 85.

119 Roßnagel, Review zum vorliegenden Gutachten v. 02.02.2020, 7, mit Verweis auf BT-Drs. 18/12611, 117 m.w.N.

120 Roßnagel in SHS, Art. 6 Abs. 3 Rn. 36.

121 Roßnagel in SHS, Art. 6 Abs. 3 Rn. 37; differenzierend Frenzel in Paal/Pauly, Art. 6 Rn. 34ff.; a.A. Buchner/Petri in Kühling/Buchner, Art. 6 Rn. 195: gleicher Regelungsumfang; unentschieden Schulz in Gola, Art. 6 Rn. 172.

122 Dierks 2019, 24; Reimer in Sydow, Art. 6 Rn. 24; Schwartmann/Jaquemain in SJTK, Art. 6 Rn. 168; a.A. Kramer in Auernhammer, Art. 6 Rn. 62: implizite Festlegung des Zwecks genügt.

123 ErwGr 10, 5 spricht von „sensiblen Daten"; demgegenüber wird hier der Begriff „sensitive Daten" verwendet, mit dem die besondere Schutzbedürftigkeit besser zum Ausdruck kommt.

124 Kühling, 23ff.; Weichert in Kühling/Buchner, Art. 9 Rn. 138ff.; zur nationalen Relevanz bei der Forschung Geminn RDV 2019, 116ff.

125 Petri in SHS, Art. 9 Rn. 76; EuGH 06.10.2015 – C-362/14 (Safe Harbor), Rn. 94, NJW 2015, 3157.

Jeweils eine umfassende fakultative Öffnungsklausel enthalten schließlich Art. 85 DSGVO für die wissenschaftliche Kommunikation und Art. 89 Abs. 2 DSGVO für „Bedingungen und Garantien" bei **Forschungs- und Statistikzwecken** sowie hinsichtlich der erforderlichen Ausnahmen von Betroffenenrechten.[126] Voraussetzung für das Zurücktreten von Betroffeneninteressen ist, dass ein öffentliches Interesse an der Durchführung eines Forschungsvorhabens besteht und davon ausgegangen werden kann, dass verlässliche wissenschaftliche Ergebnisse zu erwarten sind.[127] Von Art. 85 DSGVO nicht mit umfasst sind Informationsbegehren von Betroffenen oder Kontrollbegehren im Rahmen der Datenschutzaufsicht.[128]

Einige der Öffnungsklauseln richten sich nicht nur an die Mitgliedstaaten, sondern fakultativ auch an die **Union**. Dies gilt insbesondere für die Regelung der Verarbeitung von Gesundheitsdaten als eine Form der sensitiven Daten (Art. 9 Abs. 2 lit. a, b, g, h, i, j DSGVO) sowie von Berufsgeheimnissen (Art. 9 Abs. 3 DSGVO). In diesen Bereichen ist die EU befugt, den Mitgliedstaaten verbindliche Vorgaben zu machen. Von diesen Möglichkeiten hat die EU im Bereich der Verarbeitung von Gesundheitsdaten bzw. im Medizinbereich bisher keinen Gebrauch gemacht.

Die **Intentionen** der Öffnungsklauseln unterscheiden sich. Teilweise sind sie einer fehlenden Regelungskompetenz der EU geschuldet (so Art. 85 DSGVO für den Medienbereich).[129] Teilweise liegt der Grund für sie in nationalen Regelungstraditionen und/oder in der fehlenden Bereitschaft der Mitgliedstaaten, sich auf EU-Ebene zu einigen.[130] Deutschland legte besonderen Wert darauf, dass das teilweise stark spezifizierte Datenschutzrecht und dort insbesondere das Sozialrecht (Art. 9 Abs. 2 lit. b DSVO), das Recht der öffentlichen Verwaltung und die Regelungen des Gesundheitswesens und der Berufsgeheimnisträger (Art. 9 Abs. 2 lit. b, h, i u. Abs. 3, Art. 90) beibehalten werden können.[131] Während die EU-Kommission für die Bereiche Forschung, Archive und Statistik zunächst einen weiten Ausgestaltungsvorschlag machte, wurde der Spielraum in den Art. 89 Abs. 2–4 DSGVO letztlich darauf beschränkt, dass Betroffenenrechte die Verarbeitungszwecke zumindest ernsthaft beeinträchtigen.[132]

Die für den Bereich der medizinischen Forschung relevanten Öffnungsklauseln in der DSGVO (Art. 6 Abs. 2, 3, 9 Abs. 2, 85, 89 Abs. 2)[133] haben unterschiedliche Anwendungsbereiche und Voraussetzungen und gewähren damit den Mitgliedstaaten unterschiedliche Regelungskompetenzen. Rechtfertigen **unterschiedliche Öffnungsklauseln** eine nationale Regelung, so ergänzen sie sich gegenseitig.[134] Doch muss auch bei der Anwendung der spezifizierenden Normen in jedem Fall der von der DSGVO vorgesehene Regelungsrahmen beachtet werden. Bei der Nutzung der Öffnungsklauseln muss zudem die Verhältnismäßigkeit der Eingriffe für den verfolgten Zweck ge-

126 Geminn, DuD 2018, 642.
127 Dierks 2019, 30; BKL-R, 205.
128 Johannes in Roßnagel 2017, § 4 Rn. 89.
129 Albrecht/Jotzo, Teil 9 Rn. 5.
130 Albrecht/Jotzo, Teil 1 Rn. 16, 18
131 Albrecht/Jotzo, Teil 1 Rn. 24, Teil 3 Rn. 46, 58.
132 Albrecht/Jotzo, Teil 9 Rn. 8.
133 Dierks 2019, 23ff.
134 A.A. wohl Richter in Roßnagel 2018, § 7 Rn. 163, Roßnagel, Review zum vorliegenden Gutachten v. 02.02.2020, 6f.

wahrt bleiben. Dies hat zur Folge, dass *„angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person"* vorgesehen sein müssen.[135]

National nicht abdingbar sind die in Art. 5 DSGVO festgelegten **Datenschutzgrundsätze**. Zur nationalen Disposition stehen kann daher auch nicht die generelle in Art. 5 Abs. 1 lit. b DSGVO gewährleistete Zweckprivilegierung. Nach anderer Ansicht soll die Zweckvereinbarkeitsfiktion nur gelten, wenn es keine Regelung eines Mitgliedsstaates zur Zweckänderung aufgrund einer einschlägigen Öffnungsklausel gibt. Eine solche könne in Art. 6 Abs. 3 S. 3 i.V.m. Art. 6 Abs. 1 lit. e DSGVO gesehen werden.[136] Dem kann nicht gefolgt werden, da danach die Regelung privilegierter Forschungsprojekte völlig der Disposition der nationalen Gesetzgeber überlassen bliebe. Dies kann nicht die Intention des EU-Gesetzgebers gewesen sein. Beschränkt man die Öffnungsklausel des Art. 6 Abs. 3 S. 3 DSGVO ausschließlich auf öffentliche Stellen, so hätte dies zur Folge, dass private privilegierte Forschung immer auf Art. 5 Abs. 1 lit. b DSGVO zurückgreifen könnte, nicht aber die von öffentlicher Hand betriebene Forschung. Es ist Ziel der Privilegierung, EU-weit die Nutzung von personenbezogenen Daten für die Forschung einheitlich zu erleichtern, ohne dass dies von Mitgliedstaaten wieder zurückgenommen werden kann.

Die Anwendbarkeit von Bundes- oder Landesrecht bei der Umsetzung der Öffnungsklauseln orientiert sich weitgehend an der Art der jeweils die personenbezogenen Daten **verarbeitenden Stellen**. So gilt für Stellen des Bundes (z.B. Forschungseinrichtungen, Bundeswehrklinik), für Sozialleistungsträger und für nicht-öffentliche (private) Stellen Bundesrecht.

Für **Stellen der Länder** sowie der Kommunen (Hochschulen, öffentliche Krankenhäuser, Gesundheitsbehörden) ist Landesrecht anwendbar, soweit nicht für spezifische Fragestellungen ein Bundesgesetz erlassen worden ist. In Bezug auf das Gesundheitswesen und die Forschung enthält das Grundgesetz (GG) keine spezifischen Gesetzgebungszuständigkeiten, sodass diese gemäß Art. 70 GG weitgehend bei den Ländern liegt. Bundeszuständigkeiten bestehen in Bezug auf die Privatwirtschaft (Art. 74 Abs. 1 Nr. 11 i.V.m. Art. 72 Abs. 1 GG), die Bundesverwaltung (Art. 87 GG) sowie das gesamte Sozialrecht (Art. 74 Abs. 1 Nr. 12 i.V.m. Art. 72 Abs. 1 GG, s.o. Kap. 2.4).

Landesrecht ist bei öffentlichen Stellen der Länder und der Kommunen im Ergebnis nicht oder nur sehr eingeschränkt anwendbar, soweit die **Forschung als Wettbewerbstätigkeit** einzustufen ist.[137] In diesem Fall tritt an die Stelle des Landesrechts das BDSG. Ob eine Wettbewerbstätigkeit anzunehmen ist, muss im Einzelfall beurteilt werden. Gründe hierfür können darin liegen, dass ein enger Zusammenhang mit einem primären Behandlungszweck besteht und die Behandlung im Wettbewerb erbracht wird. Aber auch die Forschungstätigkeit selbst steht im Wettbewerb, soweit diese in Konkurrenz zu anderen Einrichtungen um Mittelzuweisungen und valide Ergebnisse steht.[138]

135 So explizit Art. 9 Abs. 2 lit. j, inhaltlich ebenso Art. 89 DSGVO.

136 Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 10f.

137 § 2 Abs. 6 LDSG BW, Art. 1 Abs. 3 BayDSG, § 2 Abs. 6 BlnDSG, § 2 Abs. 3 BbgDSG, § 2 Abs. 3 BremDSGVOAG, § 2 Abs. 3 HmbDSG, § 2 Abs. 2 HDSIG, § 2 Abs. 5 DSG MV, § 1 Abs. 4 NDSG, § 5 Abs. 5 Nr. 4 DSG NRW, § 2 Abs. 4 LDSG RP, § 2 Abs. 3 SDSG, § 2 Abs. 3 SächsDSG, § 2 Ab. 7 Nr. 1 DSAG LSA, § 2 Abs. 4 LDSG SH.

138 Schneider 2015, 91f.

4.2 Datenschutz-Grundverordnung

Die seit dem 25.05.2018 direkt anwendbare und wirkende europäische Datenschutz-Grundverordnung (DSGVO) verfolgt das **Ziel**, das Datenschutzrecht an die technische Entwicklung anzupassen, insofern zu modernisieren und dadurch den Grundrechtsschutz zu verbessern (ErwGr 1, 2, 4, 6), das Datenschutzrecht zu harmonisieren und dadurch einheitliche Bedingungen für die Datenverarbeitung im Binnenmarkt zu schaffen (ErwGr 5, 7, 8). Die Zulässigkeit der Datenverarbeitung – auch für Forschungszwecke – ergibt sich aus den allgemeinen Regelungen der DSGVO, also aus Art. 5 und 6.[139]

Hinsichtlich der Verarbeitung von besonderen Datenkategorien (sensitive Daten), also z.B. von Gesundheitsdaten, werden Art. 9 Abs. 2 DSGVO sowie darauf basierende weitere Normen als eigenständige **Rechtsgrundlagen** angesehen.[140] Dies wird damit begründet, dass die Vorgaben von Art. 6 DSGVO zu unspezifisch für die Verarbeitung von sensitiven Daten seien. Außerdem sei unklar, in welcher Kombination aus Tatbestandsvoraussetzungen des Art. 6 Abs. 1 DSGVO mit solchen des Art. 9 Abs. 2 DSGVO eine wirksame Legitimation zu sehen sei.[141] Die Vorgaben Art. 6 Abs. 1 DSGVO sind tatsächlich sehr unspezifisch. Sie sind aber in mancher Hinsicht spezifischer als die in Art. 9 Abs. 2 DSGVO, z.B. wenn es um das Abwägungserfordernis in Art. 6 Abs. 1 lit. f DSGVO geht. Richtig ist, dass sich die Art. 6 und 9 DSGVO gegenseitig ergänzen. Die Unsicherheit über die Rechtsgrundlagen besteht schon über den Umstand, dass diese oft auf den Öffnungsklauseln in Art. 6 Abs. 1 oder Art. 9 Abs. 2 DSGVO beruhen. Würde zwischen Art. 6 Abs. 1 und Art. 9 Abs. 2 DSGVO ein Ausschlussverhältnis gesehen, so bestünde die Möglichkeit, dass sensitive Daten einen geringeren Schutz genössen als nicht-sensitive Daten. Zudem ließe sich dogmatisch schwer erklären, weshalb Art. 6 Abs. 4 DSGVO bei einer sensitiven Datenverarbeitung anzuwenden wäre.[142]

Mit den Regelungen in Art. 9 Abs. 2 DSGVO werden die sehr allgemeinen Vorgaben des Art. 6 konkretisiert und eingeengt.[143] Da die Art. 6 und 9 DSGVO jeweils Öffnungsregelungen enthalten, die eine weitere Konkretisierung der Vorgaben ermöglichen, kann durch diese Rechtsgrundlagen (z.B. im BDSG oder im spezifischen Datenschutzrecht) eine weitere Präzisierung und Einengung erfolgen. Deren Anwendung muss sich aber **im Rahmen der Art. 6 und 9 DSGVO** halten.[144] Der Europäische Datenschutzausschuss benennt daher sowohl Art. 6 in seinen besonderen Ausprägungen wie auch Art. 9 DSGVO gemeinsam als Rechtsgrundlage.[145] Durch die Privilegierung für Forschungszwecke in der DSGVO erfolgen auch Befugnisausweitungen in Bezug auf die Zweckänderung oder die Betroffenenrechte. Maßstab ist der Grundrechtsein-

139 Albrecht/Jotzo, Teil 3 Rn. 72; Geminn, DuD 2018, 641.
140 Dierks 2019, 25.
141 Dierks 2019, 25.
142 Dafür Dierks 2019, 25f.; weitergehend z.B. Schiff in Ehmann/Selmayr, der unter Art. 9 DSGVO Art. 6 Abs. 4 DSGVO nicht zur Anwendung bringen will (s.u. Kap. 4.4).
143 Kühling, 45; Weichert in Kühling/Buchner, Art. 9 Rn. 4; Petri in SHS, Art. 9 Rn. 3; Golla in Specht/Mantz, § 23 Rn. 24, 26; Werkmeister/Schwaab CR 2019, 87.
144 Golla in Specht/Mantz, § 23 Rn. 34f.; Piper DANA 2019, 72; zu § 27 BDSG Johannes/Richter, DuD 2017, 302; Werkmeister/Schwaab CR 2019, 89; Krohm in Gola/Heckmann, § 27 Rn. 7f.
145 EDSA, 5f., 8f. (Rn. 10–13, 25–28).

griff in das informationelle Selbstbestimmungsrecht der Betroffenen in Abwägung mit der Ermöglichung freier Forschung.

Ein zentraler Abwägungsaspekt ist, wie hoch das **Risiko einer Zweckentfremdung**, also einer übermäßig eingreifenden Zweckänderung, ist. Hierbei spielen technische, organisatorische wie auch rechtliche Erwägungen eine Rolle. Solange kein gesetzlich garantiertes Forschungsgeheimnis vor einem Datenzugriff und einer Nutzung durch Sicherheitsbehörden oder sonstige administrativ tätige Stellen bewahrt, ist dies im Rahmen der Abwägung mit zu berücksichtigen.[146]

Bei der Abwägung zwischen Datenschutz, weiteren Betroffenengrundrechten und der Forschungsfreiheit ist von Bedeutung, aus welcher Quelle die personenbezogenen Informationen stammen. Generell gilt zwar, dass es in Zeiten der automatisierten Datenverarbeitung kein belangloses Datum gibt.[147] Dessen ungeachtet hängt die **Intensität der informationellen Eingriffe** davon ab, ob Daten zum Kernbereich privater Lebensgestaltung gehören, aus dem Intimbereich stammen, aus sozialen Beziehungen der Betroffenen oder aus der Öffentlichkeitssphäre.[148]

Daten, die der **Öffentlichkeitssphäre** zuzuordnen sind und öffentlich zugänglich sind, so wie dies bei Daten im Internet der Fall ist, unterliegen also auch dem Persönlichkeitsschutz, sodass bei deren Verarbeitung eine Abwägung zwischen den Betroffenenbelangen und den Verarbeitungsinteressen nötig ist.[149] Art. 9 Abs. 2 lit. e DSGVO setzt für die Zulässigkeit der Verarbeitung besonderer Datenkategorien voraus, dass die öffentliche Zugänglichkeit der Daten auf einer offensichtlich bewussten Handlung des Betroffenen basiert.[150] An dem Abwägungserfordernis ändert auch der Umstand der generellen Privilegierung von Forschungszwecken nichts.[151] Zwar geht die DSGVO davon aus, dass Forschung mit personenbezogenen Daten grundsätzlich für die Gemeinschaft nützlich ist und deshalb geringeren Beschränkungen unterworfen wird. Das Ergebnis einer Interessenabwägung kann aber dennoch sein, dass wegen der damit verbundenen Eingriffe in die Grundrechte der Betroffenen oder sich ergebender Risiken ein konkretes Projekt nicht zugelassen werden kann (s.u. Kap. 12.8).

4.3 Nationales Datenschutzrecht

Mit Wirkung zum 25.05.2018 wurde das allgemeine Datenschutzrecht in Deutschland novelliert und das bisherige **Bundesdatenschutzgesetz** (BDSG) durch eine völlig neue Regelung ersetzt.[152] Die wesentlichen Regelungen in den Sozialgesetzbüchern (SGB), also insbesondere § 35 SGB I und die §§ 67ff. SGB X, wurden ebenso angepasst.[153] Weitere umfangreiche Anpassungen des nationalen Datenschutzrechts erfolgten im

146 Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 7. Aufl. 2020, Rn. 506f.
147 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 422.
148 Weichert in DKWW, Einl. Rn. 11f.
149 EuGH 14.05.2014 – C-131/12, Rn. 81f.; EDPS, 18.
150 Petri in SHS, Art. 9 Rn. 57f.
151 Golla in Specht/Mantz, § 23 Rn. 39; relativierend Golla/von Schönfeld, K&R 2019, 19.
152 Art. 1 des Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) v. 30.06.2017, BGBl. I S. 2097.
153 Art. 19, 24 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften v. 17.07.2017, BGBl. I S. 2541; dazu Roßnagel/Geminn in Dierke/Roßnagel, 141.

Herbst 2019.[154] Mit den nationalen Überarbeitungen wurden insbesondere gemäß den Öffnungsklauseln in der DSGVO konkretisierende Regelungen erlassen. Dabei hat der Gesetzgeber das innovative Potenzial der DSGVO nicht ausgeschöpft, sondern seine Kompetenzen weitgehend dafür genutzt, bisherige Regelungen beizubehalten, ja sogar die Möglichkeiten zur Verarbeitung zu erweitern sowie Betroffenenrechte zu beschränken.[155]

Während der Bundesgesetzgeber die Umsetzungsregelungen zur DSGVO relativ frühzeitig verabschiedete, schafften die meisten **Bundesländer** diese Anpassung in Bezug auf das allgemeine Datenschutzrecht erst kurz vor oder nach dem 25.05.2018. Einige Anpassungen wurden bis heute nicht in Angriff genommen, so etwa das allgemeine Datenschutzgesetz von Sachsen-Anhalt oder Regelungen in den Landeskrankenhausgesetzen[156]. Auch hier beschränkten sich die Parlamente zumeist auf eine formelle Anpassung, ohne die inhaltlichen europäischen Neuorientierungen zu übernehmen. Dies gilt insbesondere auch für die Forschungsklauseln in den Landesdatenschutzgesetzen.

Wegen der eher konservativen deutschen Umsetzung der DSGVO erfolgten nur **wenige strukturelle Änderungen** gegenüber dem zuvor geltenden Recht, was eine Fortsetzung bisheriger Verarbeitungspraktiken erleichtert. Dies gilt auch für die Verarbeitung für Forschungszwecke, für die in der DSGVO weitestgehend Öffnungsklauseln zur Anwendung kommen.[157] Zugleich wird mit diesem Vorgehen der Ansatz der DSGVO, eine möglichst umfassende Modernisierung und Anpassung an neue technische, ökonomische und soziale Entwicklungen und eine Harmonisierung vorzunehmen, konterkariert.

Von der Änderung des Datenschutzrechts weitgehend unabhängig erfolgte 2017 mit dem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung an der Berufsausübung schweigepflichtiger Personen eine **Überarbeitung des § 203 StGB**, mit dem die Möglichkeiten für Schweigepflichtige erweitert wurden, *„sich im Rahmen ihrer beruflichen und dienstlichen Tätigkeiten ohne (straf-)rechtliches Risiko der Mitwirkung dritter Personen zu bedienen.“* (s.u. Kap. 6.6)[158]

4.4 Forschungsregelungen in der DSGVO

Die DSGVO verfolgt gegenüber dem bisher geltenden europäischen wie nationalen Recht einen völlig neuen Ansatz, indem sie für die Forschung weitgehende Ausnahmeregelungen enthält mit einer **Privilegierung** des Verfolgens von Forschungszwecken gegenüber sonstigen Verarbeitungszwecken. Dies gilt generell gemäß Art. 89 Abs. 2 und speziell für die zweckändernde Datennutzung (Art. 5 Abs. 1 lit. b), die Begrenzung der Speicherdauer (Art. 5 Abs. 1 lit. e), die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 lit. j), die Benachrich-

154 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) v. 20.11.2019, BGBl. I S. 1626, zuvor BT-Drs. 19/4674.

155 Roßnagel/Geminn in Dierks/Roßnagel, 141; Roßnagel, DuD 2017, 277.

156 Dierks 2019, 37ff.

157 Art. 6 Abs. 2, 9 Abs. 2 lit. j, 85 Abs. 1, 89 DSGVO.

158 G. v. 30.10.2017, BGBl. I S. 3618; BT-Drs. 18/11936, 17.

tigungspflicht der Betroffenen, wenn personenbezogene Daten nicht bei ihnen erhoben werden (Art. 14 Abs. 5 lit. b), die Löschungspflicht bzw. das Recht auf Vergessenwerden (Art. 17 Abs. 3 lit. d) sowie das Widerspruchsrecht (Art. 21 Abs. 6).[159]

Es ist umstritten, ob sich der Verantwortliche für die Forschungsnutzung auf die **Rechtsgrundlage des Primärzwecks** berufen kann.[160] Teilweise wird die Ansicht vertreten, dass die in Art. 5 Abs. 1 lit. b DSGVO enthaltene Formulierung, dass eine Weiterverarbeitung für wissenschaftliche Forschungszwecke nicht unvereinbar mit dem ursprünglichen Zweck sei, bedeutet, dass die forschende Verarbeitung sich auf die Grundlage der Erstverarbeitung stützen könne.[161] Diese Ansicht stützt sich auf ErwGr 50 S. 2, wo es in Bezug auf die Regelung zur Zweckänderung in Art. 6 Abs. 4 DSGVO heißt:

> *„In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten."*

Erwägungsgründen kommt keine verbindliche normative Kraft zu.[162] Die Formulierung von ErwGr 50 S. 2 wird aus der Entstehungsgeschichte erklärt, wonach in der Auseinandersetzung über die Reichweite der Zweckbindung dieser Satz stehengeblieben ist, während normativ die Zweckbindung in Art. 6 Abs. 4 DSGVO eingeschränkt wurde.[163] Der Europäische Datenschutzausschuss (EDSA) beruft sich zwar auf den ErwGr. 50 S. 2 und akzeptiert, dass es keiner neuen Rechtsgrundlage für eine Sekundärnutzung bedarf.[164] Er sieht aber das Risiko, dass über eine Sekundärnutzung schutzwürdige Betroffeneninteressen verletzt sein können, und meint, dass dies *„künftig besondere Aufmerksamkeit und Anleitung seitens des EDSA"* erfordert.[165] Der Europäische Datenschutzbeauftragte bestätigt, dass der Erwägungsgrund nicht dazu führen kann, dass der Vereinbarkeitstest von Art. 6 Abs. 4 DSGVO unterlassen wird.[166]

Die DSGVO enthält keine Freistellungen von der Zweckbindung, sondern lediglich eine Flexibilisierung. Dies gilt für Art. 6 Abs. 4 DSGVO. Entsprechendes gilt für Art. 5 Abs. 1 lit. b DSGVO für die Weiterverarbeitung für Forschungszwecke. Das sich an Art. 8 GRCh ausrichtende Konzept der DSGVO basiert darauf, dass **zweckbezogene Rechtsgrundlagen** gefordert werden und zweckändernde Verarbeitungen einer spezifischen Rechtsgrundlage bedürfen. Dies gilt erst recht für die Forschungsprivi-

159 Dierks 2020, 7ff.; Schäfer in Kipker/Voskamp, 334f.; Geminn DuD 2018, 641f.; zumindest missverständlich ist die Formulierung von Golla in Specht/Mantz, § 23 Rn. 4, wonach die DSGVO „keine umfassende Privilegierung wissenschaftlicher Zwecke" enthält.

160 BT-Drs. 18/11325, 99; Richter, DuD 2015, 735; ders., DuD 2016, 584f.; Graf von Kielmansegg in TMF, 102; Golla in Specht/Mantz, § 23 Rn. 56; Herbst in Auernhammer, § 27 Rn. 15; Wolff in Schantz/Wolff, Rn. 411, 413; ErwGr 50, 2 u. 5 sagen nichts anderes aus; zweifelnd dazu Hornung/Hofmann, ZD-Beilage 4/2017, 7f.; neutrale Darstellung bei BKL-R, 234ff.; richtig Kühling/Buchner-Herbst, Art. 5 Rn. 54; Graf von Kielmansegg in TMF, 102.

161 So Schulz in Gola, Art. 6 Rn. 185ff.; Frenzel in Paal/Pauly, Art. 5 Rn. 31; Roßnagel/Geminn in Dierks/Roßnagel.

162 Selmayr/Ehmann in Ehmann/Selmayr, Einführung Rn. 97; Hornung/Spiecker in SHS, Einl Rn. 270; Weichert in DWWS, Einl DSGVO Rn. 39.

163 Herbst in Kühling/Buchner Art. 5 Rn. 49; Schantz, NJW 2016, 1844; a.A. Monreal ZD 2016, 510.

164 Zum Nutzen der Sekundärnutzung von Patientendaten Zenker/Krawczak/Semler in TMF, 9.

165 EDSA, 9 (Rn. 31), vgl. auch EDPS, 7f.

166 EDPS, 23.

legierung, auf die sich der Erwägungsgrund zu Art. 6 Abs. 4 nicht explizit bezieht.[167] Art. 5 Abs. 1 lit. b DSGVO schließt nur die Unvereinbarkeit der Zwecke aus und begründet nicht eine Vereinbarkeit in jedem Fall. Als Rechtsgrundlage sind also die spezifischen Regelungen heranzuziehen, soweit Öffnungsklauseln bestehen. Anderenfalls ist direkt auf Art. 6 und Art. 9 DSGVO zurückzugreifen. Bei Anwendung der spezifischen Regelungen sind die Wertungen der Art. 6 (und evtl. Art. 9) sowie die Privilegierung in Art. 5 Abs. 1 lit. b DSGVO als höherrangiges Rahmenrecht zu beachten.[168]

Eine andere Sicht würde im Ergebnis dazu führen, dass für Forschungszwecke in jedem Fall auf die ursprüngliche Rechtsgrundlage zurückgegriffen werden könnte und innerhalb von Forschungsnutzungen eine **Zweckbindung ausgehebelt** würde.[169] Unklar wäre, in welchem Verhältnis die Rechtsgrundlage der primären Verarbeitung zu spezifizierenden Forschungsklauseln stünde. Würden Daten von einem Verantwortlichen zusammengeführt, die aus unterschiedlichen Quellen mit unterschiedlicher Rechtsgrundlage stammen, wäre unklar, welcher Rechtsgrund anwendbar sein soll. Eine einwilligungsbasierte Forschungsnutzung würde z.B. grundsätzlich die Datennutzung für beliebige sonstige Forschungszwecke eröffnen. Tatsächlich gilt der Zweckbindungsgrundsatz auch innerhalb der Forschung (s.u. Kap. 7). Die Verarbeitungserlaubnis setzt in jedem Fall das Bestehen von angemessenen Garantien voraus (vgl. Art. 89).

Wird dies anerkannt, so reduziert sich die Frage nach der Rechtsgrundlage darauf, welche Norm als Rechtsgrundlage benannt wird. Im Interesse der Betroffenentransparenz wie auch der Rechtsklarheit für alle anderen Beteiligten sollte dies jeweils die anwendbare **spezifische die Forschungsverarbeitung regelnde Norm** sein. Zu diesem Ergebnis kommt man auch, wenn auf die Rechtsgrundlage des Primärzwecks zurückgegriffen werden kann.

In Art. 85 DSGVO, der die „Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit" regelt, werden die Mitgliedstaaten zum Erlass von Rechtsvorschriften verpflichtet, wobei die Verarbeitung „von wissenschaftlichen, künstlerischen oder literarischen Zwecken" eingeschlossen wird. In Art. 89 DSGVO werden Vorgaben gemacht für die

> *„Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, **zu wissenschaftlichen oder historischen Forschungszwecken** und zu statistischen Zwecken".*

Während die DSGVO fast durchgängig den Begriff „wissenschaftliche (und historische) Forschungszwecke" verwendet, wenn es um eine spezifische Forschungsprivilegierung geht (Art. 5 Abs. 1 lit. b, e, 9 Abs. 2 lit. j, 14 Abs. 5 lit. b, 17 Abs. 3 lit. c, 21 Abs. 6, 89 Abs. 2), wird in Art. 85 DSGVO nur der Begriff der „**wissenschaftlichen Zwecke**" verwendet, der auch in Art. 6 Abs. 1 lit. b EG-DSRl Verwendung fand. Art. 85 DSGVO enthält eine Öffnungsklausel, mit welcher der Datenschutz mit der Meinungsfreiheit und der Informationsfreiheit „in Einklang" gebracht werden soll (eben-

167 Herbst in Kühling/Buchner Art. 5 Rn. 49; so im Ergebnis auch Roßnagel in SHS, Art. 6 Abs. 4 Rn. 41.
168 Piper DANA 2019, 72; Wiebe, 542f. m.w.N.
169 So tatsächlich Johannes in Roßnagel 2017, § 4 Rn. 64.

so ErwGr 165 S. 7). In Art. 85 Abs. 2 DSGVO ist bei der Verarbeitung von Personendaten eine Privilegierung im Interesse von Meinungsäußerung und Informationsfreiheit vorgesehen. Diese unterscheidet sich von den expliziten Forschungsprivilegierungen der DSGVO – zumindest teilweise – sowohl im Inhalt wie im Zweck: Gemeinsames Ziel ist der aufgeklärte demokratische Diskurs. Bei den Forschungsprivilegierungen in der DSGVO geht es um die Suche nach objektivierbarer Wahrheit. Vom Schutz der Meinungsäußerung werden auch stark subjektive Wertungen erfasst. Bei der Forschung werden teilweise quantitativ und qualitativ massive Eingriffe in die informationelle Selbstbestimmung vieler Betroffener erlaubt, was mit einer strengen Zweckbindung, einer Pflicht zur Anonymisierung und weiteren Garantien eingefangen werden soll.[170] Im Interesse der **objektivierbaren Wahrheit** werden bei der Forschung hohe Anforderungen an Methodik und Transparenz (Art. 89 Abs. 2 DSGVO) gestellt. Demgegenüber treffen Eingriffe nach Art. 85 DSGVO zumeist Einzelpersonen in bestimmten Zusammenhängen. Zugleich gibt es keine einschränkenden Vorgaben für die Verarbeitung.

Art. 85 und 89 DSGVO verfolgen selbst im wissenschaftlichen Bereich teilweise unterschiedliche Zielrichtungen. Art. 85 DSGVO ist insofern weiter und erfasst zweifellos auch die **nicht privilegierte Forschungstätigkeit**, also Aktivitäten, die z.B. wegen ihrer Anwendungsorientierung, wegen fehlender Transparenz oder einer übermäßig spekulativen Methodik nicht nach den spezifischen Regelungen der DSGVO privilegiert sind. Während Art. 89 DSGVO seinen Schwerpunkt in der Forschungsfreiheit generell hat, liegt der Schwerpunkt von Art. 85 DSGVO auf dem kommunikativen Aspekt der Wissenschaft.[171] Dieser betrifft nicht nur die Kommunikation über die Art der Forschung und deren Ergebnisse, sondern auch den Zugang zu Forschungsgrundlagen (Datenerhebung, Informationsfreiheit)[172], wovon Art. 89 nur einen Teilbereich abdeckt. Hierfür schien der Begriff „wissenschaftliche Zwecke" zu weit und wurde ersetzt durch den der „wissenschaftlichen Forschungszwecke".[173] Die weiteren Privilegierungen des Art. 85 DSGVO dürfen nicht dazu verwendet werden, die höheren Anforderungen des Art. 89 DSGVO zu umgehen.[174]

4.5 Deutsche Forschungsregelungen

Das **Bundesdatenschutzgesetz** enthält nun in § 27 eine Regelung zur „Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken", mit der die Öffnungsklauseln der DSGVO umgesetzt werden sollen. Eine Konkretisierung der generellen Zweckänderungsbefugnis nach Art. 5 Abs. 1 lit. b DSGVO erfolgt dabei nicht, sondern nur eine in Bezug auf sensitive Daten (Abs. 1, 3). Abs. 2 enthält Ausnahmeregelungen zu den Betroffenenrechten:

170 Caspar in SHS, Art. 89 Rn. 2.
171 EDPS, 10f.; Golla in Specht/Mantz, § 23 Rn. 6; Hornung/Hofmann, ZD-Beilage 4/2017, 12; SHS-Dix, Art. 85 Rn. 19.
172 Buchner/Tinnefeld in Kühling/Buchner, Art. 85 Rn. 21.
173 Albrecht/Jotzo, Teil 3 Rn. 71; zu den ausdifferenzierten Begriffen im Detail Roßnagel/Geminn in Dierks/Roßnagel, 210ff.
174 EDPS, 11.

„(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke 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 überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.“

Bei der Überarbeitung der Forschungsklauseln in den **Landesdatenschutzgesetzen** verfolgten die Länder keine gemeinsame Linie. Die Anpassungen an die DSGVO beschränken sich bisher weitgehend auf die Terminologie. Wurde auf die in der DSGVO vorgesehenen Privilegierungen Bezug genommen, so zumeist zur Einschränkung der Betroffenenrechte. Die Regelungen der Bundesländer zur Sekundärnutzung von Daten für Forschungszwecke schreiben weitgehend das bisher geltende Recht fort: § 13 LDSG BW, Art. 25 BayDSG, §§ 17, 35 BlnDSG, § 25 BbgDSG, § 13 BremDSGVOAG, §§ 24, 45 HDSIG, § 9 DSG MV, § 13 NDSG, § 17 DSG NRW, §§ 22, 31 LDSG RP, § 23 SDSG, § 12 SächsDSG, § 27 DSG LSA, §§ 13, 26 LDSG SH, § 28 ThürDSG.[175]

Für **Sozialleistungsträger** (§ 12 SGB I i.V.m. §§ 18–29 SGB I) gilt bzgl. der Datenverarbeitung für Forschungszwecke nicht § 27 BDSG, sondern gelten allgemein die Regelungen des § 75 SGB X, soweit es um die Übermittlung an Dritte geht, sowie die §§ 67b, 67c SGB X in Bezug auf Eigenforschung.[176]

175 Bernhardt/Ruhmann/Weichert mit einer Dokumentation sowie einer vergleichenden Bewertung; BKL-R, 211ff.; Graf von Kielmansegg in TMF, 103f.

176 Angepasst an die DSGVO mit G. v. 17.07.2017, BGBl. I S. 2541; ausführlich dazu Schäfer in Kipker/Voskamp, 314ff.

§ 75 SGB X zur **Übermittlung für Forschungszwecke** hat folgenden Wortlaut:

„(1) Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist für ein bestimmtes Vorhaben

1. der wissenschaftlichen Forschung im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder

2. der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben

und schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse der betroffenen Person erheblich überwiegt. Eine Übermittlung ohne Einwilligung der betroffenen Person ist nicht zulässig, soweit es zumutbar ist, ihre Einwilligung einzuholen. Angaben über den Namen und Vornamen, die Anschrift, die Telefonnummer sowie die für die Einleitung eines Vorhabens nach Satz 1 zwingend erforderlichen Strukturmerkmale der betroffenen Person können für Befragungen auch ohne Einwilligungen übermittelt werden. Der nach Absatz 4 Satz 1 zuständigen Behörde ist ein Datenschutzkonzept vorzulegen.

(2) Ergibt sich aus dem Vorhaben nach Absatz 1 Satz 1 eine Forschungsfrage, die in einem inhaltlichen Zusammenhang mit diesem steht, können hierzu auf Antrag die Frist nach Absatz 4 Satz 5 Nummer 4 zur Verarbeitung der erforderlichen Sozialdaten verlängert oder eine neue Frist festgelegt und weitere erforderliche Sozialdaten übermittelt werden.

(3) Soweit nach Absatz 1 oder 2 besondere Kategorien von Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 an einen Dritten übermittelt oder nach Absatz 4a von einem Dritten verarbeitet werden, sieht dieser bei der Verarbeitung angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor. Ergänzend zu den dort genannten Maßnahmen sind die besonderen Kategorien von Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist.

(4) Die Übermittlung nach Absatz 1 und die weitere Verarbeitung sowie die Übermittlung nach Absatz 2 bedürfen der vorherigen Genehmigung durch die oberste Bundes- oder Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist. Die oberste Bundesbehörde kann das Genehmigungsverfahren bei Anträgen von Versicherungsträgern nach § 1 Absatz 1 Satz 1 des Vierten Buches oder von deren Verbänden auf das Bundesversicherungsamt übertragen. Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle und eine weitere Verarbeitung durch diese nach Absatz 2 darf nur genehmigt werden, wenn sich die nicht-öffentliche Stelle gegenüber der Genehmigungsbehörde verpflichtet hat, die Daten nur für den vorgesehenen Zweck zu verarbeiten. Die Genehmigung darf im Hinblick auf die Wahrung des Sozialgeheimnisses nur versagt werden, wenn die Voraussetzungen des Absatzes 1, 2 oder 4a nicht vorliegen. Sie muss

1. den Dritten, an den die Daten übermittelt werden,

2. die Art der zu übermittelnden Sozialdaten und den Kreis der betroffenen Personen,

3. die wissenschaftliche Forschung oder die Planung, zu der die übermittelten Sozialdaten verarbeitet werden dürfen, und

4. den Tag, bis zu dem die übermittelten Sozialdaten verarbeitet werden dürfen,

genau bezeichnen und steht auch ohne besonderen Hinweis unter dem Vorbehalt der nachträglichen Aufnahme, Änderung oder Ergänzung einer Auflage. Nach Ablauf der Frist nach Satz 5 Nummer 4 können die verarbeiteten Daten bis zu zehn Jahre lang gespeichert werden, um eine Nachprüfung der Forschungsergebnisse auf der Grundlage der ursprünglichen Datenbasis sowie eine Verarbeitung für weitere Forschungsvorhaben nach Absatz 2 zu ermöglichen.

(4a) Ergänzend zur Übermittlung von Sozialdaten zu einem bestimmten Forschungsvorhaben nach Absatz 1 Satz 1 kann die Verarbeitung dieser Sozialdaten auch für noch nicht bestimmte, aber inhaltlich zusammenhängende Forschungsvorhaben des gleichen Forschungsbereiches beantragt werden. Die Genehmigung ist unter den Voraussetzungen des Absatzes 4 zu erteilen, wenn sich der Datenempfänger gegenüber der genehmigenden Stelle verpflichtet, auch bei künftigen Forschungsvorhaben im Forschungsbereich die Genehmigungsvoraussetzungen einzuhalten. Die nach Absatz 4 Satz 1 zuständige Behörde kann vom Antragsteller die Vorlage einer unabhängigen Begutachtung des Datenschutzkonzeptes verlangen. Der Antragsteller ist verpflichtet, der nach Absatz 4 Satz 1 zuständigen Behörde jedes innerhalb des genehmigten Forschungsbereiches vorgesehene Forschungsvorhaben vor dessen Beginn anzuzeigen und dabei die Erfüllung der Genehmigungsvoraussetzungen darzulegen. Mit dem Forschungsvorhaben darf acht Wochen nach Eingang der Anzeige bei der Genehmigungsbehörde begonnen werden, sofern nicht die Genehmigungsbehörde vor Ablauf der Frist mitteilt, dass für das angezeigte Vorhaben ein gesondertes Genehmigungsverfahren erforderlich ist.

(5) Wird die Verarbeitung von Sozialdaten nicht-öffentlichen Stellen genehmigt, hat die genehmigende Stelle durch Auflagen sicherzustellen, dass die der Genehmigung durch Absatz 1, 2 und 4a gesetzten Grenzen beachtet werden.

(6) Ist der Dritte, an den Sozialdaten übermittelt werden, eine nicht-öffentliche Stelle, unterliegt dieser der Aufsicht der gemäß § 40 Absatz 1 des Bundesdatenschutzgesetzes zuständigen Behörde.“

Die Zweckänderung für **eigene Forschungszwecke für Sozialleistungsträger** ist in § 67c Abs. 2 Nr. 2 SGB X geregelt (s.u. Kap. 8.4). Die einwilligungsbasierte Datenverarbeitung findet in § 67b SGB X eine allgemeine Regelung (s.u. Kap. 7.4). Die Weiterverarbeitung von Sozialdaten, die für Forschungszwecke gespeichert sind, ist in § 67c Abs. 5 SGB X geregelt (s.u. Kap. 8.4).

Neben den allgemeinen Forschungsregelungen im SGB X bestehen in den **speziellen Sozialgesetzbüchern** spezifische Regelungen. Die gilt für die gesetzliche Krankenversicherung mit einigen Grundregeln in §§ 287, 303a–303f, 363 SGB V sowie einer Vielzahl von weiteren Vorgaben im SGB V (z.B. §§ 25 Abs. 5, 63 Abs. 1 S. 1 Nr. 8, 68a Abs. 3 Nr. 3, 137a, 117 Abs. 1 u. 2, 287a, 327 Abs. 1 Nr. 1). Weitere Forschungsregelungen finden sich z.B. zu Daten aus der gesetzlichen Unfallversicherung (§ 9 Abs. 8 SGB VII)[177], zur Arbeitsmarkt- und Berufsforschung sowie zur Wirkungsforschung in der Grundsicherung (§§ 280–282 SGB III, § 55 SGB II)[178] oder zu Daten aus der Pflegeversicherung (§ 98 SGB XI).

Soweit **bereichsspezifische Forschungsregelungen** im Bundes- und Landesrecht bestehen, gehen diese gemäß § 1 Abs. 2 BDSG[179] bzw. generell gemäß dem Vorrang der

177 Schäfer in Kipker/Voskamp, 385ff.
178 Schäfer in Kipker/Voskamp, 402ff.
179 Für das Sozialrecht § 35 Abs. 2a SGB I.

spezielleren Regelung den allgemeinen Forschungsklauseln vor. Solche Normen finden sich in vielen Bereichen des Sozialrechts (§ 287 SGB V, § 98 SGB XI, § 119 SGB XII), im Strafprozessrecht (§ 476 StPO), in § 42a BZRG, im Strafvollzugsrecht (§ 186 StVollzG). Für die Ärzteschaft gelten die Berufsordnungen der Landesärztekammern, die sich weitgehend an § 15 MBOÄ orientieren bzw. damit identisch sind.[180] Im Medizinbereich gibt es Regeln in § 40 Abs. 2a AMG[181] und § 14 Abs. 2a, 15g TPG[182], in § 170 Abs. 7 StrlSchG, in den Psychisch-Kranken-,[183] den Krankenhaus-[184] und den Krebsregistergesetzen[185], nicht aber z.B. im Gendiagnostikrecht (§ 2 Abs. 2 Nr. 1 GenDG).[186]

Nicht eindeutig ist, wie sich die Forschungsregelungen in Bund und Ländern auf die Öffnungsklauseln der DSGVO beziehen. Teilweise beschränkt sich die Anwendung der dortigen **materiell-rechtlichen Regelungen** auf sensitive Daten nach Art. 9 Abs. 1 DSGVO, so etwa in § 27 Abs. 1 BDSG.[187] Dem liegt die Erwägung zugrunde, dass die Art. 5, 6 DSGVO in Bezug auf nicht-sensitive Daten abschließend sind.[188] Die meisten Landesgesetzgeber regelten dagegen generell die Verarbeitung von Daten für Forschungszwecke *„einschließlich solcher nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/619"*.[189] Für die Regulierung der Verarbeitung von nicht-sensitiven Daten können die Öffnungsklauseln in Art. 6 Abs. 2, 85 Abs. 1 und 89 DSGVO geltend gemacht werden (s.o. Kap. 4.1).

Es bleibt aber fraglich, inwieweit die darin enthaltenen Regelungen mit den materiell-rechtlichen Vorgaben in den Art. 5 Abs. 1 lit. b, 6 Abs. 4 DSGVO zur **Zweckprivilegierung** bzw. Zweckvereinbarkeit in Einklang zu bringen sind.[190] Einige Gesetze sehen eine Festlegung auf ein „bestimmtes Forschungsvorhaben" vor.[191] Verbundprojekte sind mit dieser Formulierung nur schwerlich in Einklang zu bringen, ebenso Projekte, in denen die wissenschaftlichen Fragestellungen zu Forschungsbeginn noch nicht endgültig feststehen und die zeitlich nicht begrenzt sind (z.B. Register). In einigen Gesetzen wird die Zweckänderung im Rahmen einer Sekundärnutzung davon abhängig gemacht, dass die Verarbeitungszwecke gegenüber den Betroffeneninteressen „überwiegen",[192] zumeist ist aber nötig, dass diese „erheblich überwiegen".[193]

180 Schneider, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, Schriftenreihe der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) 2015, 295ff.
181 Schneider 2015, 64ff.
182 Schneider 2015, 61.
183 Schneider 2015, 72.
184 Übersicht bei Dierks 2019, 37ff.; vgl. Schneider 2015, 244f.
185 Gode/Niemeck in Kipker/Voskamp, 539f.; Sachverständigenrat, 206.
186 Schneider 2015, 55.
187 Ebenso § 24 Abs. 1 S. 1 HDSIG, § 22 Abs. 1 LDSG RP.
188 Bernhardt/Ruhmann/Weichert, 5.
189 § 17 Abs. 1 BlnDSG, § 25 Abs. 1 S. 1 BbgDSG, § 11 Abs. 1 HmbDSG, § 9 DSG Abs. 1 S. 1 M-V, § 13 Abs. 1 S. 1 NDSG, § 17 Abs. 1 DSG NRW, § 22 Abs. 1 S. 1 DSG Saar, § 12 Abs. 1 SächsDSDG, § 13 Abs. 1, S. 1 LDSG SH, § 28 ThürDSG, wohl auch Art. 25 BayDSG.
190 Bernhardt/Ruhmann/Weichert, 5f.
191 § 25 Abs. 1 BbgDSG, § 11 Abs. 1 HmbDSG, § 9 Abs. 1 S. 1 DSG M-V, § 13 Abs. 1 NDSG, § 23 Abs. 1 S. 1 DSG Saar, unklar § 22 Abs. 1 LDSG RP.
192 § 13 Abs. 1 S. 1 LDSG BW, § 25 Abs. 1 S. 1 BbgDSG, § 24 Abs. 1 S. 1 HDSIG, § 13 Abs. 1 S. 1 NDSG, § 17 Abs. 1 DSG NRW, § 12 Abs. 1 SächsDSDG.
193 § 27 Abs. 1 S. 1 BDSG, § 9 Abs. 1 S. 1 DSG M-V, § 22 Abs. 1 LDSG RP, § 23 Abs. 1 S. 1 DSG Saar, keine Regelung BayDSG, ThürDSG; zur Auslegung BKL-R, 207f.

Unstreitig ist, dass sich das Recht der Mitgliedstaaten in dem von der DSGVO vorgezeichneten Rahmen halten muss. Solange keine höchstrichterliche Klärung über die Rechtsgrundlagen für Forschungszwecke vorliegt, ist es geboten, jeweils die **spezifischste Norm** heranzuziehen, auch wenn es sich hierbei um eine Regelung des deutschen Bundes- oder des Landesrechts handelt. Diese muss dann aber in jedem Fall im Lichte der Vorgaben der DSGVO ausgelegt werden und im Zweifel bei einem Verstoß hiergegen unangewendet bleiben (s.u. Kap. 8.4).[194]

Liegt eine wirksame Einwilligung vor, so kann hierauf Bezug genommen werden (s.u.). Fehlt es hieran, so ist auf eine gesetzliche Grundlage zurückzugreifen. Dabei muss in jedem Fall eine **Abwägung** vorgenommen werden zwischen den Schutzinteressen der Betroffenen und den Interessen an dem konkreten Forschungsvorhaben mit den konkreten Daten.[195]

194 Heberlein in Ehmann/Selmayr, Art. 6 Rn. 64, 71; Hornung/Spiecker in SHS, Einl Rn. 265; Ruffert in Callies/Ruffert, Art. 1 AEUV Rn. 24.

195 Zu den unterschiedlichen Abwägungsklauseln, der Offenheit der Abwägung und Abwägungsaspekten Graf von Kielmansegg in TMF, 106ff.

5 Verantwortlichkeiten

Bei der Verantwortlichkeit für die Verarbeitung von personenbezogenen Daten im Rahmen von medizinischen Forschungsvorhaben ist zu **unterscheiden** zwischen der datenschutzrechtlichen und der strafrechtlichen Verantwortlichkeit, die insbesondere in § 203 StGB thematisiert wird.[196] Da die strafrechtliche Regelung in § 203 StGB zugleich im Standes- und Medizinrecht relevant ist und Rückwirkungen auf den Datenschutz hat, wird hierauf im Folgenden ausführlich eingegangen. Weiterhin sind diese beiden Formen der Verantwortlichkeit zu unterscheiden von der zivilrechtlichen Verantwortung, also insbesondere für Ansprüche aus Vertrag, auch Behandlungsvertrag (§§ 630a ff. BGB), sowie für Schadenersatzansprüche (§§ 823 ff. BGB sowie Art. 82 DSGVO).[197]

5.1 Verantwortlichkeit

Wer Verantwortlicher i.S.d. DSGVO ist, wird in Art. 4 Nr. 7 definiert. Danach ist

> *„Verantwortlicher" die 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; sind die Zwecke und Mittel dieser Verarbeitung*

196 Auf die Verknüpfung der datenschutzrechtlichen mit der strafrechtlichen Verantwortlichkeit in § 42 BDSG wird hier nicht näher eingegangen.

197 Auf die datenschutzrechtlich begründeten Schadenersatzansprüche nach Art. 82 DSGVO wird hier nur am Rande eingegangen.

durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden."

Im Datenschutzrecht erfolgt eine **juristische Betrachtungsweise** bei der Auslegung des Begriffs.[198] Eine Sonderregelung enthält lediglich § 67 Abs. 4 S. 2 SGB X für den Bereich des Sozialdatenschutzes: Handelt es sich bei einem Sozialleistungsträger um eine Gebietskörperschaft, sind verantwortliche Stelle die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile des SGB **funktional** erfüllen.[199]

Die Mitgliedstaaten haben im Rahmen der Vorgaben der DSGVO die Möglichkeit, die Verantwortlichkeit im **nationalen Recht** zu präzisieren.[200] Solche allgemeinen Regelungen bestehen im deutschen Recht in Bezug auf die Forschung und die medizinische Datenverarbeitung nicht.

Sowohl natürliche wie auch juristische Personen, Behörden oder Einrichtungen können Verantwortliche sein (Art. 4 Nr. 7 DSGVO). Es sind letztlich immer **natürliche Personen**, auf die eine Datenverarbeitung zurückgeht. Diese können dann als Verantwortliche dem Anwendungsbereich der DSGVO unterfallen, wenn sie im Rahmen einer beruflichen oder wirtschaftlichen Tätigkeit personenbezogene Daten verarbeiten.[201] Nutzt eine natürliche Person, die für eine juristische Person handelt, Daten für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle der juristischen Person, so ist die natürliche Person der für die Verarbeitung Verantwortliche, da sie hierüber eigenständig und unabhängig entschieden hat. Der ursprüngliche für die Verarbeitung Verantwortliche kann jedoch auch eine (gemeinsame) Verantwortung tragen, etwa wenn die neue Verarbeitung aufgrund eines Mangels an angemessenen Sicherheitsmaßnahmen erfolgt.[202]

Handelt ein **Mitarbeiter** im Auftrag und im Namen einer Stelle (seines Arbeitgebers), so ist diese Stelle datenschutzrechtlich verantwortlich. Überschreitet der Mitarbeiter seine stelleninternen Kompetenzen, so ist er selbst als Verantwortlicher anzusehen (vgl. Art. 28 Abs. 10 DSGVO).[203] Der Zugehörigkeit zu einer Stelle tut es keinen Abbruch, dass der **Mitarbeiter oder ein Organisationsteil** eine gesetzlich gesicherte Unabhängigkeit genießt oder eigene Verarbeitungsrechte hat bzw. Pflichten unterworfen ist, z.B. als Arzt, Forschungsleiter oder Betriebsarzt. Auf die Belegenheit der Datenverarbeitungsanlage kommt es auch nicht an; so sind z.B. dienstlich genutzte mobile Rechner (Laptop, Notebook) eines Arbeitnehmers dem Arbeitgeber als Verantwortlichem zuzurechnen.[204]

Dies gilt auch für forschende **Professoren**, soweit sie die forschende Datenverarbeitung als Angehörige ihrer Forschungseinrichtung oder Hochschule durchführen.

198 Jung/Hansch ZD 2019, 146; a.A. noch Weichert in Kilian/Heussen, Computerrechts-Handbuch, 1993, 132 Rn. 39ff.
199 Kritisch dazu Dierks in Dierks/Roßnagel, 77ff.
200 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 36.
201 Schwartmann/Mühlenbeck in SJTK, Art. 4 Rn. 108–110; ausgeschlossen ist die Anwendbarkeit bei ausschließlich persönlicher oder familiärer Tätigkeit, Art. 2 Abs. 2 lit. c DSGVO.
202 Artikel 29-Datenschutzgruppe, WP 160 v. 16.02.2010, 20.
203 Jung/Hansch, ZD 2019, 146.
204 LAG Schleswig-Holstein, DuD 2001, 235 = RDV 2001, 107.

Zwar ist für die Feststellung der Verantwortlichkeit die autonome Entscheidungskompetenz von Bedeutung[205], die Professoren auch im Rahmen ihrer „abhängigen Beschäftigung" im Rahmen von Forschungsvorhaben zukommt. Dies ändert aber nichts daran, dass auf sie eine direkte Einflussmöglichkeit auch in diesem Bereich durch die beschäftigende Stelle besteht, wenn sie für diese und nicht für sich tätig sind. Handeln sie als privat Forschende, so sind sie persönlich als Verantwortliche anzusehen. Ausschlaggebend ist, ob sie eigenständig und nicht als Teil der sie beschäftigenden Stelle tätig sind.[206] Relevant ist dabei, wie der Professor gegenüber anderen Stellen und insbesondere gegenüber den Betroffenen auftritt, etwa durch die Verwendung eines persönlichen statt eines dienstlichen Briefkopfs.

Ist ein **Betriebsarzt** (§§ 2–4, 8–10 ASiG) Mitarbeiter des Arbeitgebers (interner Betriebsarzt), so ist er rechtlich Teil des vom Arbeitgeber geführten Betriebs und somit nicht datenschutzrechtlich Verantwortlicher.[207] Verantwortlicher ist der Arbeitgeber. Dieser ist i.d.R. auch im sachenrechtlichen Sinn über die betriebsärztliche Dokumentation verfügungsbefugt. Dass dem Arbeitgeber wegen der ärztlichen Schweigepflicht (§ 8 Abs. 1 S. 3 ASiG) keine Zugriffsrechte auf die Daten zustehen, spielt für die datenschutzrechtliche Bewertung keine Rolle. Der externe Betriebsarzt, egal ob er als Einzelperson handelt oder als betriebsärztlicher Dienst, ist als eigenständige, vom Arbeitgeber rechtlich getrennte Person nicht dem Arbeitgeber zuzuordnen. Der externe Betriebsarzt bzw. der betriebsärztliche Dienst ist also im Sinne des Datenschutzrechts selbst Verantwortlicher. Dies schließt nicht aus, dass er die Räumlichkeiten, Einrichtungen und Geräte des Arbeitgebers in Anspruch nimmt und dass der Arbeitgeber deren Eigentümer ist. Es kommt darauf an, dass der externe Betriebsarzt als natürliche oder juristische Person vertraglich mit dem Arbeitgeber hierüber eine Vereinbarung trifft und so über Mittel und Zwecke der Verarbeitung bestimmt. Möglich ist auch, dass sich die Mittel der ärztlichen Dokumentation im Eigentum des externen Betriebsarztes befinden.[208]

Die Ausführungen zum internen Betriebsarzt sind auf **verbeamtete oder angestellte Ärzte**, die für eine private oder eine öffentliche Stelle tätig sind, übertragbar. Dabei spielt es keine Rolle, ob das Beschäftigungsverhältnis mit einem Krankenhaus[209], einem medizinischen Versorgungszentrum, einer Gemeinschaftspraxis oder in einer ambulanten Arztpraxis besteht. Demgegenüber sind Ärzte in einer Praxisgemeinschaft jeweils selbstständig Verantwortliche, auch wenn sie gemeinsames Praxispersonal beschäftigen.[210]

Im Datenschutzrecht wird unabhängig vom Wissen über die Daten bei der Feststellung der Verantwortlichkeit darauf abgestellt, wer objektiv über die Verarbeitung der Daten bestimmen kann, wer die Entscheidungsgewalt über „Ob" und „Wie" zu **Zweck**

205 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 36.
206 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 12; zur Chefarztabrechnung Kühling/Seidel in Kühling/Kingreen, 89.
207 Weichert RDV 2007, 191; zu undifferenziert Washausen in Kingreen/Kühling, 420.
208 Weichert DANA 2020, 5.
209 Nicht jedoch der Klinik-Konzern, Dochow, 641.
210 Kühling/Seidel in Kühling/Kingreen, 89; zur Unterscheidung Deckenbrock in Prütting, § 705 BGB Rn. 4–19, 27–29.

und Mittel der Datenverarbeitung hat.[211] Dabei kommt es nicht darauf an, ob die Stelle über die Daten tatsächlich Besitz und Herrschaft hat.[212]

Bei vernetzten, mobilen oder sonstigen **komplexen Verarbeitungsverfahren** liegt die Verantwortlichkeit zuweilen bei unterschiedlichen Stellen. Sie kann teilweise auch beim Betroffenen bzw. Nutzenden selbst liegen.[213] Entscheidend ist, wer einen wesentlichen Teil des Datenverarbeitungsprozesses tatsächlich beherrscht.[214] Dabei kann es Schwierigkeiten der Zuordnung geben. Bei einem mobilen Datenträger, der vom Betroffenen mitgeführt wird, liegt die Verantwortlichkeit jeweils bei den Stellen, die die Herrschaft über den jeweiligen Verarbeitungsvorgang ausüben. Dies können der Betroffene, ein Plattformanbieter, ein App-Anbieter sowie der Hardware-Hersteller zugleich sein (s.u. Kap. 5.2).

Befinden sich Daten in **Verbunddateien** und sind mehrere Stellen selbstständig zur Veränderung der Datensätze berechtigt, liegt die Verantwortlichkeit kumulativ bei sämtlichen derart berechtigten Stellen. Ist z.B. ein Verbundteilnehmer zu einer Löschung oder Berichtigung verpflichtet, müssen die anderen Teilnehmer dies auch gegen sich gelten lassen. Erfolgt ein (automatisierter) Abruf eines Verbundteilnehmers von einem Datum, für das nur eine andere Stelle verantwortlich ist, liegt hierin eine Offenlegung.[215]

Teilweise wurde die Ansicht vertreten, dass bei arbeitsteiliger Datenverarbeitung eine Verantwortung nur bei **Vorliegen eines Vertragsverhältnisses** besteht und wenn die Stelle positive Kenntnis von den Tatsachen hat, welche der (möglicherweise rechtswidrigen) Verarbeitung der beteiligten anderen Stelle zu Grunde liegen.[216] Diese Ansichten haben sich mit der DSGVO und der neuen Rechtsprechung des EuGHs zur gemeinsamen datenschutzrechtlichen Verantwortlichkeit erledigt.[217]

5.2 Gemeinsame Verantwortlichkeit

Die DSGVO enthält in Art. 26 erstmals eine ausführliche Regelung zur **gemeinsamen Verantwortlichkeit.**

> *„(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der*

211 EDPS 2019, 9f.; Weichert DuD 2009, 10; Jotzo MMR 2009, 233.
212 Dammann in Simitis, § 3 Rn. 225; Weichert, ZD 2014, 605; ders., ZD 2014, 1; a.A. OVG Schleswig, ZD 2014, 643 = DuD 2014, 869 = K&R 2014, 831; VG Schleswig, ZD 2014, 51 mit Anm. Karg; offenhaltend noch die Vorlage beim EuGH durch BVerwG 25.2.2016 – 1 C 28.14, K&R 2016, 437; dazu Marosi, K&R 2016, 389; jetzt ständige Rspr. des EuGH, s.u. Kap. 5.2).
213 Von dem Bussche DB 2018, 1782; Goland K&R 2019, 535; Weichert DANA 2019, 6.
214 Art.-29-Datenschutzgruppe, Arbeitsdokument Datenschutz und RFID-Technologie v. 18.01.2005, WP 105; Kesten, RDV 2008, 100.
215 VGH Kassel, CR 1992, 693.
216 Petri ZD 2015, 103.
217 Ausführlich Monreal ZD 2019, 797ff.

Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.“

Der EU-Gesetzgeber wollte mit der neuen Regelung eine klare Zuordnung der Verantwortungsbereiche schaffen und der komplexen Realität von verschachtelten informationstechnischen Vorgängen gerecht werden. Die Verantwortlichen sollen ihre DSGVO-Pflichten klar und transparent verteilen.[218] Die gemeinsame Verantwortlichkeit ist zwar als rechtliche Konstruktion seit langem bekannt (vgl. § 6 Abs. 2 BDSGaF), spielte aber bisher in der Praxis in Deutschland keine wesentliche Rolle. Dies änderte sich mit **Entscheidungen des Europäischen Gerichtshofes** (EuGH) seit Juni 2018, in denen das oberste europäische Gericht klarstellte, dass eine solche Rechtsbeziehung unter Verantwortlichen öfter besteht, als bisher von den Daten verarbeitenden Stellen, der Datenschutzaufsicht und den Gerichten angenommen wurde.[219]

Gemeinsame Verantwortlichkeit ist gegeben, wenn eine Verarbeitung **selbstständige Entscheidungen verschiedener Stellen voraussetzen**, d.h., wenn eine Verarbeitung ohne die aktive Beteiligung jeder Stelle nicht denkbar ist, also ein kumulatives Zusammenwirken erfolgt.[220] Eine zeitgleiche und gemeinsam abgestimmte Entscheidung über Zwecke und Mittel ist nicht nötig.[221] So kann die gemeinsame Verantwortung dadurch entstehen, dass im Voraus von einem Anbieter festlegte Zwecke und Mittel von einem Nutzer akzeptiert werden, indem er diese für sich in Anspruch nimmt.[222] Beteiligt sein können zwei, aber auch viele Stellen. Für die Feststellung der gemeinsamen Verantwortlichkeit kommt es auf die objektiven tatsächlichen Umstände an, ein schriftlicher Vertrag ist nicht begriffsnotwendig.[223]

Wurde eine Vereinbarung nach Art. 26 DSGVO geschlossen, ohne dass hierfür die tatsächlichen Voraussetzungen vorliegen, so besteht keine gemeinsame Verantwortung. Eine **Bezeichnung als „Vereinbarung“** nach Art. 26 ist allenfalls ein Indiz.[224] Die in Art. 26 Abs. 1 S. 2 DSGVO geforderte Vereinbarung ist Rechtsfolge und Rechtmäßig-

218 Specht-Riemenschneider/Schneider MMR 2019, 504; Albrecht/Jotzo, 61.

219 EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = JZ 2018, 1154 = NZA 2018, 919 = ZD 2018, 357 = NVwZ 2018, 1386 = EuZW 2018, 534 = MMR 2018, 591 = BB 2018, 1480 = DuD 2018, 518; zur Prozessgeschichte Weichert DANA 2019, 4ff.; Nebel RDV 2019, 9ff.; EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), NJW 2019, 285 = NZA 2018, 991 = NVwZ 2018, 1787 = EuZW 2018, 897; kritisch dazu Thüsing/Rombey, NZA 2019, 6ff.; EuGH 29.07.2019 – C-40/17 (Fashion ID), zuvor EU-Generalanwalt Bobek, EWS 2019, 55f.

220 Weichert DANA 2019, 5.

221 Doench/Sommerfeld in Kipker/Voskamp, 113 m.w.N., a.A. Kremer CR 2019, 227; Bertermann in Ehmann/Selmayr, Art. 26 Rn. 10.

222 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3.

223 EuGH 10.7.2018 – C-25/17 (Zeugen Jehovas), Rn. 67, NJW 2019, 285 = NZA 2018, 991 = NVwZ 2018, 1787 = EuZW 2018, 897; Martini in Paal/Pauly, Art. 26 Rn. 18.

224 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3.

keitsvoraussetzung, aber nicht begründend für das Vorliegen einer gemeinsamen Verantwortlichkeit.[225]

Für eine gemeinsame Verantwortlichkeit ist es nicht erforderlich, dass jeder der für dieselbe Verarbeitung Verantwortlichen Zugang zu den betreffenden Daten hat.[226] Relevant ist, dass jede Stelle aus Eigeninteresse Einfluss auf die Verarbeitung nimmt und damit an der Festlegung über Zwecke und Mittel dieser Verarbeitung **faktisch mitwirkt**. Dies kann ausdrücklich, aber auch stillschweigend erfolgen.[227] Es ist sogar möglich, dass ein Verantwortlicher gar nicht weiß, mit wem er in gemeinsamer Verantwortung steht.[228] Jeder der Verantwortlichen hat eine rechtliche oder tatsächliche Möglichkeit, Zwecke sowie wesentliche Elemente der Mittel der Verarbeitung zu bestimmen.[229] Es muss keine Gleichrangigkeit der Entscheidungsbefugnis gegeben sein, wohl aber muss eine *„kooperative Determinierung des Zielzustands"* erfolgen.[230] Die Entscheidungen der gemeinsam Verantwortlichen müssen in der Form erfolgen, dass sie sich zum Zeitpunkt der Datenverarbeitung gegenseitig ergänzen, nacheinander erfolgende Entscheidungen in Bezug auf konkrete Verarbeitungsschritte sind nicht gemeinsam.[231] Die Einflussnahme eines Verantwortlichen kann sich auf die Organisation bzw. Koordinierung der Datenverarbeitung beschränken.[232] Selbst ein Abhängigkeitsverhältnis kann die Grundlage für eine gemeinsame Verantwortung sein, wenn in dem organisatorischen Zusammenhang dem untergeordneten Beteiligten eine wesentliche Bestimmungs- und Einflussmöglichkeit über die Verarbeitung verbleibt. Dies kann etwa bei der Tätigkeit eines privat Forschenden (z.B. eines Professors, s.o. Kap. 5.1) und der Einrichtung, bei der dieser beschäftigt ist, gegeben sein. Gleiche Augenhöhe ist nicht nötig.[233]

Eine **Entscheidung** bzgl. der Datenverarbeitung liegt vor, wenn diese ohne den direktiven, bestimmte Modalitäten der Datenverarbeitung regelnden Input einer Stelle potenziell anders ausfallen würde.[234] „Entscheiden" bedeutet, dass eine Frage endgültig geklärt wird.[235] Fehlt es an der Bestimmungsmöglichkeit, so ist i.d.R. eine Auftragsverarbeitung (Art. 28 DSGVO) gegeben. Dass und ob gemeinsam verarbeitete (erhobene) Daten von einer Stelle wieder an einen der Verantwortlichen nach einer Aufbereitung (etwa einer statistischen oder wissenschaftlichen Auswertung) zur alleinigen Nutzung zurückgespielt werden[236], spielt für die Frage der vorangehenden gemeinsamen Verantwortlichkeit keine Rolle.

225 Monreal ZD 2019, 806 Rn. 57; Kremer DB 2019, 1433; Golland K&R 2019, 533, mit weiteren Nachweisen in Fn. 8.
226 EuGH 05.06.2018 – C-210/16 (Facebook Fanpage), Rn. 38.
227 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 68, 80.
228 Monreal 2019, 804 Rn. 42.
229 EDPS 2019, 23.
230 Thüsing/Rombey NZA 2019, 10; Martini in Paal/Pauly, Art. 26 Rn. 21.
231 EDPS (2019), 23; Specht-Riemenschneider/Schneider MMR 2019, 504; Thomale in Auernhammer, Art. 26 Rn. 9; DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3.
232 EuGH 10.7.2018 – C-25/17 Rn. 70; Thüsing/Rombey NZA 2019, 10; Specht-Riemenschneider/Schneider MMR 2019, 504.
233 EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), Rn. 70, 75, NJW 2019, 290; Thüsing/Rombey, NZA 2019, 10; von dem Bussche DB 2018, 1782; Golland ZD 2019, 381; Jung/Hansch ZD 2019, 144.
234 EDPS 2019, 7; Specht-Riemenschneider/Schneider MMR 2019, 504; Ingold in Sydow-DSGVO, Art. 26 Rn. 4.
235 Monreal ZD 2019, 802, Rn. 28.
236 So wie dies bei den Facebook-Fanpages mit Facebook Insights der Fall ist.

Welches **Eigeninteresse** von den Verantwortlichen verfolgt wird, ist unbedeutend. Dieses kann ökonomischer oder altruistischer Art sein, es kann in einem Erkenntnisinteresse liegen oder in Bequemlichkeit bzw. dem Interesse an einer unaufwändigen Abwicklung eines Vorgangs. Einzige faktische Voraussetzung ist, dass sich die verfolgten Zwecke, die sich unterscheiden können, praktisch gegenseitig ergänzen.[237] Die Zwecke müssen nicht übereinstimmen.[238] Die Zwecke müssen auch nicht in einem positiven wirtschaftlichen Bedingungszusammenhang stehen.[239]

Jeder der gemeinsam Verantwortlichen muss für sich die Verarbeitung auf eine **Rechtsgrundlage** stützen können, wobei diese Rechtsgrundlagen nicht zwingend identisch sein müssen.[240] So ist es möglich, dass der eine sich auf eine Einwilligung beruft, der andere auf die Wahrnehmung berechtigter Interessen.

Bei einer Forschungsdatenverarbeitung müssen in jedem Fall bei allen Beteiligten reine Forschungs- und Erkenntnisinteressen im Vordergrund stehen, um **rechtlich privilegiert** sein zu können (Kap. 3.4 u. Kap. 8.1). Dies trifft auch für Treuhänder zu, soweit sie für Forschende tätig sind. Diese Forschungsinteressen der Beteiligten können sich im Rahmen einer gemeinsam verantworteten Datenverarbeitung aber unterscheiden.[241]

Bei der Feststellung der gemeinsamen Verantwortlichkeit muss auf den jeweiligen konkreten Verarbeitungsvorgang Bezug genommen werden. Dies kann zur Folge haben, dass ein technisch einheitlicher Prozess in verschiedene **Prozessschritte** bzw. Verarbeitungsphasen aufzuteilen ist.[242] Art. 4 Nr. 2 DSGVO umschreibt solche verschiedenen Abschnitte einer „Vorgangsreihe". Für die Differenzierung bei der Verantwortlichkeit besonders relevant sind die Schritte „Erhebung", „Speicherung", „Auswertung" und „Übermittlung".[243] Sind einzelne Prozessschritte denklogisch, nicht technisch, miteinander verbunden, so besteht insofern eine einheitliche Verantwortungszuordnung. Die Artikel 29-Datenschutzgruppe führt als Beispiel hierfür klinische Arzneimittelstudien an, in denen das Pharmaunternehmen (der Sponsor) die jeweiligen Studienprotokolle und Weisungen hinsichtlich der Datenverarbeitung vorgibt und evtl. kontrolliert, ohne selbst die Daten zu verarbeiten. Die Verarbeitung kann vollständig bei den Studienzentren liegt, die auch die konkrete Umsetzung der Vorgaben festlegen.[244]

Bei der Differenzierung der Verarbeitungsschritte wird zwischen der **Mikro- und der Makroebene** unterschieden: Bei der Mikroebene wird auf den jeweiligen Verarbeitungsschritt i.S.d. Art. 4 Nr. 2 DSGVO abgestellt, bei der Makroebene auf die Sicht der Betroffenen. Relevant für die Feststellung der gemeinsamen Verantwortung ist die Mikroebene, also die Entscheidung über den tatsächlich erfolgenden Verarbeitungsschritt. Um deshalb keine falsche Wahrnehmung der Betroffenen auszulösen, soll für diese über Art. 26 DSGVO Transparenz und Rechtsschutz gesichert werden.[245]

237 Golland ZD 2019, 382.
238 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 2; a.A. Kremer CR 2019, 227.
239 Hanloser ZD 2019, 123; dagegen richtig Golland K&R 2019, 535.
240 Petri in SHS, Art. 26 Rn. 1; Monreal ZD 2019, 805 Rn. 50.
241 Weichert DANA 2019, 6
242 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 74; DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 2f.; Piltz DB 2019, 239.
243 Golland K&R 2019, 534.
244 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 36f.
245 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 8.

Eine gemeinsame Verantwortlichkeit bedingt **keine gleichwertige Verantwortlichkeit** der Akteure. Diese können in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein, sodass der Grund der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.[246] Spätestens mit Kenntniserlangung über die Datenverarbeitung der anderen gemeinsam Verantwortlichen können alle einem Verantwortlichen zuzurechnenden Pflichten, auch die Umsetzung der Betroffenenrechte, abverlangt werden.[247] Der unterschiedliche Grad der Verantwortlichkeit hat keinen Einfluss auf die materielle Rechtmäßigkeit des jeweiligen Verarbeitungsschritts. Wohl aber können innerhalb der Gemeinschaft der Verantwortlichen durch eine Vereinbarung Aufgaben konzentriert werden, z.B. in Bezug auf die Umsetzung von Betroffenenrechten. Der Grad der Verantwortlichkeit kann daran gemessen werden, wie groß das Interesse an den Daten und der Einfluss auf die Datenverarbeitung ist. Damit wird dem Grundsatz der Verhältnismäßigkeit entsprochen.[248] Dieser Grad, der nicht von den Beteiligten frei bestimmt werden kann, sondern von den objektiven Umständen abhängt, sollte maßgeblich in der Vereinbarung nach Art. 26 DSGVO abgebildet und aus dieser abgeleitet werden können.[249] Er ist z.B. im Rahmen der Bemessung von Bußgeldern nach Art. 83 DSGVO oder bei Maßnahmen der Aufsichtsbehörde nach Art. 58 Abs. 2 DSGVO von Bedeutung.

Für die Frage, welchen der gemeinsamen Verantwortlichen eine **Aufsichtsbehörde** in Anspruch nimmt, kommt es auf den unterschiedlichen Grad der Verantwortung nicht an. Festlegungen in einer Vereinbarung nach Art. 26 DSGVO sind für die Aufsichtsbehörden nicht verbindlich; sie können aber eine Anregung dafür geben, welche Aufsichtsbehörde bei einer Prüfung die Federführung übernimmt. Eine explizite Regelung zur Federführung bei gemeinsamer Verantwortlichkeit enthält die DSGVO nicht. Erfolgt eine gemeinsame Verarbeitung unter der Verantwortlichkeit einer Behörde oder einer privaten Stelle auf der Grundlage von Art. 6 Abs. 1 lit. c oder lit. e DSGVO, so ist die Aufsichtsbehörde in jedem Fall zuständig, ohne dass es insofern eine Federführung gibt (Art. 55 Abs. 2 DSGVO). Die Aufsichtsbehörde kann sich an jeden Verantwortlichen wenden.[250] Eine geforderte Abhilfemaßnahme ist nur dann nicht ermessensfehlerfrei, wenn die konkrete Aufsichtsbehörde durch Inanspruchnahme eines anderen gemeinsam Verantwortlichen effektiver den Anlass des Einschreitens beseitigen könnte.[251]

Von der Verantwortlichkeit nicht mehr mit umfasst werden vor- und nachgelagerte Vorgänge einer **Verarbeitungskette**, für die weder Zwecke noch Mittel gemeinsam festgelegt werden.[252] So besteht z.B. für das Erheben und Übermitteln von Daten über ein Webseiten-Social-Plugin wie den „Gefällt mir"-Button von Facebook eine gemeinsame Verantwortlichkeit von Webseiten- und Plattformbetreiber, nicht mehr aber

246 EuGH 05.06.2018 – C-210/16 (Facebook Fanpage), Rn. 43; Härting/Gössling NJW 2018, 2524f.; Weichert DANA 2019, 5.
247 Weichert ZD 2014, 1; Weichert in Breiter/Wind (Hrsg.), Informationstechnik und ihre Organisationslücken, 2011, 301ff.; Weichert, DANA 2012, 18ff.
248 Petri EuZW 2018, 541; Härting/Gössling NJW 2018, 2524.
249 Schreiber ZD 2019, 58.
250 BVerwG 11.09.2019 – 6 C 15.18 Rn. 25, NJW 2020, 414.
251 BVerwG 11.09.2019 – 6 C 15.18 Rn. 35ff.
252 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 74.

für die weitere Verarbeitung durch den Plattformbetreiber.[253] Übermitteln Krankenkassen Daten an eine wissenschaftliche Stelle, um aus den Ergebnissen Erkenntnisse für sich zu erlangen, so haben die Kassen keinen Einfluss auf die Datenauswertung und tragen deshalb hierfür auch keine Verantwortung.[254] Keine gemeinsame Verantwortlichkeit besteht mit einer Stelle, wenn die Voraussetzungen einer Auftragsverarbeitung gemäß Art. 28 DSGVO vorliegen. Auch eine parallele, technisch nebeneinander erfolgende Datenverarbeitung ist nicht automatisch eine gemeinsame, auch wenn diese in gleichartigen Prozessschritten erfolgt.[255]

Unbedeutend für die Feststellung der gemeinsamen Verantwortlichkeit ist es, in wessen **Eigentum oder Herrschaftssphäre** sich die technischen Anlagen zur Datenverarbeitung befinden.[256]

5.3 Verantwortung bei Forschungsprojekten

Die Entscheidungen des EuGH zur gemeinsamen Verantwortlichkeit hatten eine intensive Fachdebatte zur Folge. Schon aus den ersten drei Urteilen war erkennbar, dass dem bisher selten angewendeten Rechtsinstitut der gemeinsamen Verantwortlichkeit künftig eine hohe praktische Relevanz zukommt. Dies gilt nicht nur für die Arbeitsteilung bei einer Internet-Datenverarbeitung, etwa dem Betreiben von Webseiten oder dem Implementieren von Plug-ins, sondern findet auch Anwendung auf sonstige digitale und analoge **arbeitsteilige Verarbeitungsprozesse**. Es ist naheliegend, dass gerade in der oft komplexen und arbeitsteiligen Datenverarbeitung im Bereich der Medizin gemeinsame Verantwortlichkeiten gegeben sind. So liegt bei der elektronischen Patientenakte, bei der ein Krankenversicherer, ein Dienstleister, medizinische Leistungserbringer und evtl. der Betroffene selbst über Zweck und Mittel der Verarbeitung bestimmen, zumindest für einzelne Verarbeitungsschritte gemeinsame Verantwortlichkeiten vor.[257]

Gemeinsame Verantwortlichkeit im Bereich der nach der DSGVO privilegierten Forschung setzt voraus, dass sämtliche Verantwortlichen die **Anforderungen an unabhängige Forschung** erfüllen (s.o. Kap. 3.3).[258] Nicht nötig ist, dass alle Verantwortlichen den gleichen spezifischen Zweck verfolgen und sich auf die gleiche Rechtsgrundlage stützen können. So kann die Tätigkeit eines Treuhänders in Forschungsprojekten einem sehr spezifischen Zweck dienen, während die Durchführenden der Projekte einen umfassenderen Zweck verfolgen. Voraussetzung für die rechtmäßige Datenverarbeitung ist aber bei allen beteiligten Verantwortlichen, dass bei ihnen die Privilegierungsvoraussetzungen vorliegen. Fehlt es bei einem der Verantwortlichen an den Voraussetzungen hierfür, so kann der gesamte gemeinsam verantwortete Verarbeitungsprozess eine Privilegierung für sich nicht mehr in Anspruch nehmen, da dann die Verarbeitung *„gleichzeitig einem anderen Zweck"* dient (Art. 89 Abs. 4 DSGVO).

253 EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 77.
254 Doench/Sommerfeld in Kipker/Voskamp, 115.
255 Kremer CR 2019, 228.
256 Specht-Riemenschneider/Schneider MMR 2019, 505; Härting/Gössling NJW 2018, 2525.
257 Kremer CR 2019, 233f.
258 Golland K&R 2019, 534.

Gemeinsame Verantwortlichkeit ist immer gegeben, wenn in einem Forschungsprozess mehrere Stellen zeitgleich **aufeinander abgestimmt agieren**, ohne dass hierbei eine reine Verarbeitungsfolge vorliegt, bei der die nachfolgenden Verantwortlichen selbstständig über die weitere Verarbeitung entscheiden. Die Entscheidungen der Stellen müssen nicht zeitgleich erfolgen. Ein aufeinander abgestimmtes Vorgehen kann z.B. bei Arzneimittelstudien gegeben sein, wenn Sponsor, Studienzentren und Ärzte zusammenwirken.[259] Voraussetzung für die Mitverantwortlichkeit des Sponsors ist, dass dieser auf die Verarbeitungsprozesse einen (mit-)bestimmenden Einfluss nimmt (s.o.). Dies ist nicht der Fall, wenn die Festlegungen für die Datenverarbeitung ausschließlich von dem Prüfer vorgenommen werden.

Stellen **Webseitenbetreiber** ihre Seiten für ein Forschungsprojekt zur Verfügung und werden hierüber personenbezogene Daten erhoben, so sind der Projektbetreiber und die Webseitenbetreiber hinsichtlich des Erhebungsvorgangs gemeinsam Verantwortliche.

Werden in einem **Verbundprojekt** von verschiedenen Stellen medizinische Daten erhoben und dann in einer gemeinsamen Datenbank zusammengeführt, die von jedem der Projektpartner zur Auswertung genutzt wird, so besteht bzgl. der Datenerhebung jeweils eine individuelle Verantwortlichkeit, hinsichtlich der Speicherung und Nutzung jedoch eine gemeinsame Verantwortlichkeit.[260] Bedarf es in einer gemeinsam betriebenen Datenbank mit Mandantentrennung für den Abruf und die Nutzung eines Datensatzes durch eine andere als die erhebende Stelle der Freischaltung durch diese, so besteht bzgl. der Erhebung und der Speicherung eine individuelle Verantwortlichkeit, für die Nutzung dagegen eine gemeinsame Verantwortung.

Bei einem **Krankheits- oder sonstigen medizinisch relevanten Register**[261] kommt es darauf an, ob die Datenanlieferungen, die Datenspeicherungen sowie die Datenabfragen und -nutzungen in getrennten Schritten mit jeweils eigenständigen Entscheidungen erfolgen. In diesem Fall besteht für jedes Verfahrensstadium eine individuelle Verantwortlichkeit. Für die Speicherung und Übermittlung zum Zweck der Nutzung ist die Registerstelle verantwortlich. Dabei spielt es keine Rolle, ob das Register auf einer gesetzlichen oder einer vertraglichen Grundlage betrieben wird. Erfolgt dagegen die Datenanlieferung oder die Datenabfrage ohne individuelle Prüfung, so liegt eine gemeinsame Verantwortung bzgl. der Speicherung und der Übermittlung vor. Besteht für ein Krankheitsregister eine Vertrauens- und eine Registerstelle, so sind diese regelmäßig gemeinsam verantwortlich. Dies ist z.B. – auf gesetzlicher Grundlage – bei den gesetzlichen Krebsregistern[262], beim Implantateregister[263] und beim GKV-Datentransparenzregister mit seinem Forschungsdatenzentrum[264] der Fall.

259 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 4; Bischoff/Wiencke ZD 2019, 8f.

260 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 3; zu gemeinsamen Datenpools von Stellen in der Schweiz und der EU Mausbach ZD 2019, 453.

261 Zenker/Krawczak/Semler in TMF, 34ff.

262 § 65 Abs. 1 S. 1Nr. 8 SGB V.

263 Implantateregister-Errichtungsgesetz (EIRD) v. 12.12.2019, BGBl. I S. 2494, dort §§ 7–19 EIRD, dazu Kuketz DANA 2020, 35; Gode/Niemeck in Kipker/Voskamp, 540.

264 §§ 303a ff. SGB V, dazu BVerfG 19.03.2020 – 1 BvQ 1/20, JZ 2020, 1012f.; Weichert DANA 2020, 20; Schäfer in Kipker/Voskamp, 353ff.; Schulz SGb 09.20, 540f.; Platzer NZS 2020, 289ff.; Bretthauer/Spiecker, JZ 2020, 990ff.; Weichert MedR 2020, 539ff.; Kühling/Schildbach NZS 2020, 41ff.; Kühling, 49ff.; Graf von Kielmansegg in TMF, 111; Schrahe/Städter DuD 2020, 714ff.; Dierks 2020, 11ff.

Keine gemeinsame Verantwortlichkeit bei einem Verbundprojekt oder einem Register besteht, wenn die Anlieferung in der Weise erfolgt, dass für den Übermittler **keine weitere Bestimmungsmöglichkeit** über die angelieferten Daten besteht. Entscheidet eine Registerstelle oder ein Verbundpartner allein über die weitere Verarbeitung, so liegt eine aufeinander folgende getrennte Verantwortlichkeit vor.

Ein Anwendungsfall für eine alleinige Verantwortlichkeit ist es, wenn an eine zentrale Stelle oder Plattform **Sozialdaten** für Forschungszwecke angeliefert werden, wenn diese zentrale Stelle nicht selbst ein Sozialleistungsträger ist. Die spezifischen Regelungen des SGB zur Zweckbindung (Sozialgeheimnis) und zur (funktionalen) Verantwortlichkeit (s.o. Kap. 5.1) erlauben es nicht, dass Sozialleistungsträger und andere gemeinsam datenschutzrechtlich verantwortlich sind. Auch keine gemeinsame Verantwortlichkeit besteht bei dem Datentransparenzregister nach §§ 303a ff. SGB V zwischen den Daten anliefernden Krankenkassen und den Stellen des Transparenzregisters. Zwischen diesen – der Vertrauensstelle nach § 303c SGB V und dem Forschungsdatenzentrum[265] nach § 303d SGB V – bestehen in Bezug auf einzelne Verarbeitungsschritte der Datenanlieferung und der Datenspeicherung gemeinsame Verantwortlichkeiten auf gesetzlicher Grundlage. Diese gesetzliche Grundlage ersetzt, soweit sie ausreichende Regelungen enthält, die in Art. 26 DSGVO genannte Vereinbarung.

5.4 Anforderungen bei gemeinsamer Verantwortlichkeit

Art. 26 DSGVO verlangt eine **Vereinbarung**, ein „Joint Controller Agreement". Für die gemeinsame Festlegung von Zweck und Mitteln der Datenverarbeitung ist keine gemeinsame Entscheidungsfindung der Akteure erforderlich, doch zwingt sie diese dazu, sich hierüber zumindest informell zu verständigen.[266] Die Vereinbarung kann von einer Seite vorgegeben werden, der dann die anderen Verantwortlichen beitreten.[267] Nicht möglich ist es, allein mit der formalen Vereinbarung eine faktisch gegebene gemeinsame Verantwortlichkeit entgegen den objektiven Gegebenheiten auf einen der Verantwortlichen zu übertragen.[268] Wohl ist es aber möglich, hinsichtlich der tatsächlichen Wahrnehmung der Verantwortung zwischen den Beteiligten eine Arbeitsteilung auszuhandeln.

Bzgl. der **Form der Vereinbarung** gibt es keine Vorgaben. Da die Inhalte der Vereinbarung festgelegt und für die Betroffenen transparent sein müssen, ist eine konkludente – lediglich durch schlüssiges Verhalten begründete – Vereinbarung praktisch ausgeschlossen.[269] Möglich ist, dass die Vereinbarung mit anderen Absprachen verbunden wird, sofern hierdurch die Qualität der Information nicht leidet.[270]

Eine Vereinbarung ist nicht nötig, wenn und soweit die Aufgabenverteilung durch **verbindliches Recht der Union oder eines Mitgliedsstaates** festgelegt wird (Art. 26 Abs. 1 S. 2 DSGVO: begrenzte Öffnungsklausel). Derartige Festlegungen können bei

265 Zuvor Datenaufbereitungsstelle.
266 Hanloser BB 34.2019, I; Härting/Gössling NJW 2018, 2525.
267 Von dem Bussche DB 2018, 1782.
268 Im Sinne eines „Single-Controllership-Agreements", Golland ZD 2019, 381.
269 Weichert DANA 2019, 6; a.A. Schantz in Schantz/Wolff, Rn. 371.
270 Petri in SHS, Art. 26 Rn. 21.

Verarbeitungen im öffentlichen Interesse eine Rolle spielen.[271] So ist es für die nationalen Gesetzgeber möglich, für spezifische Formen der Verarbeitung von (medizinischen) Daten für Forschungszwecke Festlegungen nach Art. 26 DSGVO z.B. in Bezug auf Krankheitsregister vorzunehmen. Soweit solche normativen Festlegungen fehlen, sind sie durch eine Vereinbarung zu ergänzen.

Durch die jeweilige Vereinbarung kann das durch die DSGVO oder durch sonstiges staatlich **vorgegebenes Recht nicht modifiziert** werden. Die Rechte und Pflichten gemäß der DSGVO sowie sonstiger Datenschutzgesetze gelten für jeden der Verantwortlichen gleichermaßen.

Ein **wesentlicher Inhalt der Vereinbarung** muss sein, dass sich die gemeinsam Verantwortlichen verständigen, „wer von ihnen welche Verpflichtung" gemäß der DSGVO erfüllt. Gegenstände der Arbeitsteilung können sein: das Einholen einer Einwilligung (Art. 7 DSGVO); die Information über die Verarbeitung (Art. 12–14 DSGVO), die Bearbeitung von Betroffenenanträgen, etwa auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Verarbeitungseinschränkung (Art. 18 DSGVO)[272]. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen der Beteiligten widerspiegeln (Art. 26 Abs. 2 S. 1 DSGVO).[273]

Unerlässlich ist insofern die spezifische Erfassung der **tatsächlichen logistischen Infrastruktur**, also der Anwendungsprogramme, ihrer Schnittstellen und der ihnen zu Grunde liegenden physischen Infrastruktur.[274] Nicht nur die interne Aufgabenteilung sollte die Vereinbarung enthalten, sondern auch Aussagen über die interne Haftung, wenn einer der Verantwortlichen in Anspruch genommen wird.[275]

Der wesentliche Inhalt muss den **Betroffenen zur Verfügung** gestellt werden (Art. 26 Abs. 2 S. 2 DSGVO). Zur-Verfügung-Stellen bedeutet nicht, dass den Betroffenen der Text der Vereinbarung bzw. deren wesentlicher Inhalt[276] direkt mitgeteilt wird; es genügt, dass die Betroffenen vor Beginn der Verarbeitung einen Hinweis erhalten, wo oder wie sie den Text einsehen können.[277] Die Art und Weise der Information ist nicht festgelegt. Es ist möglich, dass mehrere Verantwortliche ihre Informationspflicht über eine einheitliche, in der Vereinbarung zu vereinbarende Stelle erfüllen.[278] Die Information kann z.B. über eine Webseite erfolgen, auf welche die Betroffenen zugreifen können.[279] Dies bietet sich bei großen, einrichtungsübergreifenden Projekten sowie bei Studien ohne direkten Betroffenenkontakt an. Möglich ist auch, dass den Probanden, z.B. im Rahmen einer Klinik- oder Arzneimittelstudie, ein Hinweisblatt oder eine Mitteilung auf einem umfassenderen Informationsblatt zur Verfügung gestellt wird. Eine mündliche Information genügt nicht.[280]

271 Petri in SHS, Art. 26 Rn. 22.
272 EDPS 2019, 27–29; Petri in SHS, Art. 26 Rn. 17.
273 Petri in SHS, Art. 26 Rn. 14.
274 Petri in SHS, Art. 26 Rn. 16.
275 Härting/Gössling NJW 2018, 2526; Jung/Hansch ZD 2019, 146; Grages CR 2020, 232ff.
276 Mindestens die Aufteilung der Pflichten und die Informationen nach Art. 13, 14 DSGVO, vgl. Martini in Paal/Pauly, Art. 26 Rn. 32, Kremer in SJTK, Art. 26 Rn. 42; Hartung in Kühling/Buchner, Art. 26 Rn. 26.
277 Däubler in DWWS, Art. 26 Rn. 12; a.A. Piltz in Gola, Art. 26 Rn. 21, der eine spätere Bereitstellung und dies erst auf Antrag des Betroffenen für ausreichend ansieht.
278 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 13.
279 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 4; Martini in Paal/Pauly, Art. 26 Rn. 34.
280 Hornung in SHS, Art. 26 Rn. 27.

Bei einer **wesentlichen Inhaltsänderung** einer Vereinbarung nach Art. 26 DSGVO, etwa hinsichtlich der Verantwortlichen oder einer Änderung der Zuständigkeit unter den Verantwortlichen, muss auch diese Information zur Verfügung gestellt werden. Bei einem Verweis auf einen Webauftritt oder eine sonstige Informationsquelle genügt eine dortige Änderung der jeweiligen Informationen. Einen besonderen Hinweis gegenüber den Betroffenen auf den Umstand der Änderung fordert Art. 26 Abs. 2 S. 2 DSGVO nicht.

Um die gemeinsame Verantwortlichkeit wahrnehmen zu können, müssen sämtliche Verantwortlichen eine im Wesentlichen klare Vorstellung davon haben, wie die gemeinsam verarbeiteten Daten erlangt werden und wie diese weiterverarbeitet werden. Die gemeinsam Verantwortlichen müssen, um die **Rechtmäßigkeit** der gemeinsam verantworteten Verarbeitung beurteilen zu können, sich deshalb über die hierfür relevanten Informationen austauschen.[281]

Verarbeitet einer der gemeinsam Verantwortlichen gemeinsam erhobene Daten weiter, so müssen die anderen Verantwortlichen eine Vorstellung davon entwickeln können, ob die weitere Verarbeitung rechtmäßig ist. Dies setzt voraus, dass über die Weiterarbeitung soweit Transparenz hergestellt wird, dass eine Beurteilung der **mitverantworteten Datenübermittlung** bzw. Offenlegung an den (mit verantwortlichen) Empfänger möglich wird. Erweist sich (im Nachhinein) die Beurteilung als falsch, so besteht eine verstärkte (weitere) Verantwortlichkeit für weitere Übermittlungen. In einem gemeinsam verantworteten Register muss z.B. erkennbar sein, für welche Zwecke die abgerufenen Daten verwendet werden dürfen. Ist einer der gemeinsam Verantwortlichen z.B. für die Speicherung und Verwaltung der sog. Metadaten[282] zuständig, so ist klarzustellen, für welche Zwecke dieser Verantwortliche diese weiternutzen darf.

Werden Daten aus unterschiedlichen Quellen in gemeinsamer Verantwortung zusammengeführt, so tragen sämtliche Nutzer der gemeinsamen Datenbank auch für die **Rechtmäßigkeit der Datenanlieferung und -speicherung** die gemeinsame Verantwortung. Um diese Rechtmäßigkeit zu gewährleisten, ist es sinnvoll, die Anforderungen an die Anlieferung mit den Übermittlern festzulegen. Dies kann in der Vereinbarung nach Art. 26 DSGVO erfolgen, die den Übermittlern bereitgestellt wird, oder in separaten Absprachen mit den Übermittlern.

Hinsichtlich der datenschutzrechtlich relevanten Vertragsinhalte nach Art. 26 DSGVO kann auf Art. 28 DSGVO zur **Auftragsverarbeitung** und dort insbesondere auf Abs. 3 zurückgegriffen werden. Die darin genannten Mindestinhalte ermöglichen es jedem der Verantwortlichen, eine überschlägige Rechtmäßigkeitsprüfung durchzuführen.[283] Bei den notwendigen Regelungspunkten kann insofern eine Anleihe gemacht werden, wobei aber die anders gelagerte Beziehung zwischen den Vertragspartnern berücksichtigt werden muss: Während beim Auftrag zumindest formal ein Über-/Unterordnungsverhältnis besteht, besteht hier – auch zumindest formal – eine gleichrangige Beziehung. Bei der Auftragsdatenverarbeitung hat der Auftraggeber die vorrangige materiell-rechtliche Verantwortung; bei der gemeinsamen Verantwortung

281 Datenschutzkonferenz (DSK) 05.09.2018, Beschluss zu Facebook-Fanpages; Weichert DANA 2019, 7.

282 Also der Nutzungs- bzw. Protokolldaten.

283 Specht-Riemenschneider/Schneider MMR 2019, 505, Hartung in Kühling/Buchner, Art. 26 Rn. 25; Weichert DANA 2019, 7; Schreiber ZD 2019, 57.

liegt diese uneingeschränkt bei jedem Verantwortlichen. Entsprechendes gilt für die Voreinstellungen (Privacy by Default) gemäß Art. 25 Abs. 2 DSGVO.

Hinsichtlich der sonstigen **technisch-organisatorischen Vorkehrungen** nach Art. 32 DSGVO, die bei der Auftragsverarbeitung voll dem Auftragsverarbeiter zugeordnet werden können, lassen sich auch bei einer gemeinsamen Verantwortlichkeit bei einzelnen Stellen Abstriche machen, wenn jeweils Verantwortliche arbeitsteilig die „Verantwortung" übernehmen. Anders als beim materiellen Recht und beim Privacy by Default gibt es hier nicht nur richtige oder falsche Lösungen. Vielmehr kann ein ganzer Instrumentenkasten zum Einsatz kommen, bei dem es auch kurzfristig Änderungen bzw. Änderungsnotwendigkeiten gibt, die nicht in jedem Fall den anderen Verantwortlichen kommuniziert werden können und müssen. Aus Sicherheitsgründen und zur Wahrung von Betriebs- und Geschäftsgeheimnissen können die jeweiligen Verantwortlichen u.U. Vertraulichkeit für sich beanspruchen. Entsprechendes kann gelten, wenn einer der Verantwortlichen für seine Verarbeitung Auftragsverarbeiter in Anspruch nimmt. Die Kategorien der Auftragnehmer sind aber zumindest zu benennen (Art. 15 Abs. 1 lit. c DSGVO). Bestehen bzgl. technisch-organisatorischer Maßnahmen oder einer Auftragsverarbeitung konkret begründete Zweifel an der Rechtmäßigkeit, so besteht auch insofern ein Informationsbedarf und Auskunftsanspruch der anderen Verantwortlichen.

Folgende Aspekte sind **für die Vereinbarung wesentlich**:

- die beteiligten Stellen mit Angaben zu Sitz/Niederlassung sowie Funktion bzw. Beziehung zu den Betroffenen,
- die verfolgten Zwecke jedes einzelnen Verantwortlichen in Bezug auf jede Datenart, also z.B. Namen, Identifizierungsdaten, IP-Adressen, Standortdaten, Kommunikationsdaten zu Zeit, Dienst, Partner, (Kommunikations-)Inhaltsdaten, insbesondere Diagnose- und Behandlungsdaten, evtl. differenziert nach Vertraulichkeitsstellung der Nutzenden,
- umfassende und abschließende Darstellung der gesamten gemeinsam verantworteten Datenverarbeitung (beispielhafte Beschreibung genügt nicht),
- Differenzierung nach Datenverarbeitung auf Einwilligungsbasis, auf Vertragsbasis, auf Abwägungsbasis bei (Plattform-)Mitgliedern, auf Abwägungsbasis bei Drittnutzenden,
- Differenzierung nach Sensitivität (Art. 9 DSGVO) sowie bei Kinderdatenverarbeitung (vgl. Art. 8 DSGVO),
- Übermittlung an dritte Stellen,
- insbesondere Drittlandtransfers (Art. 15 Abs. 1 lit. c DSGVO),
- Anonymisierung und Löschfristen,

involvierte Logik beim Profiling oder bei sonstigen automatisierten Entscheidungsverfahren (Art. 15 Abs. 1 lit. h, Art. 22 DSGVO).[284]

Hinsichtlich der Wahrnehmung der **Betroffenenrechte** können Absprachen zwischen den gemeinsam Verantwortlichen vorgenommen werden. Dazu gehört insbesondere die Information der Betroffenen nach den Art. 13, 14 DSGVO. Bzgl. der Bearbeitung von Ansprüchen aus den Art. 15–18, 21 DSGVO können zentrale Anlaufstel-

284 Ähnlich Specht-Riemenschneider/Schneider MMR 2019, 505f.

len etabliert werden (Art. 26 Abs. 1 S. 3 DSGVO). Für die Umsetzung von Betroffenenrechten ist eine gegenseitige Mitteilung vorzusehen (Art. 19 DSGVO).[285]

Auch bezüglich **sonstiger Verpflichtungen** (z.B. Führen des Verarbeitungsverzeichnisses, Durchführung der Datenschutz-Folgenabschätzung, Benennung eines Datenschutzbeauftragten, Protokollierungen) kann eine Arbeitsteilung verabredet werden. Eine Ausnahme stellt die Meldung bzw. die Benachrichtigung im Fall einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde bzw. an die Betroffenen (sog. „Breach Notification", Art. 33, 34 DSGVO) dar, da wegen der Kurzfristigkeit der Reaktionspflicht, die an die Kenntniserlangung jedes einzelnen Verantwortlichen anknüpft, kein Verweis auf einen anderen Verantwortlichen möglich ist.

Eine gemeinsame Verantwortlichkeit begründet denklogisch auch jenseits der Verpflichtung zum Abschluss einer Vereinbarung **Kooperationspflichten**, soweit die gemeinsame Verarbeitung tangiert ist.[286] Dies kann immer dann relevant werden, wenn Fragen der Rechtmäßigkeit einer Verarbeitung, die von der gemeinsamen Verantwortlichkeit erfasst wird, im Raum stehen.

5.5 Rechtliche Formen der gemeinsamen Verantwortung

Die rechtliche **Ausgestaltung des Binnenverhältnisses** zwischen den gemeinsam Verantwortlichen ist von der DSGVO nicht vorgegeben.[287] Dabei sind verschiedene Vertrags- und Gesellschaftsformen möglich, auch eine Gesellschaft bürgerlichen Rechts. Selbst die Organisationsform eines Vereins ist denkbar. Bei gesellschaftsrechtlichen Lösungen ist zu klären, ob die Gesellschaft selbst datenschutzrechtlich verantwortlich ist oder ob dies für die Gesellschafter gilt. Ist die Gesellschaft oder ein sonstiger rechtlicher Zusammenschluss selbst verantwortlich, dann ist zu prüfen, ob eine alleinige Verantwortlichkeit vorliegt, sodass es für eine Datenoffenlegung gegenüber den Gesellschaftern/Mitgliedern einer eigenständigen Rechtsgrundlage bedarf oder ob eine gemeinsame Verantwortlichkeit mit den Gesellschaftern besteht.

Für die Vereinbarung nach Art. 26 DSGVO bestehen keine Formvorgaben. Daher ist es möglich, eine separate Vereinbarung zu treffen, aber auch deren Inhalt in einen anderen (Gesellschafts-)Vertrag oder in eine andere Vereinbarung, etwa eine Vereins- oder Genossenschaftssatzung zu **integrieren**.

Erfolgt keine förmliche Festlegung in der Vereinbarung nach Art. 26 DSGVO, so stellt sich die Frage, ob dadurch automatisch eine **Gesellschaft bürgerlichen Rechts** (GbR) entsteht, die in § 705 BGB geregelt ist:

> *„Durch den Gesellschaftsvertrag verpflichten sich die Gesellschafter gegenseitig, die Erreichung eines gemeinsamen Zweckes in der durch den Vertrag bestimmten Weise zu fördern, insbesondere die vereinbarten Beiträge zu leisten."*

285 EDPS 2019, 30; vgl. Hartung in Kühling/Buchner, Art. 26 Rn. 25; zum oben Stehenden vgl. Weichert DANA 2019, 7f.; Schreiber ZD 2019, 57.
286 Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 1 Rn. 61.
287 DWWS-Däubler, Art. 26 Rn. 9; Petri in SHS, Art. 26 Rn. 18.

Wie oben (Kap. 5.2) ausgeführt, knüpft die Annahme einer gemeinsamen Verantwortung an objektive tatsächliche Verhältnisse an, nicht an einen gemeinsamen Willensakt. Voraussetzung ist nicht ein gemeinsamer Zweck i.S.d. Datenschutzrechts, sondern eine gemeinsame Verarbeitung, bei der jeder der Verantwortlichen einen eigenen Zweck verfolgen kann, die sich aber faktisch gegenseitig ergänzen. Die sich hieraus ergebenden Förderpflichten ergeben sich aus Art. 26 DSGVO, nicht aus einem Vertrag i.S.v. § 705 BGB. Eine gemeinsame datenschutzrechtliche Verantwortlichkeit kann also auf einer GbR beruhen; diese muss aber **nicht zwangsläufig** gegeben sein.[288]

Liegt keine andere Rechtsgrundlage für die Kooperation der gemeinsam Verantwortlichen als die Vereinbarung nach Art. 26 DSGVO vor und wird von den gemeinsam Verantwortlichen ein **gemeinsamer Zweck** verfolgt, so wird mit der Vereinbarung eine GbR begründet. Dies wird im Forschungsbereich oft der Fall sein, etwa wenn ein unabhängiger Treuhänder eingebunden wird oder wenn eine Vielzahl von Forschungseinrichtungen eine gemeinsame Datenbank betreibt. Ein gemeinsamer übergeordneter Zweck besteht darin, ein gemeinsames Forschungsprojekt durchzuführen, auch wenn die Beteiligten hierbei unterschiedliche Beiträge leisten. Ein gemeinsamer Zweck kann auch im gemeinsamen Betrieb einer Forschungsdatenbank liegen, auf welche die Beteiligten für eigene separate Forschungsprojekte zugreifen können. Bei der Annahme einer GbR handelt es sich im Fall einer gemeinsamen Verantwortlichkeit immer um eine Außengesellschaft, da sämtliche Verantwortlichen gegenüber Betroffenen eine Rechtsbeziehung haben. Die Annahme einer GbR nach § 705 BGB hat zur Folge, dass die §§ 706ff. BGB anwendbar sind.

Erfolgt die Entscheidung über Zwecke und Mittel einheitlich durch die GbR und nicht durch einzelne Gesellschafter, so ist die **GbR Verantwortliche als Gesamtgesellschaft**; es liegt dann insoweit keine gemeinsame Verantwortlichkeit der Gesellschafter vor.

5.6 Rechtsfolgen bei gemeinsamer Verantwortlichkeit

Die gemeinsame Verantwortlichkeit für konkrete Verarbeitungsprozesse hat zur Folge, dass sämtlichen Verantwortlichen **sämtliche datenschutzrechtlichen Verpflichtungen**, wie sie insbesondere in der DSGVO festgehalten sind, obliegen. Dies gilt u.a. für die Einhaltung der Grundprinzipien des Art. 5 Abs. 1 DSGVO, also insbesondere für die Rechtmäßigkeit der Verarbeitung (lit. a). Jeden trifft die Dokumentationspflicht (Art. 5 Abs. 2 DSGVO). Jedem Verantwortlichen obliegt weiterhin die Wahrung der Betroffenenrechte (Art. 12ff. DSGVO), insbesondere, dass die erforderlichen Informationen erteilt werden (Art. 12–14 DSGVO), die Beachtung der formellen Anforderungen, insbes. das Erstellen des Verarbeitungsverzeichnisses und die Durchführung einer Folgeabschätzung (Art. 30, 35 DSGVO). Jeder der Verantwortlichen muss dafür sorgen, dass Privacy by Default sowie im Grundsatz Privacy by Design umgesetzt werden einschließlich der erforderlichen technisch-organisatorischen Sicherungsmaßnahmen (Art. 25, 32 DSGVO). Um diesen Pflichten entsprechen zu können, sind in die Vereinbarung gem. Art. 26 DSGVO Regelungen aufzunehmen,

288 Kremer CR 2019, 232; Hartung in Kühling/Buchner, Art. 26 Rn. 30.

die hierzu Aussagen enthalten; Verabredungen zur Arbeitsteilung sind möglich (s.o. Kap. 5.4).

Kann ein Verantwortlicher seinen datenschutzrechtlichen Pflichten ohne die Unterstützung oder Beteiligen eines anderen Verantwortlichen nicht nachkommen, so ergibt sich allein schon aus dem Umstand des objektiven Vorliegens einer gemeinsamen Verantwortlichkeit eine **gegenseitige Kooperationspflicht**, soweit die Kooperationsmaßnahme für die Umsetzung der Datenschutzpflichten nötig ist. Diese Kooperationspflicht ergibt sich gemäß Art. 26 DSGVO als eine direkte Rechtsfolge aus dem objektiven Vorliegen einer gemeinsamen Verantwortlichkeit.[289] Ein Beispiel hierfür ist die Tätigkeit einer treuhänderischen Vertrauensstelle, die für die Pseudonymisierung und die Verwaltung der Pseudonyme in einer Forschungsdatenbank verantwortlich ist. Wendet sich ein Betroffener an eine mitverantwortliche Forschungseinrichtung, die Daten pseudonymisiert verarbeitet, so ist die Vertrauensstelle verpflichtet, die für die Zuordnung des Pseudonyms notwendige Unterstützung zu leisten.[290] Die gemeinsam Verantwortlichen haben aus Art. 26 DSGVO gegeneinander nicht nur einen Anspruch auf Abschluss einer Vereinbarung, sondern auch auf Auskunft oder im Fall einer Verweigerung einen Schadenersatzanspruch (Art. 82 DSGVO).[291]

Teilweise wird erörtert, ob es für den **Datenaustausch zwischen den gemeinsam Verantwortlichen** einer eigenständigen Rechtsgrundlage bedarf oder ob insofern, vergleichbar mit der Auftragsverarbeitung, eine „Privilegierung" (s.u. Kap. 5.7) besteht, die insbesondere auch sensitive Daten, etwa Gesundheitsdaten, mit einschließt.[292] Diese Frage ist jedoch rein akademischer Natur, da eine gemeinsame Verantwortlichkeit nur in Bezug auf einheitliche Verarbeitungsprozesse bestehen kann, für die jeder der Verantwortlichen einer Rechtsgrundlage bedarf.[293] Es kommt also nicht zu einer Übermittlung.[294] Es erfolgt allenfalls eine Offenlegung i.S.v. Art. 4 Nr. 2 DSGVO.[295] Wohl kann, da ein Verantwortlicher keinen Zugriff auf den zu verantwortenden Datenprozess haben muss, ein Zugriff eingeräumt werden. Hierfür muss eine rechtliche Grundlage bestehen; anderenfalls ist die gemeinsame Verarbeitung unzulässig.[296]

Durch die Vereinbarung von Zuständigkeiten für die Wahrnehmung spezifischer Datenschutzaufgaben können sich die intern nicht für zuständig deklarierten Verantwortlichen extern gegenüber den Betroffenen, der Datenschutzaufsicht oder den Gerichten nicht entlasten.[297] Vielmehr besteht für jeden der gemeinsam Verantwortlichen **im Außenverhältnis** eine individuelle Verpflichtung.[298]

289 Weichert, DANA 2019, 8.
290 Graf von Kielmansegg in TMF, 113.
291 Specht-Riemenschneider/Schneider, MMR 2019, 506f.
292 Golland ZD 2019, 382; ausführlich Kremer CR 2019, 230f.
293 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 11.
294 A.A. Martini in Paal/Pauly, Art. 26 Rn. 3a, der annimmt, die Datenweitergabe sei privilegiert.
295 Kremer CR 2019, 231.
296 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 1.
297 DWWS-Däubler, Art. 26 Rn. 14; Petri in SHS, Art. 26 Rn. 24.
298 Schreiber ZD 2019, 58; zur Gerichtszuständigkeit im Außenverhältnis Specht-Riemenschneider/Schneider MMR 2019, 508.

Dies gilt auch für Schadenersatzansprüche aus Art. 82 DSGVO, für die Art. 82 Abs. 4 DSGVO eine gesamtschuldnerische **Haftung** festlegt.[299] Nach Art. 82 Abs. 5 DSGVO kann der haftbar gemachte Verantwortliche die anderen Verantwortlichen in Regress nehmen. Fehlt es an einer Vereinbarung nach Art. 26 DSVGO oder an wesentlichen Inhalten, so liegt hierin in Verbindung mit den jeweiligen Regelungspflichten gemäß DSGVO ein Rechtsverstoß gemäß Art. 5 Abs. 2 DSGVO.[300] Die Aufsichtsbehörden haben die in Art. 58 DSGVO genannten Untersuchungs- und Abhilfebefugnisse.[301] Der Verstoß gegen Art. 26 DSGVO ist zudem gemäß Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt.[302]

Die gemeinsame Verantwortlichkeit ist gemäß Art. 30 Abs. 1 S. 2 lit. d DSGVO in das **Verarbeitungsverzeichnis** aufzunehmen. Verantwortlich sind sämtliche Empfänger gemäß Art. 4 Nr. 9 DSGVO, abgesehen von Auftragsverarbeitern nach Art. 28 DSGVO, gegenüber denen die personenbezogenen Daten offengelegt werden. Auch Verantwortliche, die keinen direkten Zugang zu den Daten haben, sind dann gemeinsam verantwortlich und im Verarbeitungsverzeichnis zu dokumentieren. Dies ergibt sich aus dem Sinn und dem Zweck des Art. 30 DSGVO ungeachtet der Verwendung des Singulars in der Regelung.[303]

Ist eine gemeinsame Verantwortlichkeit tatsächlich begründet und **weigert sich einer der Verantwortlichen**, eine angemessene Vereinbarung zu schließen, so liegt wegen der gemeinsamen Festlegung von Mitteln und Zwecken einer Dritte betreffenden Datenverarbeitung eine vertragsähnliche faktische Beziehung vor, die ein gesetzliches Schuldverhältnis und einen Anspruch gegen die weigernde Stelle auf Abschluss der Vereinbarung nach Art. 26 DSGVO begründet.[304] Zur Schaffung der faktischen Grundlagen für den Abschluss der Vereinbarung sowie zwecks Wahrnehmung der Pflichten als (gemeinsame) Verantwortliche können von der sich weigernden Stelle die nötigen o.g. Informationen gerichtlich eingefordert werden. Zumindest eine entsprechende Klage ist in Bezug auf Facebook inzwischen anhängig.[305] Der Abschluss der Vereinbarung bzw. die Bereitstellung der dafür nötigen Informationen sind nicht vertretbare Handlungen der sich weigernden Stelle, die mit Zwangsgeld nach § 888 Abs. 1 ZPO erzwungen werden können.

Die gerichtliche Durchsetzung dieser Ansprüche erfolgt gemäß Art. 79 Abs. 2 S. 1 DSGVO vor dem Gericht des Mitgliedsstaates, in dem der sich weigernde Verantwortliche eine Niederlassung hat.[306] Diese Regelung gilt nicht nur für Betroffene i.S.v. Art. 79 Abs. 1 DSGVO, sondern auch für verantwortliche Stellen untereinander. Offenkundig ist dies, wenn, was bei Social Media regelmäßig der Fall ist, der Betroffene zugleich Verantwortlicher in Bezug auf die Verarbeitung von Daten über Dritte ist (s.o. Kap. 5.1). Dies gilt aber auch in den sonstigen Fällen. Gemäß ErwGr 147 DSGVO zielt die DSGVO darauf ab, vorrangige **einheitliche Gerichtsstände** festzulegen. Für

299 Specht-Riemenschneider/Schneider MMR 2019, 507; Hanloser BB 34.2019, I.
300 Petri in SHS, Art. 26 Rn. 30.
301 Petri in SHS, Art. 26 Rn. 31; Schreiber ZD 2019, 58ff.
302 Petri in SHS, Art. 26 Rn. 32; Schreiber ZD 2019, 60.
303 Bertermann in Ehmann/Selmayr, Art. 26 Rn. 14; Kremer CR 2019, 226, 232.
304 Specht-Riemenschneider/Schneider MMR 2019, 506f.
305 BT-Fraktion Bündnis 90/Die Grünen, PM 02.10.2018, Klage gegen Facebook, https://www.gruene-bundestag.de/netzpolitik/klage-gegen-facebook.html.
306 Bergt in Kühling/Buchner (Fn. 26) Art. 79 Rn. 16; Specht-Riemenschneider/Schneider MMR 2019, 508.

den Innenausgleich zwischen zwei Verantwortlichen sollen die Gerichte zuständig sein, die auch für die Klage eines Betroffenen wegen des Rückgriffs auf einen Verantwortlichen zuständig sind.[307]

5.7 Auftragsverarbeiter

Der „Auftragsverarbeiter" wird in Art. 4 Nr. 8 DSGVO definiert. Danach ist

> *„Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet."*

Für die Auftragsverarbeitung genügt es, dass eine Stelle personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet. Er übernimmt eine spezifische Aufgabe oder mehrere Aufgaben im Interesse des Verantwortlichen.[308] An die Art oder die Form des Auftrags werden nur geringe Anforderungen gestellt, wohl aber an den Inhalt. Die rechtliche Zulässigkeit ist in Art. 28 DSGVO geregelt:

> *„(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.*
>
> *(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.*
>
> *(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter*
>
> *a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;*

307 Vgl. EuGH 15.06.2017 – C-249/16 (Kareda), Rn. 31; NJW 2018, 845; ZIP 2017, 1734.
308 EDPS 2019, 16f.

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vor-

liegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher."

Liegen die in **Art. 28 DSGVO genannten Voraussetzungen** vor, so ist der Auftragsverarbeiter nicht Dritter i.S.v. Art. 4 Nr. 10 DSGVO und die Verarbeitung durch ihn ist datenschutzrechtlich zulässig. Fehlt es an den Voraussetzungen des Art. 28 DSGVO, so gilt der Auftragsverarbeiter als Verantwortlicher (Art. 28 Abs. 10). Fehlt es für die Datenweitergabe an diesen Verantwortlichen, der im Auftrag einer anderen Stelle Daten verarbeitet, ohne dass die Anforderungen des Art. 28 DSGVO erfüllt sind, an einer sonstigen Rechtsgrundlage, so ist diese Datenweitergabe bzw. Übermittlung unzulässig.

Während das frühere deutsche Recht davon ausging, dass der Auftragsverarbeiter (Auftragnehmer) dem Verantwortlichen (Auftraggeber) zuzurechnen ist mit der Folge, dass die Datenweitergabe zwischen dem Auftraggeber und dem Auftragnehmer keine Übermittlung darstellt, wird bei der DSGVO nun weitgehend angenommen, dass dem Auftragsverarbeiter eine Eigenständigkeit zukommt und die Datenweitergabe zwischen diesem und dem Verantwortlichen eine „**Offenlegung durch Übermittlung**", also ein legitimationsbedürftige Datenverarbeitung, darstellt (Art. 4 Nr. 2 u. Nr. 8 DSGVO).[309] Der Auftragsverarbeiter ist „Empfänger" (Art. 4 Nr. 9 DSGVO, nicht Dritter, vgl. Art. 4 Rn. 10 DSGVO). Nach dieser Ansicht bedarf diese Offenlegung einer eigenständigen Rechtsgrundlage, etwa in Art. 6, 9 oder 10 DSGVO.[310] Für die Offenlegung und für die Verarbeitung durch den Auftragsverarbeiter wird bei nicht sensitiven Daten Art. 6 Abs. 1 UAbs. 1 DSGVO zur Anwendung gebracht.

Demgegenüber ist eine sehr weit verbreitete Meinung, die von den deutschen Aufsichtsbehörden geteilt wird, dass Art. 28 DSGVO weiterhin eine **Privilegierungswirkung** zur Folge hat. Rechtsgrundlage für eine Verarbeitung durch einen Auftragsverarbeiter sei die des Verantwortlichen i.V.m. Art. 28 DSGVO. Der Auftragsverarbeiter

309 Wedde in DWWS, Art. 28 Rn. 5–11; Bertermann in Ehmann/Selmayr, Art. 28 Rn. 4–8; Hofmann in Roßnagel 2017, § 3 Rn. 251; LNK § 6 Rn. 6; Ingold in Sydow, Art. 28 Rn. 29; Dovas ZD 2016, 516; Piltz K&R 2016, 712; Eckhardt/Kramer DuD 2016, 145f.; wohl auch Petri in SHS Art. 28 Rn. 10.

310 Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 18.

sei weiterhin nicht Dritter, sondern Teil des Verantwortlichen.[311] Für die erstgenannte Ansicht spricht, dass dem Auftragsverarbeiter in der DSGVO eine eigenständige Verantwortung zugewiesen wird, auch wenn diese von den Vorgaben des Verantwortlichen abhängig ist. Dies ändert aber nichts daran, dass für die Zweckfestlegung und damit für die materielle Zulässigkeit der Datenverarbeitung ausschließlich der Verantwortliche zuständig ist. In der Praxis hat der Streit jedoch keine wesentlichen Auswirkungen. Diese beschränken sich darauf, dass auf unterschiedliche Rechtsgrundlagen zurückgegriffen wird, die im Rahmen von Transparenzpflichten, etwa gegenüber den Betroffenen, benannt werden müssen. In Umsetzung der Informationspflichten ist der Betroffene über die „Empfänger oder Kategorien von Empfängern", wozu die Auftragsverarbeiter gehören (Art. 4 Nr. 9 DSGVO)[312], zu informieren (Art. 13 und 14, jeweils Abs. 1 lit. e DSGVO). So kann ein Betroffener oder auch ein sonstiger Beteiligter erkennen, auf welche Rechtsgründe sich die Verarbeiter beziehen. Dass eine Auftragsverarbeitung, auch bei sensitiven Daten, grundsätzlich erlaubt ist, ist nach beiden Meinungen anerkannt.[313]

Die Auftragsverarbeitung definiert das Verhältnis einer datenschutzrechtlich verantwortlichen Stelle (Auftraggeber) zu einer Stelle (Auftragsverarbeiter bzw. Auftragnehmer), die den Verantwortlichen als **Hilfsunternehmen bei der Verarbeitung** unterstützt. Beim Verantwortlichen müssen alle datenschutzrechtlichen Voraussetzungen (Einwilligung oder gesetzliche Gestattung) für eine Verarbeitung vorliegen.

Der **Verlauf der Trennlinie** zwischen Auftragsverarbeitung und eigenständiger Verantwortlichkeit, die aus rechtlicher Sicht zu ziehen ist, war schon nach altem Recht umstritten.[314] Hieran hat sich nichts geändert. Die Bezeichnung „Auftragsverarbeitung" und „gemeinsame Verantwortlichkeit" in einem Vertrag bzw. einer Vereinbarung kann insofern nur ein Indiz dafür sein, was von den Partnern beabsichtigt ist. Ob eine reine Hilfstätigkeit vorliegt oder ob ein Partner wesentliche Entscheidungen zur Verarbeitung beiträgt, hängt von der konkreten Ausgestaltung des Vertrags bzw. der Vereinbarung und den tatsächlichen Gegebenheiten ab.[315] Letztentscheidend ist, wer die Entscheidungshoheit über die Zwecke und Mittel der Verarbeitung ausübt.[316] Auch dem Auftragsverarbeiter kann hinsichtlich seiner Entscheidungskompetenz ein gewisser Spielraum eingeräumt sein. Wann dieser Spielraum so groß wird, dass eine Eigenverantwortlichkeit anzunehmen ist, hängt von dem konkreten Kontext, den bestehenden Regelungen und der gelebten Praxis ab. Während für den Auftragsverarbeiter bzgl. der Zwecke und des „Ob" der Datenverarbeitung kein Spielraum besteht, gibt es einen solchen bzgl. der Mittel und des „Wie".[317]

311 DSK, Kurzpapier Nr. 13 v. 17.12.2918, 2; Albrecht/Jotzo, Teil 5 Rn. 22f.; Martini in Paal/Pauly, Art. 28 Rn. 8a–10; BMH, Art. 28 Rn. 15–23; Schmitz/von Dall'Armi ZD 2016, 429, 432; Schmidt/Freund ZD 2017, 14; Krohm/Müller/Peltzer RDV 2016, 307; Cremer CR 2019, 230; Schantz in Schantz/Wolff, Rn. 939; Gola in Gola, Art. 4 Rn. 58: Art. 28 DSGVO als Rechtsgrundlage; ausführlich Hartung in Kühling/Buchner, Art. 28 Rn. 13–23.

312 Weichert in DWWS, Art. 4 Rn. 99.

313 Schantz in Schantz/Wolff, Rn. 379, zu möglichen Konsequenzen beim Widerspruchsrecht Hartung in Kühling/Buchner, Art. 28 Rn. 21.

314 Petri in Simitis, § 11 Rn. 22–24.

315 Petri in SHS, Art. 28 Rn. 21.

316 Petri in SHS, Art. 4 Nr. 7, Rn. 20; Weichert in DWWS, Art. 4 Rn. 87; 96f.; Klabunde in Ehmann/Selmayr, Art. 4 Rn. 36; Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 10.

317 Hartung in Kühling/Buchner, Art. 4 Nr. 7 Rn. 13, Art. 4 Nr. 8 Rn. 7, Art. 28 Rn. 26–30.

Mit der Ablösung des bisherigen Datenschutzrechts durch die DSGVO wurde teilweise die These vertreten, dass die Abgrenzung zwischen Auftragsverarbeitung und Funktionsübertragung obsolet werde, weil die Definition des Art. 4 Nr. 8 DSGVO eigenverantwortliches Handeln des Auftragsverarbeiters nicht ausschließe, es auf Verantwortlichkeiten nicht ankomme.[318] Diese Ansicht übersieht, dass nach Art. 28 Abs. 3 lit. a DSGVO die **Weisungen des verantwortlichen Auftraggebers** konstituierend für das Auftragsverhältnis sind und nach Art. 28 Abs. 10 DSGVO eine eigene Verantwortlichkeit des Auftragsnehmers nur begründet wird, wenn eine Verarbeitung entgegen den Weisungen erfolgt, also wenn der Auftragnehmer und nicht der Auftraggeber *„Zwecke und Mittel der Verarbeitung bestimmt"*.[319] Die durch die DSGVO neu eingeführten Pflichten (Bestellung eines Vertreters, Art. 27 Abs. 1, Führen eines Verarbeitungsverzeichnisses, Art. 30, Meldepflicht bei Datenpannen, Art. 33, 34) sind nicht konstituierend für die Abgrenzung zwischen dem Auftragsverarbeiter und dem Verantwortlichen.

Die **Mittel der Verarbeitung**, also die Art und Weise der Auftragserledigung, kann der Auftragsverarbeiter nach Art. 28 DSGVO selbst bestimmen. Er ist bei der Ausgestaltung der von ihm eingesetzten und verwendeten Hard- und Software sowie der verwendeten technischen und organisatorischen Infrastruktur grundsätzlich weisungsfrei.[320] Dies hindert den Verantwortlichen aber nicht, dem Auftragsverarbeiter für die Abwicklung des Auftrags bestimmte verpflichtende Vorgaben zu machen.[321] Schon nach dem bisherigen Recht bedurfte es für die Annahme einer Datenverarbeitung im Auftrag nach § 11 BDSGaF nicht einer bis ins Detail gehenden Anweisung. Der Auftragsdatenverarbeiter war für die Festlegung der technisch-organisatorischen Maßnahmen nach § 9 BDSGaF (mit) verantwortlich (§ 11 Abs. 4 BDSGaF). Entgegen teilweise vertretener Meinung[322] hat sich insofern rechtlich nichts geändert.[323]

Der Umfang der Entscheidungsspielräume des Auftragsverarbeiters bei der **Wahl der technisch-organisatorischen Maßnahmen** ist für die Annahme einer Auftragsverarbeitung unerheblich. Es entspricht der typischen Aufgabenverteilung, dass sich damit der Auftraggeber nicht im Detail befassen muss.[324] Während Art. 28 Abs. 3 S. 1 DSGVO präzise Vorgaben des Verantwortlichen bzgl. bzgl. der Art und des Zwecks der Verarbeitung verlangt, begnügt sich Art. 28 Abs. 3 S. 2 lit. c DSGVO mit der Verpflichtung, dass der Auftragnehmer *„alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift"*.

Eine Auftragsverarbeitung setzt ein **bipolares Verhältnis** voraus. Ein Auftragsverhältnis kann nur zwischen einem Verantwortlichen und einem Auftragsverarbeiter bestehen. Weitere Stellen können nur als Unterauftragsverarbeiter, also als Auftragnehmer eines Auftragsverarbeiters, eingebunden sein. Ein Auftragsverhältnis nach Art. 28 DSGVO mit mehreren Verantwortlichen ist ausgeschlossen, da dadurch keine

318 Härting, Rn. 579; Dovas ZD 2016, 516f.; Doench/Sommerfeld in Kipker/Voskamp, 120; Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 20f.

319 Petri in SHS Art. 4 Nr. 8 Rn. 6; Härting/Gössling NJW 2018, 2524; zum Verhältnis zwischen altem und neuem Recht ausführlich Thomale in SJTK, Art. 28 Rn. 9–13.

320 Artikel 29-Datenschutzgruppe, WP 169 v. 16.02.2010, 17; Däubler in DWWS, Art. 28 Rn. 15; Bertermann in Ehmann/Selmayr, Art. 28 Rn. 3.

321 Petri in SHS, Art. 28 Rn. 73; Däubler in DWWS, Art. 28 Rn. 15.

322 Müthlein, RDV 2016, 78f.; Rücker/Kugler, DB 2016, 2768

323 Petri in SHS, Art. 28 Rn. 7, 8; Ingold in Sydow, Art. 28 Rn. 16.

324 Kremer CR 2019, 229; Schreiber ZD 2019, 55.

eindeutige Verantwortlichkeit des jeweiligen Auftraggebers sichergestellt werden kann. Dies gilt auch für gemeinsam Verantwortliche: Zwar kann hier eine einheitliche Verarbeitung gegeben sein, doch auch hier ist es möglich, dass Weisungen und Entscheidungen der Verantwortlichen voneinander abweichen. Beauftragten mehrere Verantwortliche einen Auftragnehmer, so handelt es sich bei jedem Verhältnis um je eine Auftragsverarbeitung. Eine Vermischung der Daten beim Auftragnehmer ist unzulässig. Der Auftragnehmer ist zur Mandantentrennung verpflichtet.[325]

5.8 Datenempfänger

Der **Begriff** „Empfänger" wird in Art. 4 Nr. 9 S. 1 DSGVO definiert:

> *„[...] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht."*

Empfänger ist der Dritte als Übermittlungsempfänger und der Auftragsverarbeiter (s.o. Kap. 5.7). Der Begriff setzt eine rechtliche Eigenständigkeit gegenüber der die Daten weitergebenden Stelle voraus.[326] Nicht dazu zu zählen sind Organisationseinheiten innerhalb einer verantwortlichen Stelle, da die Regelung eine weitergehende rechtliche Eigenständigkeit verlangt.[327] Auch der Betroffene selbst ist kein Empfänger. Relevant ist der Empfängerbegriff in der DSGVO im Rahmen der Informationspflichten (Art 14), der Auskunftsrechte (Art. 15), der Mitteilungspflichten (Art. 19) und bei der Verzeichniserstellung (Art. 30).

Der Begriff der **Funktionsübertragung**, der nach dem alten Datenschutzrecht als Datenverarbeitung im Auftrag einer anderen Stelle in eigener Verantwortung verwendet wurde[328], wird heute von vielen als nicht mehr nützlich angesehen.[329] Der Begriff fand sich schon in der Vergangenheit und findet sich auch heute in keinem Datenschutzgesetz. Er wurde und wird weiterhin in der Literatur und in der Wissenschaft verwendet. Mit diesem Begriff wird in Abgrenzung von der Auftragsverarbeitung ein Dienstleistungsverhältnis verstanden, bei dem der Dienstleister einen eigenen Beurteilungs-, Ermessens- und Entscheidungsspielraum in Bezug auf konkrete Verarbeitungsinhalte hat.[330]

Dadurch begründet sich eine **eigenständige datenschutzrechtliche Verantwortlichkeit** des Empfängers der übertragenen Daten. Diese besteht z.B. bei einem externen Treuhänder (s.u. Kap. 5.9) wie auch in anderen Fällen, in denen gemeinsam Verantwortliche einen gemeinsamen Zweck verfolgen (s.o. Kap. 5.2). Für die dadurch nöti-

325 Datenschutzkonferenz (DSK), Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit, Version 1.0 v. 11.10.2012.

326 Unsicher insofern Ernst in Paal/Pauly, Art. 4 Rn. 57.

327 A.A. Kühling/Buchner, Art. 4 Nr. 9 Rn. 5; Gola/Schomerus, § 3 Rn. 51; Gola, RDV 2011, 66.

328 Krasemann in Jandt/Steidle, B. II Rn. 148, 185.

329 DSK, Kurzpapier Nr. 16, Stand 19.03.2018, 2; Kremer CR 2019, 228f.; Kremer in SJTK, Art. 28 Rn. 48, Hartung in Kühling/Buchner, Art. 28 Rn. 44; Thomale in Auernhammer, Art. 28 Rn. 19ff.; Müthlein, RDV 2016, 84f.; Mantz/Marosi in Specht/Mantz, § 3 Rn. 145.

330 Petri in SHS, Art. 28 Rn. 11, Härting, Rn. 575.

ge Datenoffenlegung bedarf es einer eigenständigen Rechtsgrundlage, also einer Rechtfertigung aufgrund einer Einwilligung oder eines Gesetzes. Der Begriff ist mit der DSGVO nicht überflüssig oder hinfällig geworden[331]; er ist weiterhin zur Abgrenzung von der Auftragsverarbeitung geeignet. Er eignet sich aber nicht, um eine individuelle von einer gemeinsamen Verantwortlichkeit abzugrenzen.

Werden personenbezogene Daten an Dritte weitergegeben, damit diese damit ausschließlich eigene Zwecke verfolgen, so liegt eine **Datenübermittlung** an allein verantwortliche Dritte vor. Ein Beispiel hierfür ist die Weitergabe von Daten, die im Rahmen der Aufgabenerfüllung einer Stelle entstanden sind, an eine andere Stelle für Forschungszwecke. Auch die Weitergabe von Forschungsdaten an eine andere Forschungseinrichtung mit einer eigenständigen wissenschaftlichen Zielrichtung ist eine Datenübermittlung.

5.9 Datentreuhänder

Treuhänderschaft ist ein im Zivilrecht anerkanntes Rechtsinstitut. Treuhänderaufgaben gehören z.B. zum Kernbereich notarieller oder sind ein Bestandteil anwaltlicher Tätigkeit. Möglich ist eine mehrseitige Treuhand, bei der eine Vertrauenstätigkeit gegenüber mehreren Personen oder Stellen mit möglicherweise entgegengesetzten Interessen erfolgt. Bei der treuhänderischen Tätigkeit wird dem Treuhänder eine **Rechtsmacht übertragen**, die er gemäß einer Treuhandanweisung einzusetzen hat. Besteht ein Interessenkonflikt, so bestehen regelmäßig besondere Benachrichtigungs- oder Transparenzpflichten.[332] Datentreuhänderschaft kann so organisiert sein, dass sie insbesondere Betroffeneninteressen wahrnimmt, dies möglicherweise auch im Interessengegensatz zu verarbeitenden Stellen[333], oder dass sie eher dem Bereich dieser Stellen zugeordnet werden, etwa zum Zweck der Datenminimierung (s.u. Kap. 10.4). Die unabhängige Stellung eines Treuhänders soll regelmäßig beiden Seiten dienlich sein.[334]

In der medizinischen Forschung ist der Einsatz eines Treuhänders oft Bestandteil eines umfassenden Datenschutzkonzepts (s.u. Kap. 11.4). Mit dessen Einsatz soll der Schutz der Daten gewährleistet und der Eingriff in die Betroffenenrechte minimiert werden, ohne dass der Informationsumfang für die Forschung beeinträchtigt wird. Er nimmt die Funktion eines rechtlich (teil-)selbstständigen bzw. unabhängigen **vertrauenswürdigen Dritten** wahr, der zwischen den speichernden und den forschenden Stellen sowie den Betroffenen seine Aufgabe wahrnimmt. Er sollte weisungsunabhängig sein und sich im Interesse des Vertraulichkeitsschutzes auf ein Aussageverweigerungsrecht und ein entsprechendes Verbot der Dokumentenbeschlagnahme

331 Ingold in Sydow, Art. 28 Rn. 15ff.; Schwartmann/Hermann in SJTK, Art. 4 Rn. 135; Spittka in Specht/Mantz, § 12 Rn. 68; Petri in SHS, Art. 4 Nr. 8 Rn. 6, Art. 28 Rn. 21.

332 ULD, 38.

333 Zur Treuhänderschaft im Verbraucherinteresse Blankertz, Designing Data Trusts, Why we need to test Consumer Data Trusts now, February[[in der folgenden Fußnote: Februar]] 2020, https://www.stiftung-nv.de/de/publikation/designing-data-trusts-why-we-need-test-consumer-data-trusts-now.

334 Ausführlich zu den Potentialen von Datentreuhändern Blankertz, Designing Data Trust, Why we need to test consumer data trusts now, Februar 2020, https://www.stiftung-nv.de/de/publikation/designing-data-trusts-why-we-need-test-consumer-data-trusts-now.

stützen können.[335] Dies ist der Fall, wenn ein Forschungsprojekt in einen ärztlich geleiteten Behandlungszusammenhang integriert ist und der Treuhänder als Mitwirkender nach § 203 Abs. 3, 4 StGB verpflichtet wird (s.u. Kap. 6.6). Die Vertrauenswürdigkeit eines Datentreuhänders sollte in jedem Fall durch vertragliche Festlegungen, kann aber auch durch öffentlich-rechtliche Bestimmungen abgesichert werden.[336] Sie setzt u.a. voraus, dass der Treuhänder mit den anvertrauten Daten nicht selbst Forschung betreibt.[337]

Typische **Aufgaben von Datentreuhändern** im medizinischen Forschungsbereich sind es, die Anonymisierung oder Pseudonymisierung sowie Aufgaben der Reidentifizierung vorzunehmen. Es geht also zumeist darum, die Verkettbarkeit von Daten zu handhaben und die hierfür nötigen Daten materiell-rechtlich, technisch und organisatorisch zu sichern und diese vorzuhalten. Die Funktion des Datentreuhänders besteht darin, Daten entgegenzunehmen, zu archivieren und bereitzustellen. Über den Treuhänder kann „informationelle Gewaltenteilung" sichergestellt werden.[338] Diese Aufgaben sind insbesondere relevant bei großen Datenbeständen, verschiedenen Datenquellen, komplexen und mehrfachen Datennutzungen und langfristigen Datenspeicherungen.[339] Eine Aufgabe von Treuhändern kann auch darin bestehen, für andere Stellen Transparenz- und Rechenschaftspflichten zu übernehmen, z.B. indem sie gewährleisten, dass Betroffenenrechten entsprochen wird.[340] Der Einsatz von Treuhändern ist somit eine spezifische Maßnahme zur Sicherung der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO, s.u. Kap. 10.3) oder der Wahrung der Betroffenenrechte (Art. 12ff. DSGVO) unter Einsatz technisch-organisatorischer Maßnahmen (Art. 25, 32 DSGVO).

Die Rolle von Treuhändern ist im allgemeinen **Datenschutzrecht** nicht geregelt. Eine solche findet sich vereinzelt in medizinrechtlichen Regelungen. So sieht § 12 Abs. 4 HambKHG vor, dass bei genetischer Forschung zu prüfen ist, *„ob die Sicherheit der betroffenen Personen vor einer unbefugten Zuordnung ihrer Proben und Daten es erfordert, dass die Pseudonymisierung durch eine unabhängige externe Datentreuhänderin oder einen unabhängigen externen Datentreuhänder erfolgt."* Ein Treuhänder wird rechtlich oft „Vertrauensstelle" genannt. Regelungen dazu finden sich in Krebsregistergesetzen der Länder, so etwa in § 5 Hessisches Krebsregistergesetz (HKRG)[341] oder § 6 Krebsregistergesetz Schleswig-Holstein (KRG SH)[342]. Eine Regelung gab es auch in Art. 7 Bayerisches Krebsregistergesetz.[343] Ähnliche Regelungen bestehen im Sozialgesetzbuch V (§§ 303a ff. SGB V)[344], für das Implantateregister (§§ 8, 9 IRegG) sowie zur Gewährleistung der Spenderanonymität im Transplantationsgesetz (§§ 12ff., 15c TPG) und im Transfusionsgesetz (§ 21 TFG).[345]

335 Metschke/Wellbrock, 43; Bizer, 195ff. m.w.N.; zum Beschlagnahmeschutz nach alter Rechtslage Dierks B2 F2.1, F2.2–F2.8.
336 Bizer DuD 1999, 394.
337 Böhm/Wagner, CR 1987, 625.
338 Metschke, 26f.; Dierks 2008, A1.
339 Bizer DuD 1999, 393ff.; Bizer, 196f.
340 TA-Projekt: Biobanken für die humanmedizinische Forschung und Anwendung, BT-Drs. 16/5374, 84, 103.
341 G. v. 17.10.2001, Hess GVBl. I 2001, 582.
342 G. v. 04.11.2015, GVOBl. SH 2015, 372.
343 G. v. 25.07.2000, Bay GVBl. S. 274, außer Kraft getreten am 31.03.2017; zu den Gesetzen auch Dierks 2008, B41ff.
344 Kühling, 52f.
345 ULD, 41ff.

So vielfältig die Aufgaben von Treuhändern sein können, so unterschiedlich können auch die **rechtlichen und organisatorischen Strukturen** sein, in die diese eingebunden sind. Sie können als gemeinnützige, privatwirtschaftliche oder staatliche Stellen eigenständig oder in Kooperation oder als Organisationsteil einer größeren Stelle tätig sein.[346]

Um seine Aufgabe als vertrauenswürdige Stelle wahrnehmen zu können, darf ein Treuhänder bei seiner grundlegenden Tätigkeit nicht an Weisungen gebunden werden. Das Vertrauen in ihn wird durch seine Unabhängigkeit und Neutralität begründet. Zugleich ist es aber für die Vertrauenswürdigkeit erforderlich, dass der Treuhänder **nach klaren vorgegebenen Regeln** agiert und dass die Einhaltung dieser Regeln überwacht wird bzw. das Handeln hinreichend transparent ist.[347] Die Regeln können durch Gesetze oder sonstige hoheitliche oder standesrechtliche Normen festgelegt sein, möglich ist aber auch eine vertragliche Grundlage.[348]

Gemäß den Vorgaben der DSGVO bestehen für eine rechtliche Einordnung von Datenverarbeitern nur die Alternativen einer eigenen Verantwortlichkeit oder der Auftragsverarbeitung. Da Treuhänder bzgl. ihrer Hauptfunktion weisungsunabhängig sein sollen und Weisungsabhängigkeit ein zentrales Wesensmerkmal für die Auftragsverarbeitung darstellt, kommt für den Datentreuhänder eine rechtliche **Einordnung als Verantwortlicher** in Betracht.[349] Handelt es sich bei einem Treuhänder um eine eigenständige juristische oder natürliche Person, so wird mit der Datenverarbeitung eine Verantwortlichkeit nach Art. 24 DSGVO begründet.

Rechtlich nicht ausgeschlossen ist jedoch, dass es sich bei dem Treuhänder um einen **Organisationsteil einer größeren juristischen Person** handelt. In diesem Fall liegt die datenschutzrechtliche Verantwortlichkeit gemäß DSGVO bei der juristischen Person. Die datenschutzrechtliche Letztverantwortung verbleibt bei der jeweiligen Stellenleitung.[350] Die Verantwortlichkeit für die Wahrnehmung der Treuhänderfunktion kann durch Gesetz, durch vertragliche Regelung oder auch durch einen einfachen internen Organisationsakt des Verantwortlichen begründet werden. Eine solche Delegation der Verantwortlichkeit ist dem Datenschutzrecht nicht fremd. Sie besteht in Bezug auf die Wahrung der beruflichen Verschwiegenheit durch Ärzte, also gebunden an eine persönliche Qualifikation eines Mitarbeiters (s.u. Kap. 6), aber auch funktional, etwa bei einem Betriebsarzt (§ 3 ASiG), beim Betriebsrat (§ 37, 78 S. 2 BetrVG)[351], beim (internen) Datenschutzbeauftragten (Art. 37f. DSGVO, §§ 5–7, 38 BDSG) sowie bei anderen Organisationsteilen, denen durch normative Vorgaben hin-

346 TA-Projekt: Biobanken für die humanmedizinische Forschung und Anwendung, BT-Drs. 16/5374, 84.
347 Dierks 2008, B44.
348 Dierks 2008, B45; Bizer, 197.
349 Dierks 2008, B63; Schneider 2015, 290f.
350 Dierks 2008, B46.
351 Bzgl. Betriebsräten ist dies hoch umstritten, wie hier Däubler, Gläserne Belegschaften, Rn. 640g, 850a; Brandt, CuA 11/2018, 30; Zieske, DANA 2018, 89; Hartung in Kühling-Buchner, Art. 4 Nr. 7 Rn. 11; Cumanns, RDV 2018, 55; Specht/Mantz-Ströbel/Wybitul, Teil B § 10 Rn. 77–82; Lücke, NZA 2019, 660; tendenziell Jung/Hansch, ZD 2019, 146f.; zweifelnd Gola in Gola, Art. 4 Rn. 55f.; Kranig/Wybitul, ZD 2019, 1ff.; offen lassend Hamann/Wegmann, BB 2019, 1348f.; a.A. LfDI BW, 34. Tätigkeitsbericht 2018, 1.6.1 (S. 37f.); LAG Sachsen-Anhalt 18.12.2018 – 4 TaBV 19/17, DB 2019, 1156; Kleinebrink, DB 2018, 2567f.; Beilecke, Landesdatenschutzgesetz Schleswig-Holstein, 2. Aufl. 1996, § 3 Rn. 3; zur Eigenverantwortlichkeit des Betriebs- bzw. Personalrats BAG, NJW 1998, 2466 = RDV 1998, 64.

sichtlich der Verarbeitung personenbezogener Daten eine gewisse Unabhängigkeit zugewiesen ist.

Weitgehend offen und deshalb gestaltungsfähig ist das Verhältnis, das sich datenschutzrechtlich durch die Unabhängigkeit des (internen) Treuhänders zwischen diesem und der Leitung der umfassenderen juristischen Person ergibt. Die **Beziehung Treuhänder – Stellenleitung** sollte so gestaltet sein, dass der letztlich verantwortliche Organisationsteil, also die Leitung, seine Verantwortlichkeit gemäß der DSGVO wahrnehmen kann, ohne dass die Unabhängigkeit des Treuhänders beeinträchtigt wird. Dies kann dadurch erfolgen, dass dem (internen) Treuhänder Dokumentations- und Rechenschaftspflichten gegenüber der Stellenleitung auferlegt werden, damit diese den Pflichten nach Art. 5 Abs. 2 DSGVO genügen kann. Die individuelle Bearbeitung der Betroffenenrechte (Art. 15ff. DSGVO) kann weitgehend an den Treuhänder delegiert werden.

Mangels konkreter gesetzlicher Vorgaben obliegt die Sicherstellung der Unabhängigkeit des internen Treuhänders der Organisationshoheit der Stellenleitung. Eine Rechtsform ist nicht vorgegeben. Möglich ist sowohl eine direktive Vorgabe durch die Stellenleitung als auch eine Vereinbarung zwischen Stellenleitung und Treuhänder.[352] Der **Organisationsakt** der Stellenleitung muss aber verbindlich sein, um als Garantie für die Rechte und Freiheiten der Betroffenen i.S.v. Art. 89 Abs. 1 S. 1, 2 DSGVO anerkannt werden zu können. Es ist angezeigt, eine Festschreibung der Prozessabläufe, der organisatorischen und technischen Vorkehrungen und des Entscheidungsspielraums des Treuhänders im Datenschutzkonzept (s.u. Kap. 11.4) vorzunehmen und die wesentlichen Informationen den Betroffenen (z.B. auf einem Hinweisblatt oder einer Webseite) zur Verfügung zu stellen.

Sonstige Aufgaben gemäß der DSGVO, bei denen es auf die konkrete Verarbeitung nicht ankommt, so etwa die Installation von Hard- und Software, die Festlegung und Umsetzung der technisch-organisatorischen Vorkehrungen (Art. 25, 32 DSGVO), die Erstellung der Verarbeitungsverzeichnisse (Art. 30 DSGVO) oder die Durchführung der Datenschutzfolgenabschätzung (Art. 35 DSGVO), obliegt der Stellenleitung, die in Respektierung der Unabhängigkeit des Treuhänders eine kooperative Lösung mit diesem anstreben sollte. Die Leitung der Stelle ist letztlich die Instanz innerhalb des Verantwortlichen, die über „Zweck und Mittel" der Verarbeitung bestimmt.

Bei einem externen Treuhänder ist dieser im Verhältnis zur Daten liefernden oder speichernden Stelle Dritter und erhält die personenbezogenen Daten im Rahmen seiner Aufgabenwahrnehmung in Ausübung der eigenen Verantwortlichkeit und nicht als Auftragsverarbeiter.[353] Die Rolle des Treuhänders als Dritter und als Übermittlungsempfänger hat zur Folge, dass er mit der Datenübermittlung zum **Verantwortlichen** wird. Er bestimmt (mit) über Zweck und Mittel der eigenen Verarbeitung.[354] Die Ausgestaltung einer Datentreuhänderschaft als Auftragsverarbeitung (Art. 28 DSGVO) ist zwar rechtlich nicht ausgeschlossen, aber nicht zu empfehlen. Dadurch würde der Vorteil der Datentreuhänderschaft, der Verweis auf die Vertraulichkeit durch Unabhängigkeit des Treuhänders, verloren gehen, da Auftragsver-

352 Dierks 2008, B44ff. in Bezug auf klinische Prüfungen.

353 Dierks 2008, B64.

354 A.A. hinsichtlich der alten Rechtslage Dierks (2008), B63ff., der für den Treuhänder die Regeln der Auftragsverarbeitung analog anwendete.

arbeitung insbesondere in Bezug auf die materielle Rechtmäßigkeit der Datenverarbeitung eine umfassende Weisungsabhängigkeit bedingt (Art. 28 Abs. 3 lit. a DSGVO). Weitere Vorteile einer Treuhänderschaft, etwa die technisch-organisatorische Trennung durch File-Trennung und Pseudonymisierung sowie durch die räumliche, organisatorische und personelle Abschottung, sind auch in der Ausgestaltung einer Auftragsverarbeitung erreichbar. Es ist dann aber nicht mehr angebracht, von einer Treuhänderschaft zu sprechen.

Externe Datentreuhänder im medizinischen Bereich sind in der Regel in einen umfassenderen Verarbeitungsprozess eingebunden, der mit der Datenerhebung oder zumindest der Datenübermittlung durch einen medizinischen Leistungserbringer beginnt, bei dem es zu einer Datenspeicherung bei einer weiteren Stelle kommt, über die letztlich Übermittlungen an Empfänger erfolgen, die die Daten auswerten oder anderweitig nutzen. Diese Nutzung kann für medizinische Forschungszwecke erfolgen. Die Einbindung des Treuhänders erfolgt zumeist bei einem Datentransfer zwischen Verantwortlichen. Grundlage solcher Treuhänderprozesse sind regelmäßig gemeinsame Entscheidungen, in die außer dem Treuhänder selbst zumindest die speichernde Stelle eingebunden ist. Auch die anliefernden sowie die auswertenden Stellen können einbezogen sein. Bei derartigen arbeitsteiligen Verarbeitungsprozessen für einen gemeinsamen Zweck gemäß einem verabredeten Verfahren handelt es sich um typische Formen **gemeinsamer Verantwortung** (s.o. Kap. 5.2–5.6). Welche Stellen bei dieser gemeinsamen Verantwortung mit einbezogen sind, hängt von den objektiven tatsächlichen Umständen ab. Relevant ist insbesondere, ob die Übermittlung zum Zweck der Speicherung sowie die Übermittlung zum Zweck der Auswertung/Nutzung jeweils auf einer Einzelfallentscheidung beruht oder die Entscheidung hierüber im gemeinsam vorgegebenen Prozessablauf vorweggenommen wird.

Eine **Funktionsübertragung** (s.o. Kap. 5.8) an einen Treuhänder kommt nur dann in Betracht, wenn diesem das ausschließliche Bestimmungsrecht über den Umgang mit treuhänderisch übertragenen Daten zugestanden wird, d.h., wenn dem Datentreuhänder in einer Verarbeitungskette das alleinige Bestimmungsrecht über die durch ihn erfolgende Verarbeitung zugestanden wird. Dies dürfte regelmäßig nicht im Interesse der Daten anliefernden noch in dem der Daten nutzenden Stellen liegen. Der Zweck der Treuhänderschaft liegt ja gerade darin, dass vom Treuhänder zwar unabhängig, aber gebunden an spezifische Vorgaben und somit vertrauenswürdig gehandelt wird. Insofern liegt die Ausgestaltung als gemeinsame Verantwortlichkeit nahe. Eine Funktionsübertragung (Kap. 5.8) ist aber nicht ausgeschlossen. Diese kann angenommen werden, wenn dem Treuhänder die ausschließliche Entscheidungshoheit über den treuhänderisch verwalteten Prozess (z.B. über die Reidentifizierung von pseudonymisierten Datensätzen) zugewiesen wird, ohne dass dieser Prozess eine notwendige Bedingung für sonstige Verarbeitungsprozesse ist. Eine solche notwendige Bedingung der Kooperation von Treuhändern mit weiteren Verantwortlichen ist z.B. bei der Behandlung von Betroffenenansprüchen bei einem pseudonym geführten Krankheitsregister gegeben.

An die Stelle einer gemeinsamen Entscheidung der Verantwortlichen in einer Form, die Eingang in eine Vereinbarung nach Art. 26 DSGVO findet, kann eine vollständig oder teilweise normativ, etwa durch den **Gesetzgeber**, vorgegebene Regelung treten (Art. 26 Abs. 1 S. 2 DSGVO).

Für die Beteiligung eines Treuhänders in einem Forschungsvorhaben bedarf es einer rechtlichen Einbindung. Fehlen gesetzliche oder sonstige übergeordnete rechtliche Vorgaben, so kommt als rechtlicher Rahmen eine **vertragliche Regelung** in Betracht. Bei der Festlegung der wesentlichen Vertragsinhalte sind die Anforderungen an eine gemeinsame Verantwortung zu beachten; dabei ist eine Orientierung an den rechtlichen Vorgaben für die Auftragsverarbeitung angesagt (s.o. Kap. 5.4).[355]

Inhalt der vertraglichen Regelung sollte u.a. eine spezifische **Vertraulichkeitsvereinbarung** sein.[356] Die rechtliche Absicherung der Vertraulichkeit kann darin bestehen, dass die Person, die mit der Treuhänderfunktion beauftragt wird, als Mitwirkende einer beruflichen Vertraulichkeitsverpflichtung unterliegt (s.u. Kap. 6.6). Notare, Rechtsanwälte oder auch Ärzte sind nicht allein wegen ihres Berufes schweigepflichtig, sondern auch wenn sie unabhängig von ihrer ursprünglichen Berufstätigkeit eine Treuhänderaufgabe wahrnehmen.[357] Es ist darauf zu achten, dass der Treuhänder nicht mit weiteren Aufgaben betraut wird, die zu Interessenkonflikten führen können.

Angesichts der technischen Möglichkeiten der digitalen Verkettung besteht die Notwendigkeit, die Datenbestände des Datentreuhänders so von den Forschungsmerkmalsdaten oder auch von sonstigen Datenbeständen abzuschotten, dass nur eine kontrollierte Zusammenführung, etwa zu Identifizierungszwecken, erfolgen kann.[358] Eine Absicherung der Vertraulichkeit kann durch die vertragliche Gewährleistung einer personellen, organisatorischen und räumlichen **Trennung der Wahrnehmung der Treuhändertätigkeit** von sonstigen Aufgaben erfolgen. Eine solche Trennung ist bei Forschungsprojekten insbesondere gegenüber wissenschaftlichen Datenauswertungen geboten.[359]

Um das Vertrauen der Betroffenen als Datengeber wie auch der Forschenden als Datennutzer zu rechtfertigen, sollte das Verfahren beim Datentreuhänder transparent sein in Bezug auf Datenquellen, Datenherausgaben und die dazwischen erfolgenden Prozesse. Das **Transparenzerfordernis** erstreckt sich damit auch auf das Verfahren, die Entscheidungsprozesse wie die Maßnahmen der Datensicherheit. Vertrauensfördernd sind Zertifizierungen und Auditierungen sowie die Umsetzung von Kontroll- und Berichtspflichten während des laufenden Betriebs.[360]

355 Ebenso Dierks 2008, B64.
356 Dierks 2008, B65.
357 Dierks 2008, B80.
358 Umfassend ULD, 50f.
359 Dierks 2008, B65; Dierks in Dierks/Roßnagel, 34; vgl. § 303a SGB V gemäß BT-Drs. 19/14867.
360 Martini/Hohmann NJW 2020, 3574.

6 Berufliche Schweigepflicht

Berufsgeheimnisse sind nicht ausdrücklich im GG oder in der GRCh garantiert. Wohl aber haben sowohl das BVerfG wie auch der EuGH[361] einen verfassungsrechtlichen Schutz solcher Geheimnisse anerkannt. Für bestimmte Berufs- und Personengruppen ist von Verfassungs wegen eine besondere Vertraulichkeit Voraussetzung für eine wirksame Tätigkeit. Dies hat rechtliche Grenzen bei Eingriffen in die Sphäre der Berufsausübenden zur Folge. Die Rechtsprechung gesteht **keine absolute Vertraulichkeit** bei der Berufsausübung zu. Zur Rechtfertigung von informationellen Eingriffen wird aber der Schutz hochrangiger Güter verlangt.[362]

Der Schutz beruflich begründeter Vertraulichkeit findet in Art. 339 AEUV eine normative Konkretisierung für EU-Institutionen.[363] Zur Begründung von Berufsgeheimnissen wird nicht nur auf das Recht auf Datenschutz bzw. auf das allgemeine Persönlichkeitsrecht zurückgegriffen, sondern zudem auf weitere **Verfassungsprinzipien**.[364] Zentrales Begründungsmuster für den gesteigerten verfassungsrechtlichen Schutz von Berufsgeheimnissen ist aber das allgemeine Persönlichkeitsrecht bzw.

361 EuGH 08.04.2014 – C-293/12 u. C-594/12 (Vorratsdatenspeicherung), Rn. 58, NJW 2014, 712; Hatje in Schwarze Art. 6 EUV Rn. 3.

362 BVerfG 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 Rn. 131–133, NJW 2016, 1788; MVVerfG 18.5.2000 – LVerfG 5/98, NVwZ 2000, 1038; SächsVerfGH 14.5.1996 – Vf. 44-II/94, NJW 1996, 1954 = DuD 1996, 496f.; Weichert 2018, Kap. 6.17.

363 BGH 10.08.1995 – IX ZR 229/94, NJW 1995, 2916; Wronka RDV 2017, 129; Eisele in Schönke/Schröder, § 203 Rn. 3.

364 Zur anwaltlichen Schweigepflicht BVerfG 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1919; BVerfG 20.4.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, Rn. 257, DVBl 2016, 779; Dochow, 802ff.

das Recht auf informationelle Selbstbestimmung der Person, die Hilfe bei der berufsausübenden Person in Anspruch nimmt.[365] Bei einem Seelsorger hat das BVerfG sogar auf den Schutz des „Kernbereichs privater Lebensgestaltung" zurückgegriffen.[366] Das BVerfG hat in Bezug auf die berufliche Tätigkeit eines Anwalts dargelegt, dass das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein darf. Dies leitet es auch aus der Schutzwirkung der Berufsfreiheit des Art. 12 GG ab. Die Notwendigkeit des Schutzes wird dabei nicht nur mit der Wahrung der Vertraulichkeit des Berufsgeheimnisträgers begründet, sondern auch mit den sich daraus ergebenden beschränkenden Auswirkungen auf dessen wirtschaftliche Entfaltung.[367] Wird das Vertrauensverhältnis im Rahmen der Telekommunikation beeinträchtigt, so wird Art. 10 GG herangezogen.[368] Vertrauensverhältnisse können eine stark kommunikative, demokratisch und wissenschaftlich meinungsbildende Relevanz haben, sodass die entsprechenden Grundrechte (Art. 5 GG, Art. 11, 13 GRCh) tangiert sein können.[369]

Das **Patientengeheimnis** (ärztliche Schweigepflicht) geht im Gesundheitsbereich auf den Eid des Hippokrates (um 460 bis um 370 vor Christus) zurück, der weiterhin Aktualität hat.[370] Das Patientengeheimnis hat neben dem Datenschutz seine Grundlage im Schutz der Unversehrtheit des Patienten (Art. 2 Abs. 2 S. 1 GG, Art. 3 GRCh), dem Schutz der Berufsausübung des medizinischen Helfers (Art. 12 GG, Art. 15 GRCh)[371] sowie im Sozialstaatsprinzip (Art. 20 GG bzw. Art. 34, 35 GRCh).[372] Er beruht auf der Erwägung, dass eine Hilfe suchende Person sich einem potenziellen Helfenden nur umfassend anvertrauen wird, wenn sich für sie hieraus keine nachteiligen Folgen ergeben können. Das umfassende Anvertrauen ist für den Helfenden nötig, um adäquat – individuell, kompetent, situationsbezogen und ausreichend – Hilfe leisten zu können. Dies gilt insbesondere, wenn die Hilfe dem Schutz der Unversehrtheit dient und eine staatliche Schutzpflicht besteht, wie dies im Hinblick auf die Gesundheit gegenüber der Allgemeinheit der Fall ist (s.u. Kap. 6.1). Die gesellschaftliche Funktion der Berufsgeheimnisse ändert nichts an dem Umstand, dass bei der Auslegung wie der bei konkreten Anwendung der Regelungen der Individualrechtsschutz bestimmend ist.

6.1 Rechtsgrundlagen

Die berufliche Schweigepflicht ist u.a. in § 203 StGB geregelt und gilt für eine Vielzahl von Berufen, bei denen eine besondere Vertrauensbeziehung der Berufsausübenden zu Betroffenen erforderlich ist. Im Rahmen der medizinischen Forschung sind

365 BVerfG 23.10.2006 – 1 BvR 2017/02, MMR 2007, 93f. = DuD 2006, 818f.; Dochow, 802.
366 BVerfG 25.1.2007 – 2 BvR 26/07.
367 BVerfG 12.4.2005 – 2 BvR 1027/02, NJW 2005, 1919.
368 BVerfG 30.4.2007 – 2 BvR 2151/06, NJW 2007, 2752f.
369 Zu Journalisten und die Pressefreiheit BVerfG 10.12.2010 – 1 BvR 2020/04, NJW 2011, 1863f.; BVerfG 27.2.2007 – 1 BvR 538/06 u.a., NJW 2007, 1118; allgemein Weichert 2018, Kap. 6.8.
370 Weichert DuD 2014, 831; Dochow, 800.
371 Ruffert in Callies/Ruffert, Art. 15 GRCh Rn. 24: „Vertrauensschutz".
372 Bernsdorff in Meyer Art. 15 Rn. 12; vgl. Hatje in Schwarze Art. 339 Rn. 6; Wegener in Callies/Ruffert, Art. 339 AEUV Rn. 2; zum Vertraulichkeitsschutz des Sozialarbeiters BVerfG 19.7.1972 – 2 BvL 7/71, NJW 172, 2214.

insbesondere folgende in § 203 Abs. 1 StGB genannten **Berufsausübenden im Gesundheitsbereich** relevant:

> *„Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als*
>
> *1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,*
>
> *2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung, ...*
>
> *6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder*
>
> *7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen ... Verrechnungsstelle*
>
> *anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."*

Der § 203 StGB ist als **strafrechtlicher Tatbestand** formuliert. Durch die Digitalisierung und die zunehmende Arbeitsteilung in der beruflichen Praxis von Berufsgeheimnisträgern und durch die damit unbegrenzten Möglichkeiten zur Verarbeitung von Geheimnissen und eine oft unbedachte Praxis des Austauschs hierüber ist die soziale Wirklichkeit des § 203 StGB zu einem in ihrer Häufigkeit kaum überbietbaren Massendelikt geworden. Beim Austausch unter Berufsgeheimnisträgern werden oft, z.B. wegen des Kosten- und Zeitdrucks, nicht nur die erforderlichen Daten weitergegeben, so wie dies § 203 StGB erfordert.[373] Bei der Kommunikation über das Internet wird oft nicht die technisch mögliche und von § 203 StGB geforderte Ende-zu-Ende-Verschlüsselung eingesetzt.[374] Bis zur rechtlichen Zulassung der Mitwirkung von technischen Dienstleistern im Jahr 2017 war eine Kenntnisgabe von Patientendaten nach § 203 StGB verboten, aber dennoch gängige, oft alternativlose Praxis.[375]

Eine **ernsthafte strafrechtliche Verfolgung** findet zumeist nicht statt. Die Rechtsgemeinschaft begnügt sich eher mit symbolischen Akten. Die rechtspraktische Bedeutung des § 203 StGB liegt in seinem Verbotsausspruch und dessen Auswirkung auf zivil-, verwaltungs-, sozial- und berufsrechtliche Regelungssysteme[376], also auch auf die rechtliche Bewertung der personenbezogenen Datenverarbeitung im Bereich der medizinischen Forschung. So ist nicht nur eine strafrechtliche, sondern auch eines standesrechtliche Sanktionierung möglich. Aus einer Verletzung der Schweigepflicht können sich Haftungsansprüche oder kann sich die Unwirksamkeit von Verträgen ergeben (§ 134 BGB).[377]

---

373 Eisele in Schönke/Schröder, § 203 Rn. 41, 51, 52.

374 8. TB Sächsischer Datenschutzbeauftragter, 2000, 102f.; a.A. Schöttle, BRAK-Mitteilungen 3/2018, 131.

375 Dochow, 815 m.w.N. auch für die Gegenmeinung.

376 Fischer, Strafgesetzbuch, 66. Aufl. 2019, § 203 Rn. 5; im Jahr 2017 kam es zu lediglich 7 Verurteilungen nach § 203 StGB in Deutschland, Statistisches Bundesamt, Fachserie 10 Reihe 3, Rechtspflege Strafverfolgung, 2017, 502.

377 Grundlegend BGH 10.10.1991 – VIII ZR 296/90, BGHZ 115, 123; BGH 10.10.2013 – III ZR 325/12, Rn. 22f. m.w.N., NJW 2014, 141 = MDR 2013, 1388 = VersR 2014, 1220; Fechtner/Haßdenteufel CR 2017, 356.

Im Medizinrecht findet die Schweigepflicht als Berufsgeheimnis bzw. als **Patientengeheimnis** weitere Ausformungen.[378] So findet sich in § 9 MBOÄ die folgende Musterformulierung für die konkret geltenden Berufsordnungen der Landesärztekammern:

> *„(1) Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen. Dazu gehören auch schriftliche Mitteilungen der Patientin oder des Patienten, Aufzeichnungen über Patientinnen und Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.*
>
> *(2) Ärztinnen und Ärzte sind zur Offenbarung befugt, soweit sie von der Schweigepflicht entbunden worden sind oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben unberührt. Soweit gesetzliche Vorschriften die Schweigepflicht der Ärztin oder des Arztes einschränken, soll die Ärztin oder der Arzt die Patientin oder den Patienten darüber unterrichten.*
>
> *(3) Ärztinnen und Ärzte dürfen ihren Mitarbeiterinnen und Mitarbeitern sowie Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, Informationen über Patienten zugänglich zu machen. Über die gesetzliche Pflicht zur Verschwiegenheit haben sie diese zu belehren und dies schriftlich festzuhalten.*
>
> *(4) Gegenüber den Mitarbeiterinnen und Mitarbeitern von Dienstleistungsunternehmen sowie sonstigen Personen, die an der beruflichen Tätigkeit mitwirken, sind Ärztinnen und Ärzte zur Offenbarung befugt, soweit dies für die Inanspruchnahme der Tätigkeit der mitwirkenden Personen erforderlich ist. Ärztinnen und Ärzte haben dafür zu sorgen, dass die mitwirkenden Personen schriftlich zur Geheimhaltung verpflichtet werden. Diese Verpflichtung zur Geheimhaltung haben Ärztinnen und Ärzte vorzunehmen oder auf das von ihnen beauftragte Dienstleistungsunternehmen zu übertragen.*
>
> *(5) Wenn mehrere Ärztinnen und Ärzte gleichzeitig oder nacheinander dieselbe Patientin oder denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis der Patientin oder des Patienten vorliegt oder anzunehmen ist."*

Entsprechende Regelungen bestehen z.B. für Psychotherapeuten[379], Apotheker[380] oder Hebammen und Entbindungspfleger[381].

Die berufliche Schweigepflicht kann dadurch aufgehoben werden, dass eine **Schweigepflichtentbindung** erfolgt. Dabei handelt es sich um eine Einwilligung zur Preisgabe des Patientengeheimnisses.[382] Einer solchen Schweigepflichtentbindung bedarf es nicht, wenn die Adressaten der Offenbarung Gehilfen oder Mitwirkende i.S.v. § 203 StGB sind (s.u. Kap. 6.6, vgl. § 9 MBOÄ). Untersuchen oder behandeln mehrere Ärzte gleichzeitig oder hintereinander denselben Patienten, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis anzunehmen ist (vgl. § 9 Abs. 4 MBOÄ). Nicht ausreichend als Legitimation für eine Offenbarung ist

378 Generell zum Verhältnis des § 203 StGB zu Befugnisnormen in Berufsordnungen Eisele JR 2018, 82f.
379 § 8 Abs. 1 der Musterberufsordnung der Bundespsychotherapeutenkammer.
380 Z.B. § 14 Berufsordnung der Landesapothekerkammer Baden-Württemberg.
381 Z.B. § 5 Berufsordnung für Hebammen und Entbindungspfleger NRW.
382 Dochow, 830ff.

es, dass der Adressat selbst einer beruflichen Schweigepflicht unterliegt oder vertraglich hierzu verpflichtet wurde, wenn keine Einbindung in die berufliche Tätigkeit erfolgt ist (s.u. Kap. 6.6).[383]

Gegenüber dritten Stellen gewährt das Gesetz Berufsgeheimnisträgern ein **Aussageverweigerungsrecht** sowohl im Zivilprozess (§§ 383 Abs. 1 Nr. 6, 385 As. 2 ZPO) als auch im Strafverfahren (§ 53 Abs. 1 Nr. 3 StPO) oder im Verwaltungsprozess (§ 98 VwGO).

6.2 Forschung durch Berufsgeheimnisträger

Damit ein Geheimnis als fremd im Sinne der beruflichen Schweigepflicht eingestuft werden kann, muss es dem Geheimnisträger *„in seiner beruflichen Tätigkeit anvertraut oder sonst bekannt geworden sein"*. Grundlage des Geheimschutzes ist ein **Vertrauensakt**.[384] Es muss ein innerer Zusammenhang mit der Ausübung des Berufes bestehen.[385] Nicht zwingend nötig ist, dass die Vertrauensbeziehung direkt zwischen dem Betroffenen und dem Berufsausübenden besteht, diese kann durch andere Vertrauenspersonen vermittelt sein. Was konkret zur beruflichen Tätigkeit gehört, ergibt sich „aus dem beruflichen Rollenbild" des Berufsausübenden. Berufsfremd sind Tätigkeiten, *„die überwiegend von anderen Personen professionell wahrgenommen werden"*.[386]

Die **forschende Tätigkeit eines Berufsgeheimnisträgers**, etwa eines Arztes, ist als berufliche Tätigkeit i.S.d. § 203 StGB zu bewerten, wenn die Forschung im Rahmen der beruflichen Funktion erfolgt. Die Forschungstätigkeit eines Arztes mit den von ihm erhobenen Daten ist seiner beruflichen Tätigkeit zuzurechnen, unabhängig davon, ob er in einem Universitätskrankenhaus, einem sonstigen Krankenhaus oder in einer ambulanten Arztpraxis tätig ist.[387] Etwas anderes gilt, wenn ein Arzt nicht im medizinischen Kontext forscht.[388]

Medizinische Forschung erfolgt nicht mehr nur mit den Daten der eigenen Patienten; Gesundheitsdaten werden dabei regelmäßig aus einer Vielzahl von Quellen zusammengeführt und ausgewertet. Voraussetzung ist, dass der Forschende „als Arzt" tätig wird und die forschende Tätigkeit seiner **Berufsausübung zuzurechnen** ist. Insofern ist auf § 1 MBOÄ zu verweisen:

> *„Ärztinnen und Ärzte dienen der Gesundheit des einzelnen Menschen und der Bevölkerung [Abs. 1 S. 1]. Aufgabe der Ärztinnen und Ärzte ist es, das Leben zu erhalten, die Gesundheit zu schützen und wiederherzustellen, Leiden zu lindern, Sterbenden Beistand zu leisten und an der Erhaltung der natürlichen Lebensgrundlagen im Hinblick auf ihre Bedeutung für die Gesundheit der Menschen mitzuwirken [Abs. 2]"*.

383 Rehborn in Prütting, § 9 MBO-Ä Rn. 8.
384 Roßnagel/Geminn in Dierks/Roßnagel, 234; Clernlack/Niehaus in MüKo StGB, § 203 Rn. 48.
385 Lenckner/Eisele in Schönke/Schröder, § 203 Rn. 13; Dochow, 823.
386 Kargl in Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Aufl. 2017, § 203 Rn. 13.
387 Vgl. § 303e Abs. 4 S. 2, 3 SGB V für medizinische Forschung mit Daten des Transparenzregisters.
388 Roßnagel/Geminn in Dierks/Roßnagel, 237ff.; a.A. Dierks in Dierks/Roßnagel, 72, wonach anders als bei einem Arzt in einer Uni-Klinik bei einem Vertragsarzt die Forschung nicht zur beruflichen Tätigkeit gehört.

Verfolgt die forschende Tätigkeit eines Arztes nicht diese Zielsetzungen, so sind das ärztliche Schweigerecht und die entsprechende Pflicht nicht anwendbar. Fraglich kann dies etwa im Bereich der Kosmetik sein.[389] Benutzt ein Arzt sein medizinisches Wissen und seine Forschung, um Menschen zu schaden, so kann er sich bei seiner Forschungstätigkeit nicht auf seine ärztliche Geheimnisprivilegierung berufen. Dies gilt auch, wenn ein Arzt nicht in einem medizinischen, sondern einem anders gearteten Kontext forscht.[390]

Wird ein medizinisches Forschungsprojekt **von einem Arzt durchgeführt** bzw. geleitet, ohne dass er eine Behandlung der Betroffenen durchführt, so kann er auch der ärztlichen Schweigepflicht unterliegen. Dies gilt, wenn er als ärztlicher Forschender Daten erhebt, die ihm in seiner Eigenschaft als Arzt anvertraut worden oder bekannt worden sind, indem er nicht nur die Daten des Betroffenen erhebt, sondern ihn hierbei zugleich berät.[391] Maßgebliches Kriterium der Zuordnung zum Geheimnisbereich ist das individuelle Interesse des Patienten, dass bestimmte Informationen geheim gehalten werden.[392] Der rein forschende Arzt, der unabhängig von einer individuellen Beziehung zum Betroffenen ärztlich wirkt, soll nicht vom Schutzbereich des Patientengeheimnisses erfasst sein.[393]

6.3 Materielles Verhältnis zum Datenschutzrecht

Das neue BDSG enthält ebenso wie im alten Recht (§ 1 Abs. 3 S. 2 BDSGaF) in § 1 Abs. 2 S. 2 eine ausdrückliche Regelung zum Verhältnis des Datenschutzrechts zu den Berufs- und besonderen Amtsgeheimnissen. Entsprechendes ist für das Sozial(datenschutz)recht in § 35 Abs. 2a SGB I geregelt[394]:

> *„Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt."*

Danach sind Rechtsvorschriften, die einen Sachverhalt regeln, für die das BDSG (bzw. das SGB) nicht abschließend ist, neben den Regelungen des BDSG (bzw. des SGB) anwendbar. Datenschutzrecht und Geheimnispflichten sind parallel anzuwenden (sog. **Zwei-Schranken-Prinzip**).[395]

Trotz großer Übereinstimmungen **unterscheiden** sich das Datenschutzrecht und das Recht der Berufsgeheimnisse in Bezug auf die Schutzziele, den materiellen Inhalt, die Verpflichteten (s.u. Kap. 6.4), die Vorkehrungen und Maßnahmen, die Aufsicht

389 Rehborn in Prütting, § 1 MBO-Ä Rn. 6a.
390 Roßnagel/Geminn in Dierks/Roßnagel, 240.
391 Dierks 2008, B31 in Bezug auf das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Nr. 3 und den Beschlagnahmeschutz nach § 97 StPO.
392 Dochow, 821.
393 Dierks 2008, B31.
394 Bieresborn NZS 2017, 891f.
395 Hauser/Haag, 13; Dierks in Dierks/Roßnagel, 14; Dierks 2019, 76; Weichert in Kühling/Buchner Art. 9 Rn. 141, 146; Graf von Kielmansegg in TMF, 115; a.A. Wronka RDV 2017, 131.

und die Sanktionen.[396] So sind die Anforderungen an eine datenschutzrechtliche Einwilligung in mancher Hinsicht strenger als die an eine Entbindung von der beruflichen Schweigepflicht.[397]

Oft ist unklar, inwieweit **datenschutzrechtliche Befugnisregelungen** eine Legitimation zur Offenbarung von Berufsgeheimnissen geben. Dies ist zweifellos der Fall, wenn eine Regelung sich ausdrücklich auf ein Berufsgeheimnis bezieht (so z.B. § 76 SGB X[398]). Eindeutig sind auch die Fälle, in denen die datenschutzrechtliche Befugnisregelung typischerweise Daten erfasst, die einem Berufsgeheimnis unterliegen, etwa in Krankenhausgesetzen.[399] So legitimieren z.B. die Regelungen des SGB V die Offenbarung von Patientengeheimnissen durch Leistungserbringer v.a. an die Krankenkassen oder die Kassenärztlichen Vereinigungen für Zwecke der Abrechnung, der Abrechnungskontrolle, aber auch für Maßnahmen im Bereich der Wirtschaftlichkeitskontrolle oder der Qualitätssicherung.

Erfasst eine Datenschutzregelung Fallgestaltungen, die sowohl innerhalb wie außerhalb des Bereichs des Berufsgeheimnisschutzes anwendbar sind, so ist es regelmäßig nicht die Absicht des Gesetzgebers, damit eine Offenbarungsbefugnis zu begründen. Es muss geprüft werden, ob mit der Regelung eine derartige Absicht verfolgt wurde. Ein Indiz hierfür ist, dass beim Empfänger eines Berufsgeheimnisses ein **gesteigerter rechtlicher Schutz** vorgesehen ist, z.B. in Form einer strengen Zweckbindung oder eines Weitergabe- oder Beschlagnahmeverbots, und wenn organisatorische, technische oder prozedurale Sicherungen eine Anhebung des Schutzniveaus bewirken. Wegen den Anonymisierungspflichten, der strengen Zweckbindung sowie weiterer Anforderungen (z.B. Genehmigungsvorbehalten) können die Forschungsregelungen im Datenschutzrecht eine Übermittlung bzw. eine Erhebung von Berufsgeheimnissen rechtfertigen, auch wenn kein gleichwertiger Beschlagnahmeschutz gesichert ist. Bestehen also Forschungsregelungen im nationalen Recht, die eine Zweckänderung für die Wissenschaft erlauben und zugleich einen gesteigerten Schutz dieser Daten vorsehen, so können diese Regelungen auch auf Patientengeheimnisse angewendet werden. Im Zweifel bleibt der Berufsgeheimnisschutz aber von der datenschutzrechtlichen Regelung unberührt.[400]

6.4 Personelles Verhältnis zum Datenschutzrecht

Hinsichtlich der Verpflichteten bzw. der Adressaten unterscheiden sich die Berufsgeheimnisse vom Datenschutzrecht. Straf- und standesrechtlich verpflichtet sind nicht auch die juristischen, sondern die handelnden natürlichen Personen. Diese Pflicht trifft vorrangig den Leiter der medizinischen Einrichtung, also z.B. den

396 Kircher in Kingreen/Kühling, 204f.; Roßnagel/Geminn in Dierks/Roßnagel, 232f.; ausführlich zur Wechselbeziehung und zu unterschiedlichen Theorien Dochow, 577ff.

397 Fechtner/Haßdenteufel CR 2017, 362.

398 Kühling, 73f.; Dierks in Dierks/Roßnagel, 15, 62ff.; Dierks will auf § 76 SGB X die Mitwirkungsregelung des § 203 Abs. 3, 4 StGB wegen „erheblichen Subsumtionsproblemen" nicht anwenden; dies ist nicht nachvollziehbar.

399 Roßnagel/Geminn in Dierks/Roßnagel, 233; Graf von Kielmansegg in TMF, 115.

400 Weichert in Kühling/Buchner Art. 9 Rn. 148; enger Schneider 2015, 76ff. zu den Befugnisregelungen des BDSGaF generell.

leitenden Arzt, im Krankenhaus den ärztlichen Direktor, oder sonstige Personen, die den Status eines originären **Berufsgeheimnisträgers** innehaben.

Von der Geheimnispflicht des Berufsgeheimnisträgers abgeleitet ist die der „berufsmäßig tätigen Gehilfen" (§ 203 Abs. 3 S. 1 StGB), also der **Mitarbeiterinnen und Mitarbeiter**, die in der Sphäre des Geheimnisträgers tätig sind.[401] Der Begriff des „Gehilfen" orientiert sich daran, dass ein Beschäftigungsverhältnis besteht. Das Beschäftigungsverhältnis, also eine arbeitsrechtliche Beziehung, muss nicht mit der Person des Berufsgeheimnisträgers bestehen, sondern kann auch mit einer juristischen Person vorliegen, der sowohl der Berufsgeheimnisträger wie auch der Mitarbeiter angehört. Weitere Voraussetzung ist, dass der Berufsgeheimnisträger zum Mitarbeiter in Bezug auf die Wahrung des Berufsgeheimnisses ein **Weisungsrecht** hat. Die Mitarbeiterfunktion erstreckt sich damit auch auf das gesamte Verwaltungspersonal z.B. eines Krankenhauses bis zum Verwaltungsdirektor.[402]

Die Berufsgeheimnisträger trifft in Bezug auf die Geheimhaltung nicht nur eine Pflicht zur persönlichen Verschwiegenheit, sondern auch eine **technisch-organisatorische Pflicht**. Durch Unterlassen von Sicherungsmaßnahmen kann es zu Offenbarungen kommen.[403] Offenbaren i.S.v. § 203 StGB ist schon das bloße Eröffnen der Möglichkeit der Kenntnisnahme.[404] Auch das Verschaffen von Gewahrsam mit der Möglichkeit der Kenntnisnahme ist ein Offenbaren.[405] Die Pflicht zum technischen Schutz der Berufsgeheimnisse obliegt i.d.R. und insbesondere dem hierarchisch obersten Berufsgeheimnisträger, also in einem Krankenhaus z.B. dem ärztlichen Direktor.

Es besteht somit ein gewisses Spannungsverhältnis zwischen dem Datenschutzrecht, das letztlich die Leitung einer verantwortlichen Stelle verpflichtet, und Berufsgeheimnissen, die insbesondere personell den leitenden Berufsausübenden zur Vertraulichkeit verpflichtet. Dieses Spannungsverhältnis wird durch den zwischen dem datenschutzrechtlich Verantwortlichen und dem Berufsausübenden bestehenden **Arbeitsvertrag** aufgelöst, der beide Seite dazu verpflichtet, bei der Umsetzung der Pflichten die jeweils andere Seite zu unterstützen.

6.5 Geheimnis

Gegenstand (Tatobjekt) der Geheimhaltungspflicht ist ein **fremdes Geheimnis**. Voraussetzung ist, dass der Geheimnisträger oder der Betroffene ein sachlich begründetes Geheimhaltungsinteresse hat. Darunter fallen im medizinischen Bereich Angaben zur Krankheit (Art, Verlauf, Anamnese, Diagnose, Therapie, Prognose), festgestellte Auffälligkeiten und Mängel, Patienten betreffende Dokumente, Akten und Daten, Untersuchungsmaterial und Untersuchungsergebnisse, Angaben über persönliche, familiäre, berufliche, wirtschaftliche oder finanzielle Umstände. Es muss sich nicht um zum persönlichen Lebensbereich gehörende Geheimnisse handeln,

401 BT-Drs. 18/11936, 23; dazu Ruppert K&R 2017, 612.
402 Tsambikakis in Prütting, § 203 StGB Rn. 21; Hauser/Haag, 27f., OLG Oldenburg 10.06.1082 – 2 Ws 204, 82, NJW 1982, 2616; ebenso, aber zweifelnd Eisele in Schönke/Schröder, § 203 Rn. 70; Eisele JR 2018, 80f.
403 Roßnagel/Geminn in Dierks/Roßnagel, 233; Pohle/Ghaffari CR 2017, 490, 493.
404 BT-Drs. 18/11936, 28; Roßnagel/Geminn in Dierks/Roßnagel, 230; Ruppert K&R 2017, 610.
405 Eisele JR 2018, 80.

möglich sind auch Betriebs- und Geschäftsgeheimnisse. Erfasst wird schon der Umstand einer medizinischen Behandlung oder dass eine Kranken-, Unfall- oder Lebensversicherung abgeschlossen wurde.[406]

6.6 Geheimhaltung der mitwirkenden Person

Angesichts der Digitalisierung der Berufstätigkeit von Berufsgeheimnisträgern stellte sich in immer stärkerem Maße die Frage, inwieweit deren informationstechnische (IT-)Dienstleister Kenntnis von Berufsgeheimnissen erlangen dürfen. Die von diesen installierten und administrierten Geräte und Programme verarbeiten die Geheimnisse, ohne dass die **Dienstleister** die Befugnis zur Kenntnisnahme hatten und auch keiner Pflicht zur besonderen Geheimhaltung unterworfen waren. Zugleich bestand zunehmend die Notwendigkeit einer entsprechenden Kenntnisnahme, zumal die Berufsgeheimnisträger regelmäßig nicht über die nötigen technischen Kenntnisse verfügen, um die von ihnen verantwortete Datenverarbeitung zu installieren, zu administrieren und insbesondere auch die Geheimnisse technisch abzusichern.[407]

Die herrschende Ansicht in Rechtsprechung und Literatur ging davon aus, dass eine Offenbarung an externe (IT-)Dienstleister nicht von dem **bisher verwendeten Gehilfenbegriff in § 203 StGB** abgedeckt wird, da sie nicht der Sphäre des Berufsgeheimnisträgers zugehören.[408] Voraussetzung für eine zulässige Mitteilung innerhalb des eigenen Wirkungsbereichs ist, dass diese in einem inneren funktionalen Zusammenhang mit der beruflichen Tätigkeit steht.[409] Teilweise wurde dies weniger eng gesehen und externe Dienstleister wurden als Gehilfen behandelt, denen im Rahmen des Erforderlichen Geheimnisse offenbart werden durften.[410] Teilweise wurde die Meinung vertreten, dass kein „Offenbaren" vorliegt, wenn eine Weitergabe zu reinen Verarbeitungszwecken erfolgt.[411] Die beiden letztgenannten Ansichten waren aber nicht in der Lage, eine hinreichende Eingrenzung vorzunehmen und die mit der Offenbarung verbundenen Risiken einzugrenzen.[412] Zugleich verstärkte sich mit zunehmender Arbeitsteilung z.B. im Medizinbereich unter Einbindung Externer immer mehr die Diskrepanz zwischen praktischer Notwendigkeit und normativer Festlegung. Diese rechtliche Diskrepanz ließ sich in der Praxis auch nicht mit der Einwilligung der Betroffenen aufheben.[413] Das Problem sollte mit dem „Gesetz zur Neuregelung des

406 BGH 10.02.2010 – VIII ZR 53/09, NJW 2010, 2511; Eisele in Schönke/Schröder, § 203 Rn. 5; Hauser/Haug, 32; Pohle/Ghaffari CR 2017, 490; Dochow, 817ff.

407 Roßnagel/Geminn in Dierks/Roßnagel, 232; Grosskopf/Momsen CCZ 2018, 98; Härting MDR 2018, 2.

408 Z.B. LG Flensburg 05.07.2013 – 4 O 54/11; Eisele in Schönke/Schröder, § 203 Rn. 25; Jandt/Roßnagel MedR 2011, 140ff.; Gödeke/Ingewersen VersR 2010, 1155; Kroschwald/Wicker CR 2012, 761; möglich wäre aber eine Arbeitnehmerüberlassung oder eine Anstellung auf Abruf, dazu Grosskopf/Momsen CCZ 2018,106; Pohle/Ghaffari CR 2017, 491.

409 Eisele JR 2018, 81, 86.

410 LBerufsG ZÄ Stuttgart 14.06.1975 – LQs 1/75, NJW 1975, 2255; Otto wistra 1999, 205; Heghmann/Niehaus NStZ 2008, 59; Jahn/Palm AnwBl 2011, 621; Kort NStZ 2011, 194; Schuster medstra 2015, 283f.; Ruppert StraFo 2016, 333ff.; Hartung VersR 2012, 408ff.; Lensdorf/Mayer-Wegelin/Mantz CR 2009, 64f.

411 Ziegler-Jung DuD 1980, 136; dagegen die h.M. BGH 10.08.1995 – IX 220/94, MDR 1005, 1169f = NJW 1995, 2916.

412 So auch die Bundesregierung in ihrer Gesetzesbegründung, BT-Drs. 18/11936, 18; zu dem früheren Meinungsstreit auch Fechtner/Haßdenteufel CR 2017, 357.

413 Roßnagel/Geminn in Dierks/Roßnagel, 228f.

Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“[414] behoben werden.

Die Notwendigkeit einer Ausweitung der Berufsgeheimnisse auf (IT-)Dienstleister, auf die über Jahre hinweg immer wieder fachlich hingewiesen wurde[415], hat 2017 dazu geführt, dass eine **Änderung des § 203 StGB** erfolgte. Das Offenbarungsrecht wird in § 203 Abs. 3 S. 2 StGB im Rahmen der Erforderlichkeit auf Dienstleister erweitert. Zugleich werden die „mitwirkenden Personen“ in § 203 Abs. 4 StGB im Fall eines durch sie bewirkten unbefugten Offenbarens mit Strafe bedroht.[416]

In diesem Kontext ist darauf hinzuweisen, dass mitwirkende Personen zur Geheimhaltung aufgrund **eines spezifischen Gesetzes** verpflichtet sein können (§ 203 Abs. 2 S. 1 Nr. 6 StGB). Derartige Verpflichtungen enthalten die §§ 476, 487 Abs. 4 StPO. Darin wird die Übermittlung von Akten oder sonstigen Daten aus der Strafverfolgung an Hochschulen, andere Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentliche Stellen für Forschungszwecke erlaubt und zugleich begrenzt. Außerdem sind gemäß § 16 Abs. 7 BStatG Personen, die statistische Einzelangaben vom Statistischen Bundesamt erhalten sollen, vor der Übermittlung zur Geheimhaltung zu verpflichten, soweit sie nicht Amtsträger oder Amtsträgerinnen oder für den öffentlichen Dienst besonders Verpflichtete sind. Das Verpflichtungsgesetz gilt entsprechend.[417] Danach kann eine Person, die nicht Amtsträger ist, förmlich zur gewissenhaften Erfüllung ihrer Obliegenheiten verpflichtet werden, was strafrechtliche Folgen im Fall der Pflichtverletzung zur Folge haben kann.[418] Derart können Personen, die keine öffentlichen Aufgaben wahrnehmen, in den Kreis besonders geschützter Geheimnisträger einbezogen werden.[419]

In der Gesetzesbegründung zur Änderung von § 203 Abs. 3, 4 StGB werden **Beispiele für „mitwirkende Tätigkeiten“** gegeben. Darunter fallen:

„Schreibarbeiten, Rechnungswesen, Annahme von Telefonanrufen, Aktenarchivierung und -vernichtung, Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art, Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten sowie Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers“.[420]

Ein zentraler Anwendungsfall soll die Datenverarbeitung in einer Cloud sein.[421] Der Katalog in der Gesetzesbegründung ist nicht abschließend.

414 G. v. 30.10.2017, BGBl. I S. 3618; zu den Positionen im Gesetzgebungsverfahren Fechtner/Haßdenteufel CR 2017, 360ff.
415 Nachweise bei Fechtner/Haßdenteufel CR 2017, 358, Fn. 37.
416 Momsen/Savić, KriPoZ 2017, 303.
417 Eisele in Schönke/Schröder, § 203 Rn. 95.
418 Verpflichtungsgesetz v. 02.03.1974, BGBl. I S. 469, 547, 1942.
419 Kubsch, Staats- und Kommunalverwaltung 1974, 279f.; § 31 Abs. 2 S. 2 EIRD sowie § 303e Abs. 4 S. 4 SGB V sehen nun auch die (entsprechende) Anwendung des Verpflichtungsgesetzes für forschende Datenempfänger vor.
420 BT-Drs. 18/11936, 22; Härting MDR 2018, 2.
421 Zu den weiteren Anforderungen Momsen/Savić, KriPoZ 2017, 302.

Das neue Gesetz will *„keinen möglichen Rechtsgrund, auf dem eine sonstige Mitwirkung beruhen kann, ausschließen"*.[422] Typischerweise wird ein Vertragsverhältnis bestehen. Notwendig ist die **Einbindung in die berufliche Tätigkeit** und das Einvernehmen hierüber mit dem Berufsgeheimnisträger. Diese soll sich nicht auf informationstechnische Aktivitäten beschränken, sondern umfassend Unterstützungsleistungen einbeziehen.[423] In Bezug auf externe Dienstleister für den öffentlichen Dienst (§ 203 Abs. 2 StGB) weist die Gesetzesbegründung darauf hin, dass ein Offenbarungsbedarf auch für Ausschuss- und Ratsmitglieder (Nr. 4) oder öffentlich bestellte selbstständige Sachverständige (Nr. 5) bestehen kann.[424]

Bei der **helfenden Tätigkeit** soll eine weite Auslegung möglich sein. Es genügt, dass die Gehilfen „in irgendeiner Weise" in den Umgang mit den Geheimnissen eingebunden sind. Obgleich die Digitalisierung das zentrale Motiv für die Gesetzesänderung war, erstreckt sich die zulässige Hinzuziehung auch auf „analoge" Tätigkeiten, etwa Übersetzungen oder das Erstellen von Gutachten.[425] Aufgrund eigenständiger Entscheidungsbefugnisse der Handelnden ist die Tätigkeit solcher Personen datenschutzrechtlich zumeist als Funktionsübertragung einzuordnen (s.o. Kap. 5.8).[426] Nicht dazu zählen sollen z.B. Pförtner, Hausmeister, Reinigungskräfte oder Fahrer.[427]

Auch bei einer **Mitwirkung an einer ärztlichen Forschungstätigkeit** ist eine weite Auslegung geboten. Die Mitwirkung muss sich nicht auf die Behandlungs- und Beratungstätigkeit des Arztes beziehen. Da zu den originären beruflichen Tätigkeitsbereichen eines Arztes auch dessen Forschungstätigkeit gehört, ist eine ausschließlich hierauf bezogene Tätigkeit eine hinreichende Legitimation für die Offenbarung von Patientengeheimnissen. Notwendig ist ein innerer Bezug der Tätigkeit der mitwirkenden Person zur Forschungstätigkeit.[428]

Durch die Neuregelung des § 203 StGB ist es möglich, dass auch **Treuhänder** zu Mitwirkenden des Arztes werden. Unterstützen diese den Arzt bei seiner forschenden Arbeit und sind die rechtlichen Voraussetzungen für die Mitwirkung gegeben[429], so unterliegen sie insofern auch der beruflichen Schweigepflicht. Dabei spielt es keine Rolle, ob die Treuhänder als Notar, Anwalt oder Arzt bzgl. ihrer originären Tätigkeit beruflich begründet schweigepflichtig sind. Eine solche sonstige berufliche Tätigkeit kann aber zusätzlich – nicht juristisch begründet – vertrauensfördernd sein. Sind die rechtlichen Voraussetzungen für eine Mitwirkung nicht gegeben, so kommt für öffentliche Stellen eine Verpflichtung nach dem Verpflichtungsgesetz in Betracht, um dem Treuhänder eine besondere Geheimnispflicht aufzuerlegen (s.o.).

§ 203 StGB unterscheidet zwischen (**internen**) **Gehilfen und sonstigen** (**externen**) **mitwirkenden Personen** dogmatisch dadurch, dass bei einer Mitteilung eines Geheimnisses an einen internen Gehilfen keine Offenbarung erfolgt, bei einer Mittei-

422 BT-Drs. 18/11936, 22f.; Eisele JR 2018, 83.
423 Grosskopf/Momsen CCZ 2018, 99.
424 BT-Drs. 18/11936, 19; dazu Eisele JR 2018, 83.
425 Eisele JR 2018, 83f.
426 Petri in Simitis, § 11 Rn. 28; Gola/Klug/Körffer in Gola/Schomerus, 12. Aufl. § 11 Rn. 11; Pohle/Ghaffari CR 2017, 492; Wronka RDV 2017, 130.
427 BT-Drs. 18/11936, 18; Roßnagel/Geminn in Dierks/Roßnagel, 236; Eisele JR 2018, 81; zur Offenheit der Regelung Dochow, 1346ff.
428 Roßnagel/Geminn in Dierks/Roßnagel, 239.
429 Siehe oben sowie weiter unten: Erforderlichkeit, Einbindung, Auswahl, Verpflichtung.

lung an einen externen Mitwirkenden dagegen eine rechtfertigungsbedürftige Offenbarung. Bei der Mitteilung an interne Gehilfen genügt es, dass diese im Rahmen der Berufsausübung stattfindet. Die Offenbarung an den Mitwirkenden ist nur zulässig, *„soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist"*.[430]

Es wird gefordert, dass die Tätigkeit, bei der ein Geheimnis zur Kenntnis genommen wird oder werden kann, erforderlich ist. Gegen diese Regelung ist aus Bestimmtheitsgründen nichts einzuwenden; eine präzisere Eingrenzung ist angesichts der vielfältigen möglichen Fallgestaltungen, die von der Neuregelung erfasst werden sollen, nicht möglich.[431] Die **Erforderlichkeit der Dienstleistung** setzt voraus, dass diese nicht ohne Kenntnis des fremden Geheimnisses durchgeführt werden kann. Bei der Feststellung der Erforderlichkeit muss eine Prüfung des konkreten Einzelfalls erfolgen. Es kann kein strenger Maßstab angelegt werden.[432] Es liegt in der Freiheit des forschenden Berufsgeheimnisträgers, seine Methoden selbst festzulegen. Hierzu gehört auch die Einbindung externer Unterstützung. Insofern genügt eine gesteigerte „Dienlichkeit".[433] Es ist zu unterscheiden zwischen der Erforderlichkeit der Dienstleistung und der Erforderlichkeit der Offenbarung. Die Dienstleistung ist erforderlich, wenn sie von dem Forschenden und seinem Team nicht erbracht werden kann und keine zumutbare Alternative besteht. Gründe dafür, dass die Leistung nicht erbracht werden kann, können in fehlenden materiellen oder kognitiven Ressourcen liegen. Der Geheimnisträger hat einen weitgehenden Ermessensspielraum.[434] Auch das Ziel der Kostenersparnis sowie Qualitäts- und Verfügbarkeitsgründe können eine Erforderlichkeit begründen, wenn diese Gründe erheblich sind.[435]

Hinsichtlich der **Erforderlichkeit der konkreten Offenbarungen** muss dagegen ein strenger Maßstab angelegt werden. Die Grundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) sind anwendbar, wobei wegen der Sensitivität der Daten besonders hohe Anforderungen zu stellen sind.[436] Verfügbare technische Mittel der Datenminimierung, etwa der Verschlüsselung oder der Ano- bzw. der Pseudonymisierung, sind einzusetzen.[437] Bei der Verarbeitung von Berufsgeheimnissen kommt hinzu, dass möglichst wenige Personen bei einem externen Dienstleister eingebunden werden.

Die Tätigkeit eines **externen Treuhänders** lässt sich als mitwirkende Tätigkeit im Rahmen eines medizinischen Forschungsprojektes ausgestalten, wenn dieses selbst unter dem Schutz des Berufsgeheimnisses steht. Die Erforderlichkeit sowohl der Einbindung des Treuhänders generell wie auch der einzelnen Offenbarungen bei der konkreten Umsetzung des Projektes lässt sich als technisch-organisatorische Maßnahme i.S.v. Art. 89 Abs. 1 DSGVO, §§ 27 Abs. 1, 22 Abs. 2 S. 2 BDSG einordnen.

430 Momsen/Savić, KriPoZ 2017, 302.
431 Härting MDR 2018, 3; Eisele JR 2018, 6; a.A. Fechtner/Haßdenteufel CR 2017, 360.
432 Ruppert K&R 2017, 612–613.
433 Strenger Grosskopf/Momsen CCZ 2018, 102.
434 Eisele JR 2018, 84.
435 Momsen/Savić, KriPoZ 2017, 301; weitergehend Pohle/Ghaffari CR 2017, 493, die die wirtschaftliche Beurteilung vollständig dem Berufsgeheimnisträger überlassen; ähnlich die Gesetzesbegründung BT-Drs. 18/11936, 17f.
436 Dochow, 1355ff. m.w.N.
437 Eisele JR 2018, 84f.; Weichert in DWWS, Art. 5 Rn. 48.

Die Berufsgeheimnisträger müssen die mitwirkenden Personen **sorgfältig auswählen** und die Zusammenarbeit sofort beenden, wenn die Einhaltung der gemachten Vorgaben nicht gewährleistet ist. Im Ausland ansässige Dienstleister oder von im Ausland erbrachte Dienstleistungen dürfen die Berufsgeheimnisträger nur in Anspruch nehmen, wenn der dortige Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist (s.u. Kap. 13).[438] Im Rahmen der Auswahl ist auf die fachliche Eignung und Zuverlässigkeit sowie auf sonstige Qualifikationsnachweise zu achten. Die Qualifikation muss sich auch auf die sichere Verarbeitung der Berufsgeheimnisse durch Ergreifen der nötigen technisch-organisatorischen Maßnahmen erstrecken.[439] Hierbei kann auf Zertifikate sowie auf persönliche Dokumente über die Aus- und Fortbildung sowie zu Qualifikationen zurückgegriffen werden. Ein Zertifikat nach Art. 42 DSGVO kann als Nachweis verwendet werden, wenn darin ausdrücklich die Geheimhaltung von Berufsgeheimnissen als Zertifizierungsgegenstand aufgenommen ist.[440] Bei sonstigen Nachweisen gilt dies ebenso.[441]

Unklar ist, inwieweit die Tätigkeit der mitwirkenden Personen durch den Berufsgeheimnisträger kontrolliert werden muss. Eine solche **Überwachung der mitwirkenden Personen** war im Referentenentwurf noch vorgesehen, wurde aber nicht Gesetz.[442] Berufsgeheimnisträger müssen eine Zusammenarbeit beenden, wenn die Einhaltung der dem Dienstleister gemachten Vorgaben nicht gewährleistet ist, also wenn der Dienstleister unbefugt Daten weitergibt oder sich Kenntnis von fremden Geheimnissen verschafft, die für die Vertragserfüllung nicht erforderlich ist. Auch wenn eine Kontrollpflicht nicht gesetzlich konkretisiert wurde, so besteht die Pflicht zu technisch-organisatorischen Maßnahmen, was durch ein „Managementsystem für Geheimschutz" umgesetzt wird. Eine gesetzliche Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ist ausdrücklich in Art. 35 DSGVO in den dort vorgesehenen Fällen vorgesehen. Diese konkretisiert sich bei medizinischen Forschungsprojekten in der Notwendigkeit der Erstellung eines Datenschutzkonzeptes, dessen Umsetzung regelmäßig überwacht werden muss (s.u. Kap. 11.4), wozu auch die Kontrolle der mitwirkenden Personen gehört.[443]

§ 203 Abs. 3 StGB legitimiert eine Mitteilung eines Berufsgeheimnisträgers an eine mitwirkende Person. Dies gilt generell für im Rahmen der Berufstätigkeit anvertraute Informationen. Doch können insofern materiell-rechtliche Einschränkungen gelten. Die wesentlichste Beschränkung besteht, wenn der Betroffene sein Anvertrauen **auf den Schweigepflichtigen persönlich beschränkt** hat. Generell kann davon ausgegangen werden, dass ein Anvertrauen alle mitwirkenden Personen miteinschließt. Sowohl aus einer expliziten Erklärung des Betroffenen wie auch durch die äußeren Umstände kann die „Einwilligung" an eine Mitteilung an Mitwirkende aber eingeschränkt oder gar völlig ausgeschlossen sein. Dies ist der Fall, wenn ein Patient im Rahmen eines Behandlungs- oder Beratungskontakts ausdrücklich darauf hinweist, dass die anvertraute Information nicht an Personen auch innerhalb des Behandlungs-

438 Grosskopf/Momsen CCZ 2018, 99–100.
439 Grosskopf/Momsen CCZ 2018, 99, 102.
440 Weichert in DWWS, Art. 42 Rn. 47.
441 Grosskopf/Momsen CCZ 2018, 101.
442 Grosskopf/Momsen CCZ 2018, 104; Pohle/Ghaffari CR 2017, 494.
443 A.A. Pohle/Ghaffari CR 2017, 494, die eine ausdrücklich gesetzliche Überwachungspflicht verlangen, wie sie z.B. in § 43e Abs. 2–5 BRAO oder in § 26a Abs. 2–5 BNotO geregelt ist.

und Beratungszusammenhangs weitergegeben werden darf. Auch ist es möglich, dass zwar der Mitteilung an Mitwirkende generell zugestimmt wird, hiervon aber ausdrücklich genannte Mitwirkende ausgeschlossen werden. Oder ein Patient besteht darauf, dass weitergehende Offenbarungen an mitwirkende Dritte nur durch den Berufsgeheimnisträger persönlich erfolgen und nicht durch Gehilfen.[444]

Rechtsfolge einer wirksamen Einbindung als mitwirkende Person ist, dass diese gemäß § 53a StPO ebenso wie die diese einbindenden Berufsgeheimnisträger zeugnisverweigerungsberechtigt ist. Über die Ausübung dieses Rechts entscheidet der Berufsgeheimnisträger. Es handelt sich um ein abgeleitetes **Zeugnisverweigerungsrecht**.[445]

6.7 Mitwirkung und Auftragsverarbeitung

Zentraler faktischer Anknüpfungspunkt für die Änderung des § 203 StGB war die Einbindung von IT-Dienstleistern in die Tätigkeit von Berufsgeheimnisträgern. Diese IT-Dienstleister sind regelmäßig als Auftragsverarbeiter gemäß Art. 28 DSGVO tätig, indem sie die informationsverarbeitenden Systeme der Berufsgeheimnisträger installieren, programmieren und administrieren und damit reine Hilfstätigkeiten ausüben. Es handelt sich auch dann um eine Auftragsverarbeitung, wenn bestimmte Formen der beruflichen **Datenverarbeitung „as a service"** ausgelagert werden, also die Datenspeicherung, der Betrieb einer Software oder gar der Betrieb einer komplexen Verarbeitungsinfrastruktur.[446]

Schon im klassischen Bereich der Berufsausübung können die **Anforderungen des Art. 28 DSGVO** nicht immer eingehalten werden. Dies gilt immer dann, wenn von der mitwirkenden Person derart komplexe Tätigkeiten bei der Datenverarbeitung notwendig werden, dass selbst abstrakte Weisungen nicht genügen, um die Aktivitäten des Auftragsverarbeiters zu dirigieren, und wenn diesem eigene wesentlich bestimmende Entscheidungen in Bezug auf die Art der Verarbeitung abverlangt werden. In diesem Fall ist datenschutzrechtlich Art. 28 DSGVO nicht mehr anwendbar. Es besteht entweder eine gemeinsame Verantwortlichkeit oder eine allein verantwortete Funktionsübertragung (s.o. Kap. 5.2–5.6, Kap. 5.8).

Für die berufsrechtliche Geheimhaltung kommt es auf diese **datenschutzrechtlichen Unterscheidungen** nicht an. Die Mitwirkung gemäß § 203 Abs. 3, 4 StGB kann als Auftragsverarbeitung oder als gemeinsame Verantwortlichkeit ausgestaltet sein. Eine Funktionsübertragung mit ausschließlicher Verantwortlichkeit des „Auftragnehmers" ist unwahrscheinlich, weil mit der Einbindung eines Dienstleisters ein gemeinsames Ziel verfolgt wird, das zumeist in der Datenverarbeitung liegt. Ist dies aber nicht der Fall, etwa wenn Berufsgeheimnisse für die Funktionswahrnehmung übertragen werden müssen, ohne dass eine weitere arbeitsteilige Verarbeitung erfolgt, so kommt selbst eine Funktionsübertragung in Betracht.

444 Eisele JR 2018, 86.

445 Neubeck in Kleinknecht/Müller/Reitberger, Kommentar zur Strafprozessordnung, Stand 2018, § 53a Rn. 3; Schmitt in Meyer-Goßner/Schmitt, Strafprozessordnung, 62. Aufl. 2019, § 53a Rn. 11.

446 Grosskopf/Momsen CCZ 2018, 99, 103.

Bei einer Auftragsverarbeitung ist ein Vertrag erforderlich (Art. 28 Abs. 3 DSGVO), bei dem ein Auftragnehmer zumeist als juristische Person vom verantwortlichen Auftraggeber verpflichtet wird. Erstreckt sich die Auftragsverarbeitung auf Berufsgeheimnisse, so muss eine rechtliche Bindung zwischen dem Berufsgeheimnisträger und der mitwirkenden Person hergestellt werden. Dies ist im Rahmen eines Vertrags nach Art. 28 Abs. 3 DSGVO möglich, wobei jedoch eine weitergehende Präzisierung der eingebundenen Personen erfolgen muss, die dann gemäß § 203 Abs. 4 S. 2 Nr. 2 StGB **persönlich zur Geheimhaltung zu verpflichten** sind.[447] Der Berufsgeheimnisträger muss für die Belehrung „Sorge tragen". Es genügt, dass die konkrete Geheimnisverpflichtung nicht durch ihn, sondern durch den Auftragnehmer oder im Fall einer Unterbeauftragung durch den Unterauftragnehmer erfolgt. Wird die Verpflichtung der mitwirkenden Person zur Geheimhaltung unterlassen, so macht sich der Verpflichtete strafbar, wenn der Mitwirkende gegen seine Geheimhaltungspflichten verstößt.[448] Dies gilt auch, wenn der Mitwirkende trotz der unterlassenen Verpflichtung seine eigene Schweigeverpflichtung kannte.[449] Eine formlose Verpflichtung genügt.[450] Aus Beweisgründen ist aber eine Dokumentation der erfolgten Verpflichtung sinnvoll. Bei wiederkehrenden Beauftragungen genügt eine einmalige Belehrung.[451] Keine ausdrückliche Geheimhaltungsverpflichtung per Vertrag muss erfolgen, wenn die sonstige mitwirkende Person selbst ein Berufsgeheimnisträger nach § 203 Abs. 1 oder 2 ist (§ 203 Abs. 4 S. 2 Nr. 1 StGB am Ende).

Erfolgt eine Unterbeauftragung durch den Auftragnehmer, so ist dies gemäß Art. 28 Abs. 4 DSGVO möglich, wobei die inhaltlichen Anforderungen der Auftragsverarbeitung sich von denen des Erstauftrags nicht unterscheiden. Werden beim **Unterauftragnehmer** Geheimnisse an Mitarbeitende offenbart, so kann auch diese Offenbarung nach § 203 StGB befugt sein, wenn bei den handelnden Personen die Anforderungen der § 203 Abs. 3, 4 StGB erfüllt sind. Mehrstufige Mitwirkungsverhältnisse sind möglich. Es bedarf nicht einer direkten Rechtsbeziehung zwischen Berufsgeheimnisträger und Unterauftragnehmer, wohl aber muss gewährleistet werden, dass die handelnden mitwirkenden Personen persönlich zur Geheinhaltung verpflichtet und insofern ein Weisungsrecht des Berufsgeheimnisträgers hergestellt wird. Eine lückenlose Weisungskette zwischen dem Berufsgeheimnisträger und der tatsächlich mitwirkenden Person ist nötig, nicht eine direkte Beziehung.[452]

Zum Verhältnis zwischen den neuen Regelungen zur Mitwirkung Externer bei der Berufsausübung von Schweigepflichtigen nach § 203 StGB und zur Auftragsverarbeitung nach Art. 28 DSGVO kann also festgehalten werden, dass sich bzgl. der Regelungsintentionen wie auch der Regelungsinhalte Art. 28 DSGVO und die Mitwirkungsregelungen in § 203 Abs. 3, 4 StGB unterscheiden:

- Während Art. 28 DSGVO sich auf **personenbezogene Datenverarbeitungen** beschränkt, erstreckt sich § 203 StGB weitergehend auch auf sonstige anvertraute Informationen, etwa Berufs- und Geschäftsgeheimnisse (s.o. Kap. 6.5).

447 Zu den Anforderungen an die Geheimhaltungsverpflichtung Grosskopf/Momsen CCZ 2018, 100.
448 Eisele in Schönke/Schröder, § 203 Rn. 101, 104; Eisele JR 2018, 86f.
449 Kritisch hierzu Eisele JR 2018, 87.
450 BT-Drs. 18/11936, 29.
451 Grosskopf/Momsen CCZ 2018, 100.
452 BT-Drs. 18/11936, 23; Pohle/Ghaffari CR 2017, 492; Eisele JR 2018, 84.

- Während in Art. 28 eine **juristische Person** als Auftragsverarbeiter verpflichtet wird, zielt § 203 auf die konkret mitwirkenden natürlichen Personen, die Mitarbeiter eines Auftragsverarbeiters sein können (s.o. Kap. 6.4).
- Während Art. 28 DSGVO **jede Form der Datenverarbeitung** im Auftrag nach Weisung legitimiert, ist § 203 StGB enger und gilt nur für solche Formen der Datenverarbeitung, die für die Berufsausübung erforderlich sind. Das Erforderlichkeitskriterium ist jedoch nicht streng anzuwenden.
- Die **Weisungsgebundenheit** bei Art. 28 DSGVO unterscheidet sich von der der Mitwirkung nach § 203 StGB: Bei der Auftragsverarbeitung besteht insbesondere in Bezug auf die technisch-organisatorischen Maßnahmen ein Ermessenspielraum für den Auftragsnehmer. Bei der Mitwirkung kann der Spielraum des Mitwirkenden bzgl. seiner Entscheidungsmacht größer sein und muss sich nicht auf reine Hilfstätigkeiten beschränken. Zwar werden dem Mitwirkenden von Schweigepflichtigen die Zwecke der Mitwirkung und damit regelmäßig auch der Datenverarbeitung vorgegeben, doch können insofern Entscheidungsspielräume verbleiben. Bei einer gemeinsamen Verantwortlichkeit kann der einzelne Verantwortliche die von ihm genutzten Mittel eigenständig bestimmen, muss hierüber aber den anderen Verantwortlichen lediglich Rechenschaft ablegen, damit diese hierfür die Verantwortung mit übernehmen können. Bei einer Mitwirkung nach § 203 StGB kann eine gemeinsame Verantwortlichkeit nach § 26 DSGVO gegeben sein kann. Eine gemeinsame Zweckfestlegung auf Forschungsfragestellungen durch den behandelnden Arzt und die Forschenden führt zu einer gemeinsamen Verantwortlichkeit, wobei die Einbindung der Forschenden von der Mitwirkungsregelung des § 203 StGB erfasst wird.

Ein gewisser Unterschied besteht zudem bei einer Auftragsverarbeitung mit **pseudonymen Daten**. Besteht die Möglichkeit der Reidentifizierung über den Auftraggeber, bleibt das Datenschutzrecht anwendbar. Demgegenüber ist keine Offenbarung nach § 203 StGB gegeben, wenn der Auftragnehmer selbst keine Identifizierung der verarbeiteten Datensätze vornehmen kann. Dies bedeutet, dass nicht auf die Mitwirkungsregelung in § 203 Abs. 3, 4 StGB zurückgegriffen werden muss, wenn der Auftragnehmer nicht über eine Zuordnungsfunktion verfügt. Dies gilt selbst, wenn bei der pseudonymen Datenverarbeitung wegen der generellen Zuordnungsmöglichkeit der Datensätze noch ein Personenbezug anzunehmen ist.[453]

6.8 Komplexe Mitwirkungsbeziehungen

Die ärztliche Behandlung von Patienten wird durch Arbeitsteilung und Digitalisierung zunehmend komplexer. Der **ärztlichen Leitung** kommt insofern eine koordinierende Funktion zu. Sie ist für den gesamten Komplex der individuellen medizinischen Behandlung federführend und damit auch verantwortlich für die Beachtung des Patientengeheimnisses bzw. der Schweigepflicht. Dieser Verpflichtung wird dadurch entsprochen, dass durch technisch-organisatorische Maßnahmen die Daten-

453 Fechtner/Haßdenteufel CR 2017, 357f.; Dierks in Dierks/Roßnagel, 64, unsicher Graf von Kielmansegg in TMF, 115; s.u. Kap. 10.3 am Ende.

verarbeitung der Behandlung abgeschottet wird. Mitwirkende Personen sind auf ihre Verschwiegenheitspflicht hinzuweisen (§ 203 Abs. 4 S. 2 Nr. 2 StGB). Die Kontrolle über die mitwirkenden Personen muss zumindest im Einzelfall gewährleistet sein. Eine solche hierarchische Strukturierung ist bei medizinischen Forschungsprojekten oft nicht möglich.

Medizinische Forschungsvorhaben setzen zudem oft voraus, dass große Datenbestände aus unterschiedlichen Quellen zusammengeführt werden. In der digitalen Agenda der Bundesregierung wird als ein Ziel formuliert, dass Wissenschaftler *„unkompliziert wissenschaftliche Informationen austauschen und über Ländergrenzen hinweg zusammenarbeiten"*.[454] Es geht also letztlich darum, Forschenden einen möglichst offenen Zugang (**Open Access**) zu relevanten Daten (Open Data) zu verschaffen. Die Forschenden sollen komplexe Analyse-Werkzeuge (Big Data Analytics) einsetzen können, um neue Erkenntnisse zu erlangen, ohne dass hierbei der Datenschutz und die Vertraulichkeitserwartungen der Betroffenen verletzt werden.[455]

Bei Kooperationen zwischen Krankenhäusern oder niedergelassenen Ärzten mit Forschungseinrichtungen erfolgt i.d.R. eine Offenbarung von Patientengeheimnissen. Hierfür bedarf es einer Offenbarungsbefugnis sowie einer datenschutzrechtlichen Legitimation. Die ärztliche Behandlungstätigkeit und eine Forschungstätigkeit erfolgen unabhängig voneinander. Unabhängige Forschung setzt ein weitgehendes selbstständiges Bestimmungsrecht der Leitung des Forschungsprojektes bzw. der Forschungseinrichtung voraus (s.o. Kap. 3.3). Damit nicht vereinbar wäre es, dass die Forschungsdaten anliefernden Ärzte ein Bestimmungsrecht über die Durchführung des Forschungsvorhabens in Anspruch nähmen. Als Legitimation für die Offenbarung bzw. Datenübermittlung bedarf es dann entweder einer **Einwilligung bzw. Schweigepflichtentbindung oder einer gesetzlichen Grundlage**.

Eine besondere Form der Kooperation kann in der **Personalüberlassung** liegen. Dabei stellt eine Forschungseinrichtung einer ärztlich geleiteten Stelle Mitarbeiter zur Verfügung, damit diese unter der ärztlichen Aufsicht Patientendaten sichten und auswerten, um diese dann als Originalunterlagen oder in ausgewerteter Form für das Forschungsvorhaben zur Verfügung zu stellen, also zu offenbaren bzw. zu übermitteln. Die Personalüberlassung wird gewählt, wenn der Daten haltenden, also hier der ärztlichen Stelle weder das Personal noch die sonstigen Ressourcen zur Verfügung stehen, um die Sichtung und Auswertung der Patientenunterlagen vorzunehmen.[456] Die Möglichkeit einer Personalüberlassung für Forschungszwecke kann ausdrücklich gesetzlich zugelassen sein.[457] Nach der Änderung des § 203 StGB bedarf es für eine Einschaltung externen Personals bei der Erfassung oder Auswertung von Behandlungsdaten nicht mehr einer ausdrücklichen Anstellung bei der ärztlich geleiteten Stelle. Möglich ist auch eine Beauftragung und Verpflichtung als externe mitwirkende Person.

454 Bundesregierung, Digitale Agenda 2014–2017 – Bildung, Forschung, Wissenschaft, Kultur und Medien, 2014, 27, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=3.

455 Schaar ZD 2016, 225f.; Thüsing/Rombey NZW 2019, 201f.

456 Landesbeauftragter für Datenschutz Schleswig-Holstein, 21. TB 1999, Kap. 4.9.4.; Landesbeauftragter für den Datenschutz Brandenburg, 6. TB 1998 (LT-Drs. 2/5253), 93; ausführlich Metschke/Wellbrock, 49–51.

457 So z.B. ehemals § 22 Abs. 2 LDSG SH v. 09.02.2000, GVOBl. 2000, 169.

Eine solche rechtliche Vorgehensweise ist aber problematisch, wenn sich die „Mitwirkung" nicht auf die Wahrnehmung der ärztlichen Aufgaben bezieht, sondern ausschließlich im Interesse der Forschungsauswertung eines Dritten erfolgt. Zwar legitimiert die neue Mitwirkungsregelung in § 203 StGB die Offenbarung von Patientengeheimnissen gegenüber einem Externen zur Unterstützung bei einer medizinischen Forschungstätigkeit. Davon nicht abgedeckt ist aber die Nutzung dieser Daten durch den **Externen für die eigene Forschung**. Die Offenbarungsbefugnis beschränkt sich auf das Erforderliche hinsichtlich der Unterstützung des berechtigten Berufsgeheimnisträgers. Ein eigenes Forschungsvorhaben des Mitwirkenden wird damit nicht mehr abgedeckt. Die Mitwirkung muss gemäß der Weisung des primär zur Geheimhaltung Verpflichteten erfolgen. An diesem Ergebnis ändert sich nichts, wenn der Mitwirkende selbst Arzt ist und nach § 203 Abs. 1 Nr. 1 StGB geheimhaltungspflichtig ist. Die Legitimation zu der Offenbarung liegt in diesem Fall nicht im beruflichen Status, sondern in der mitwirkenden Funktion.

Dem kann nicht entgegengehalten werden, dass mit der Forschungsnutzung keine neue Offenbarung erfolgt, weil der Datenumfang für die Forschung des Mitwirkenden nicht über den hinausgeht, den er als Mitwirkender am Forschungsprojekt des Arztes erlangt. Das Berufsgeheimnis schützt die Vertrauensbeziehung des beruflichen Helfers hinsichtlich der Hilfstätigkeit für den Betroffenen. Dieses Vertrauen wird verletzt, wenn mit den Daten Forschung durchgeführt wird, die nicht mehr unter der **Verantwortung des beruflichen Helfers** erfolgt.

Dem Berufsgeheimnisschutz liegt eine eigene **Zweckkomponente** inne. Diese liegt in der Wahrung der Vertraulichkeit im Rahmen des **Behandlungs- oder Beratungsverhältnisses**. Diese Zweckkomponente kann nicht durch eine allgemeine datenschutzrechtliche Zweckänderungsregelung aufgehoben werden. Art. 9 Abs. 3 DSGVO erlaubt zwar eine zweckändernde Nutzung sensitiver Daten, wenn der Nutzende nach nationalem Recht selbst einer Berufsgeheimnispflicht unterliegt. Diese Regelung ist aber nicht als eigenständige Zweckänderungsregelung zu verstehen, mit der weitere Zwecke der Datenverarbeitung zugelassen werden, sondern als Öffnungsklausel für den nationalen Gesetzgeber zur Erhöhung des Vertraulichkeitsschutzes.

Der deutsche Gesetzgeber hat in **§ 27 Abs. 1 BDSG** geregelt, dass eine Zweckänderung für die wissenschaftliche Forschung im Rahmen der Erforderlichkeit[458] erlaubt ist, wenn die Forschungsinteressen die Betroffeneninteressen *„erheblich überwiegen"* und wenn *„angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2"* BDSG vorgesehen werden. Damit soll die datenschutzrechtliche Privilegierung von Forschung gemäß der DSGVO nationalrechtlich umgesetzt werden.[459] Diese wird nach § 27 Abs. 3 BDSG auch auf sensitive Daten erstreckt, wenn eine frühestmögliche Anonymisierung erfolgt. Der deutsche Gesetzgeber hat von der Öffnungsklausel in der DSGVO zur Regelung von Berufsgeheimnissen Gebrauch gemacht. Nach § 1 Abs. 2 S. 2 BDSG finden Vorschriften Anwendung, für die das BDSG nicht abschließend ist. Gemäß § 1 Abs. 2 S. 3 BDSG bleibt die Verpflichtung zur Wahrung von Berufsgeheimnissen unberührt. Dies hat zur Folge, dass die in Deutschland geltenden Normen zu Berufsgeheimnissen parallel zum BDSG und zur

458 Zur Problematik des Begriffs der Erforderlichkeit Graf von Kielmansegg in TMF, 104ff.

459 Krohm in Gola/Heckmann, § 27 Rn. 13; Weichert in DWWS, § 27 BDSG Rn. 8; kritisch zum „erheblichen Überwiegen" schon Schneider 2015, 344f.

DSGVO anwendbar bleiben (Zwei-Schranken-Prinzip, s.o. Kap. 6.3).[460] Die Regelungen zum Patientengeheimnis sehen keine Aufhebung der Schweigepflicht für eigene Forschungsnutzungen des Mitwirkenden vor. Der Patient soll sich darauf verlassen können, dass die dem Arzt anvertrauten Daten zur Behandlung und Beratung verwendet werden und im Verfügungsbereich des Arztes verbleiben. Daher kann nicht auf § 27 BDSG als Legitimation für eine vom behandelnden Arzt unabhängige Forschungsnutzung zurückgegriffen werden.[461]

Anders ist der Fall zu behandeln, dass der mitwirkende Arzt zugleich **mitbehandelnder Arzt** ist und insofern direkt aus § 203 Abs. 1 StGB verpflichtet und als Offenbarungsempfänger (vgl. § 9 Abs. 4 MBOÄ) berechtigt ist. Die in dieser Funktion erlangten Daten darf er auch für eigene Forschungsaktivitäten nutzen.

6.9 Gemeinschaftsbetrieb

Der Schutz und der Austausch von Berufsgeheimnissen in einem medizinischen Forschungsprojekt lassen sich rechtlich dadurch realisieren, dass für das jeweilige Forschungsprojekt ein ärztlich geleiteter Gemeinschaftsbetrieb eingerichtet wird. Ein solcher gemeinsamer Betrieb besteht, *„wenn die in einer Betriebsstätte vorhandenen […] Betriebsmittel für einen einheitlichen arbeitstechnischen Zweck zusammengefasst, geordnet und gezielt eingesetzt werden und der Einsatz der menschlichen Arbeitskraft von einem einheitlichen Leitungsapparat gesteuert wird“*.[462] Nach § 1 Abs. 2 BetrVG wird ein gemeinsamer Betrieb mehrerer Unternehmen unter bestimmten Voraussetzungen vermutet. Die dort enthaltene Auflistung ist nicht abschließend. So besteht ein gemeinsamer Betrieb, wenn sich mehrere Unternehmen zur Führung eines gemeinsamen Betriebs rechtlich verbunden haben. Dies kann ausdrücklich, aber auch konkludent erfolgen. Dabei kommt es auf die tatsächlichen Umstände im Einzelfall an. Nicht nötig ist die Benutzung gemeinsamer Betriebsmittel oder ein Austausch der Beschäftigten. Relevant sind vor allem ein **einheitlicher Zweck und eine einheitliche Leitung** in personalen und sozialen Angelegenheiten.[463] Dabei können und müssen die beteiligten Unternehmen auch einen betrieblichen Zweck verfolgen; wichtig ist, dass im Gemeinschaftsbetrieb ein gemeinsames Ziel verfolgt wird. In diesem Fall wird ein abgrenzbarer Teil der jeweiligen unternehmerischen Tätigkeit ausgegliedert, wodurch jeweils neben dem eigenständigen Betrieb ein gemeinsamer Betriebszweck entsteht. Auf die konkrete Rechtsform kommt es nicht an. Diese arbeitsrechtliche Bewertung hat zur Folge, dass die im gemeinsamen Betrieb Beschäftigten als Gehilfen i.S.v. § 203 StGB behandelt werden können.[464]

Hinsichtlich der **datenschutzrechtlichen Einordnung** eines Gemeinschaftsbetriebs ist ausschlaggebend, dass dieser als Verantwortlicher eingestuft werden kann. Art. 4 Nr. 7 DSGVO lässt insofern einen weiten Spielraum, als er eine „juristische Person“ oder eine „Einrichtung oder andere Stelle“ zulässt. Damit können selbst nicht-rechtsfähige Vereine oder sonstige Vereinigungen wie z.B. eine BGB-Gesellschaft Verant-

460 Weichert in DWWS, § 1 BDSG Rn. 13f.; Dierks in Dierks/Roßnagel, 14.
461 Weichert in DWWS, § 27 Rn. 14.
462 BAG 11.02.2004 – 7 ABR 27/03, Rn. 14; NZA 2004, 618.
463 BAG 11.02.2004 – 7 ABR 27/03, Rn. 16, 25.
464 Grosskopf/Momsen CCZ 2018, 107.

wortliche sein.[465] Möglich wäre auch eine Festlegung durch nationales Recht.[466] Welche Art von personenbezogenen Daten verarbeitet wird, ist unerheblich; so können also auch sensitive Daten, also z.B. genetische oder medizinische Daten, verarbeitet werden.

Ein Gemeinschaftsbetrieb kann sowohl als privatrechtliches wie auch als öffentlich-rechtliches Unternehmen geführt werden. Aus berufs-, arbeits- und datenschutzrechtlicher Sicht möglich ist selbst eine Kooperation von **öffentlichen und privaten Stellen**. Die datenschutzrechtliche Einordnung als öffentliches oder privates Unternehmen richtet sich nach § 2 Abs. 3 BDSG. Danach handelt es sich um eine öffentliche Stelle des Bundes, wenn diese über den Bereich eines Landes hinaus tätig ist und dem Bund die absolute Mehrheit der Anteile oder der Stimmen zusteht.[467]

465 Petri in SHS, Art. 4 Nr. 7, Rn. 16; Hartung in Kühling/Buchner, Art. 4 Nr. 7, Rn. 9; Raschauer in Sydow, Art. 4 Rn. 131; Schwartmann/Mühlenbeck in SJTK, Art. 4 Rn. 115.

466 Klabunde in Ehmann/Selmayr, Art. 4 Rn. 37.

467 Weichert in DWWS, § 2 Rn. 11; zum insofern kompatibel zu gestaltenden Landesrecht Schulz in Gola/Heckmann, § 2 Rn. 29f.

7 Die Rolle der Einwilligung

Informationelle Selbstbestimmung bedeutet, selbst bestimmen zu können, wer was wann bei welcher Gelegenheit über einen weiß. Hierauf hat jeder Mensch ein Recht. Dieses Recht wird dadurch realisiert, dass der Mensch selbst Informationen über sich offenbart oder dass er Dritten erlaubt, Informationen über ihn zu sammeln und weiterzuverarbeiten. Informationelle Selbstbestimmung wird eingeschränkt, wenn ohne eine solche willentliche Entscheidung des Betroffenen Informationen über ihn erhoben und verarbeitet werden. Dies bedarf seit der Volkszählungsentscheidung des BVerfG in jedem Fall einer gesetzlichen Grundlage, die im allgemeinen Interesse steht. Dieses Interesse muss gegenüber dem Selbstbestimmungsinteresse des Betroffenen überwiegen. Demgemäß sieht Art. 6 Abs. 1 UAbs. 1 DSGVO vor, dass eine Verarbeitung personenbezogener Daten nur rechtmäßig ist, wenn der Betroffene seine Einwilligung hierzu erteilt (lit. a), dieser einen Vertrag abschließt, wozu die Verarbeitung nötig ist (lit. b), oder wenn bestimmte gesetzlich definierte Voraussetzungen vorliegen (lit. c bis lit. f).

Der datenschutzrechtlichen Einwilligung kommt somit eine wichtige Bedeutung dafür zu, eine personenbezogene Datenverarbeitung zu legitimieren. Mit ihr geht keine Einschränkung der informationellen Selbstbestimmung einher; sie ist vielmehr eine Form von deren **praktischer Umsetzung**.[468] Was datenschutzrechtlich unter einer Einwilligung zu verstehen ist, wird in Art. 4 Nr. 11 DSGVO definiert:

468 Weichert in DWWS Art. 4 Rn. 102.

> *„Einwilligung" der betroffenen Person (ist) jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".*

Voraussetzung einer wirksamen Einwilligung sind also **Freiwilligkeit, Informiertheit und Willensbetätigung**.[469] Die konkreten Anforderungen hieran werden in Art. 7 DSGVO formuliert. Die Einwilligung soll sicherstellen, dass die Datenverarbeitung den Werten und Präferenzen der Betroffenen entspricht.[470]

Soll sich eine Datenverarbeitung auf **besondere Kategorien personenbezogener Daten** beziehen, so ist es gemäß Art. 9 Abs. 2 lit. a DSGVO nötig, dass der Betroffene hierin „ausdrücklich eingewilligt" hat. Solche sog. sensitive Daten sind gemäß Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Aus datenschutzrechtlicher Sicht gibt es keine materiell-rechtlichen Differenzen zwischen einer Einwilligung nach **europäischem und nationalem Recht**. Art. 7 DSGVO ist für die Mitgliedstaaten verbindlich.[471] Unterschiede kann es nur geben, soweit von einer Einwilligung nicht nur die Erlaubnis zur Datenverarbeitung, sondern zu weiteren Maßnahmen gewährt wird, so wie dies zu körperlichen Eingriffen im Rahmen der ärztlichen Behandlung oder bei klinischen Studien der Fall sein kann (s.u. Kap. 7.2). Nationale Sonderwege kann es auch geben, um Einwilligung auszuschließen oder prozedural einzuschränken (vgl. Art. 9 Abs. 2 lit. a DSGVO).

Bei medizinischen Forschungsprojekten werden i.d.R. sensitive Daten gemäß Art. 9 Abs. 1 DSGVO verarbeitet. Sollen diese dort auf Grundlage einer Einwilligung verarbeitet werden, so muss sich diese auf diese Datenart „ausdrücklich" beziehen. Bei der **ausdrücklichen Einwilligung** muss für den Betroffenen eindeutig erkennbar sein, dass eine Verarbeitung solcher sensitiven Daten erfolgen soll. Ein erhöhtes Maß an Bestimmtheit und Präzision wird gefordert. Dies kann durch Erwähnung der Datenart erfolgen. Möglich ist auch, dass die Sensitivität aus dem Kontext offensichtlich erkannt wird.[472]

469 EDPB, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, zur Freiwilligkeit S. 8ff, zur Bestimmtheit S. 15f., zur Informiertheit S. 17ff.

470 Datenethikkommission, 126.

471 Klement in SHS, Art. 7 Rn. 14; Heckmann/Paschke in Ehmann/Selmar, Art. 7 Rn. 29f; Schwartmann/Klein in SJTK, Art. 7 Rn. 51; Kramer in Auernhammer, Art. 7 Rn. 33; Schulz in Gola, Art. 7 Rn. 18; zur Widerruflichkeit der Einwilligung im AMG-Kontext Bischoff/Wiencke ZD 2019, 9f.

472 EDPB, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, 23ff.; Petri in SHS, Art. 9 Rn. 33; Weichert in Kühling/Buchner, Art. 9 Rn. 47; Kühling, 49.

7.1 Datenschutzeinwilligung und Schweigepflichtentbindung

Mit der Verarbeitung von **Gesundheitsdaten** ist oft eine Offenbarung des Patientengeheimnisses, also eines Berufsgeheimnisses, verbunden. Es war vor dem Wirksamwerden der DSGVO im nationalen Recht anerkannt, dass insofern standes- bzw. medizinrechtlich begründet – anders als bei den strengeren Anforderungen im Datenschutzrecht – in engen Grenzen auch eine konkludente Einwilligung als Legitimation ausreichen kann.[473] An dieser Rechtslage ändert sich durch die DSGVO nichts.

Die Datenschutzeinwilligung und die Schweigepflichtentbindung können in einer **einheitlichen Erklärung** abgegeben werden. Diese muss den jeweiligen rechtlichen Anforderungen genügen, wenn sowohl eine datenschutzrechtliche Legitimation wie auch die Erlaubnis zu einer Offenbarung erteilt werden soll.[474]

7.2 Einwilligung in medizinische Forschung

Sämtlichen **nationalen Regelungen** zur Forschung ist in Deutschland gemein, dass eine Datennutzung ohne Einwilligung der Betroffenen nur im Ausnahmefall nach einer Güterabwägung erlaubt sein kann. Vorrang hat die Legitimation durch eine Einwilligung.[475] Dieser Grundsatz folgt dem Wunsch, dass der Betroffene idealerweise selbst bestimmen soll, wer worüber mit seinen Daten forschen darf.

In der medizinischen Forschung kommt das Prinzip der Selbstbestimmung mit der Anforderung an eine informierte Einwilligung („**informed consent**") zum Ausdruck. Eine wichtige Grundlage für diese international akzeptierte Anforderung wurde mit dem Nürnberger Kodex von 1947 gelegt, wo in Nr. 1 die freiwillige Einwilligung der Versuchsperson bei medizinischer Forschung unbedingt gefordert wird.[476] Darauf aufbauend verlangt die Deklaration von Helsinki des Weltärzteverbands[477] aus dem Jahr 1964 die informierte Einwilligung zur Nutzung identifizierbaren Materials oder von solchen Daten bei der medizinischen Forschung. Die ärztlichen Berufsordnungen verweisen in ihren Forschungsklauseln (vgl. § 15 Abs. 3 MBOÄ) auf die Deklaration und integrieren diese damit in das Berufsrecht.[478] Der Europarat nahm 1997 die Bioethikkonvention an, in der in Art. 5 grundsätzlich die informierte Einwilligung des Betroffenen als Legitimation eingefordert wird.[479]

473 Hauser/Haag, 8 f; Kircher in Kingreen/Kühling, 219 f.; Blobel/Koeppe, Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 39ff.; Buchner in Buchner, Datenschutz im Gesundheitswesen, Stand 2019, A/2, 5: „mutmaßliche Einwilligung".

474 Weichert in Kühling/Buchner, Art. 9 Rn. 49.

475 In den allgemeinen Datenschutzgesetzen ist damit keine ausdrückliche Offenbarungsbefugnis verbunden.

476 Nachweis unter http://www.ippnw-nuernberg.de/aktivitaet2_1.html.

477 World Medical Association's Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects, zuletzt geändert 2013, No. 25–32, aktuelle Version abrufbar unter https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/, deutsch unter https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/International/Deklaration_von_Helsinki_2013_20190905.pdf.

478 Graf von Kielmansegg in TMF, 115.

479 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Nachweise unter https://www.humanrights.ch/de/internationale-menschenrechte/europarat-abkommen/biomedizin/.

Die notwendige Information vor Erteilung der Einwilligung enthält sowohl eine **informationelle wie eine medizinische Komponente**. Die informationelle Seite bezieht sich auf Zweck, Verantwortliche, verwendete Daten und deren Verwendung. Aus medizinischer Sicht ist zusätzlich über Risiken und mögliche Schäden zu informieren.[480] Die datenschutzrechtliche Einwilligung ist aus rechtlicher Sicht von der medizinrechtlichen Einwilligung zu unterscheiden.[481] So geht die Einwilligung in die Teilnahme an einer klinischen Prüfung über die in die hierbei stattfindende Datenverarbeitung hinaus.[482] Da sie sich aber inhaltlich gegenseitig widerspruchsfrei ergänzen, können sie in einer Erklärung erteilt werden.

Das Kernprinzip der **informationellen Selbstbestimmung** durch Einwilligung kann nicht uneingeschränkt realisiert werden. In Zivilgesellschaften ist stets eine Balance zwischen individuellen und gemeinschaftlichen Belangen zu wahren. Im überwiegenden Allgemeininteresse müssen Abweichungen zulässig sein, wobei es allerdings (gesetzlicher) Regeln bedarf, welche die Wahrung der Verhältnismäßigkeit garantieren. Insofern sind im Zuge einer (Neu-)Regulierung der Nutzung von (medizinischen) Daten für Forschungszwecke organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die einer Verletzung von Persönlichkeitsrechten effektiv vorbeugen und das Fehlen einer Einwilligung kompensieren können.[483]

Zur Einwilligung in medizinische Forschung äußert sich **ErwGr 33 zur DSGVO**:

> *„Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen."*

Diese Ausführungen sollen nicht die Informiertheit der Einwilligung einschränken, sondern bestätigen die Zweckprivilegierung der Forschung nach Art. 5 Abs. 1 lit. b DSGVO (s.u. Kap. 8.2). ErwGr 33 DSGVO befreit nicht von einer möglichst umfassenden Aufklärung, wie sich dort aus Satz 3 ergibt.[484]

Eine wirksame Einwilligung bzw. Schweigepflichtentbindung setzt voraus, dass sie informiert erfolgt, d.h. auf hinreichend präzisen Informationen darüber basiert, welche Stelle für welche Zwecke mit welchen Daten forschen können soll. Die Unbestimmtheit eines wissenschaftlichen Verarbeitungszwecks kann teilweise dadurch kompensiert werden, dass die Betroffenen abgestufte Einwilligungen erteilen (tiered consent) oder während der Nutzung ihrer Daten regelmäßig oder auf Nachfrage über aktuelle und geplante Forschungsprojekte informiert werden (dynamic consent).[485]

480 Ausführlich EDPS 2020, 13–16.
481 EDSA, 6; EDPS 2020, 19f.
482 Bischoff/Wiencke ZD 2019, 9.
483 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 (LS 2).
484 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DS-GVO v. 04.04.2019; Schiff in Ehmann/Selmayr, Art. 9 Rn. 34.
485 EDPS 2020, 14, 20; Datenethikkommission, 126; Deutscher Ethikrat, 122ff., 178 (B2)

Mehrebenen-Datenschutzerklärungen erlauben eine Anpassung der Betroffeneninformation und Willenserklärung an spezifische, evtl. erst nachträglich auftretende Verarbeitungsnotwendigkeiten.[486]

Differenzierte und zeitlich abgestufte Einwilligungen lassen sich mit Privacy Management Tools (PMT) oder Personal Information Management Systems (PIMS) realisieren, mit denen für die Betroffenen in Form von **digitalen Einwilligungsassistenten** oder eines Datencockpits ein hohes Maß an Transparenz hergestellt und zugleich die Möglichkeit eröffnet wird, im Sinne von Opt-in und Opt-out Nutzungsermächtigungen zu erteilen bzw. zu entziehen.[487] Praktische Erfahrungen mit diesen Ansätzen fehlen jedoch noch weitgehend.

Aus den nachstehenden Gründen fehlt aber eine **klare Information** bei Medizinforschung oftmals.[488]

Medizinische Daten bilden ebenso wie Biomaterialien eine **dauerhafte Erkenntnisquelle** für die Forschung, die nur selten ihren wissenschaftlichen Wert vollends verliert. Viele wissenschaftliche Fragestellungen, die sich mit Daten und Biomaterial bearbeiten lassen, sind zum Erhebungs- bzw. Gewinnungszeitpunkt noch gar nicht genau bekannt. Im Laufe der Forschungsarbeiten können sich neue Fragestellungen ergeben, die ursprünglich ebenso wenig absehbar waren wie die Identität der Einrichtungen, die für die Bearbeitung dieser Fragestellungen am besten qualifiziert und geeignet wären.[489]

Ändern sich die **Rahmenbedingungen der Datenverarbeitung**, etwa durch rechtliche oder ökonomische Veränderungen beim Verantwortlichen oder durch die Einbeziehung weiterer Stellen, so ist u.U. eine erneute Einwilligung einzuholen, weil die ursprüngliche Einwilligung die Änderungen nicht mit einschließt. Dies kann schwierig bis praktisch unmöglich sein, etwa wenn die Betroffenen nicht mehr erreichbar sind.[490]

Wegen der Unbestimmtheit der angestrebten Datenverarbeitung werden im Kontext der medizinischen Forschung zunehmend Einwilligungen erbeten, die sehr umfassend und allgemein formuliert sind. Es ist zweifelhaft, ob derartige Einwilligungen (sog. **broad consent**) noch als „informiert" gelten können und die Funktion einer wirksamen Erlaubnis zur Verarbeitung persönlicher Daten erfüllen.[491] Voraussetzung ist in jedem Fall, dass weitere technische, organisatorische und prozedurale Vorkehrungen getroffen werden.[492] Dies gilt insbesondere für Einwilligungen, die sich in ihrer Unbestimmtheit auch auf ethische „Randzonen" (z.B. militärische Forschung

486 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 9, 13f., 23ff.

487 Datenethikkommission, 126ff.; Graf von Kielmansegg in TMF, 99f.; Wiebe, 538, 550f.; Kollmar/El-Auwad K&R 2021, 77f.; Martini/Hohmann NJW 2020, 3575; vgl. das nun in § 10 Onlinezugangsgesetz vorgesehene Datencockpit für den Einsatz einer nationalen Identitätsnummer; zum Forschungsnutzungskonzept bei der elektronischen Patientenakte Sachverständigenrat, 90ff., 127.

488 Graf von Kielmansegg in TMF, 100f.

489 GMDS, 9f.; Deutscher Ethikrat, 121.

490 Fechtner/Haßdenteufel CR 2017, 356.

491 Datenethikkommission, 126; Dierks in Dierks/Roßnagel, 47; Wiebe, 537; Zenker/Krawczak/Semler in TMF, 42; zum Einsatz in der Medizininformatik-Initiative Streck in TMF, 62f.; Graf von Kielmansegg in TMF, 93ff.

492 Beschluss der DSK v. 15.04.2020 zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung.

oder Human Enhancement) erstrecken.[493] Die Datenschutzaufsichtsbehörden weisen ausdrücklich darauf hin, dass die DSGVO für Forschung keine geringeren Anforderungen an die Einwilligung stellt als in anderen Bereichen. Die Anforderungen der Art. 4 Nr. 11, 6 Abs. 1 lit. a, 7, und 9 Abs. 2 lit. a DSGVO sollen uneingeschränkt anwendbar sein. Je geringer die Möglichkeit einer Zweckspezifizierung ist, umso höhere Anforderungen sind an kompensierende Sicherungsmaßnamen zu stellen.[494]

- Auch der Einsatz von **tiered oder dynamic consent** ist oft nicht umsetzbar, z.B. wenn sich die Erreichbarkeit der Betroffenen ändert, die Komplexität der Verarbeitung zu hoch ist, die Mitteilung der Informationen das Recht auf Nichtwissen der Betroffenen verletzt, oder ein laufender Kontakt mit Forschenden entweder zu aufwändig oder aus fachlicher Sicht abträglich ist.

Bei einer **großen Zahl von Betroffenen** ist das Einholen spezifizierter Erklärung oft nicht praktikabel.[495] Bei einer ungenügenden Rücklaufquote kann die Repräsentativität des Forschungsprojektes beeinträchtigt sein. Dieses Defizit lässt sich nur beschränkt dadurch ausgleichen, dass statt des Einzelnen die Öffentlichkeit als Ganzes informiert wird und die Betroffenen auf die Möglichkeit der Wahrnehmung eines Widerrufsrechts für spezielle Forschungsfragen hingewiesen werden. Ein derartiges Opt-out entspräche auch nicht mehr den Anforderungen an eine datenschutzrechtliche Einwilligung.[496]

Werden Forschungsdaten anonymisiert, so entfallen die Notwendigkeit und die Möglichkeit einer informationellen Selbstbestimmung. Eine Löschung des Personenbezugs steht aber in vielen Fällen den Forschungsinteressen entgegen, da z.B. **Langzeitstudien** eine fortlaufende Zuordnung neuer Daten zu bereits vorhandenen Daten erfordern. Langzeitstudien sind für die medizinische Forschung unerlässlich, da die Wirksamkeit von Therapien und Umweltfaktoren oft erst nach Jahren feststeht.[497]

Bei **Biomaterialien** und genetischen Daten besteht wegen der darin enthaltenen Erbinformation ein inhärenter Personenbezug. Ihre unumkehrbare Anonymisierung ist daher unmöglich. Eine Einwilligung in ihre Nutzung ist wegen der bisher kaum zu erfassenden Aussagekraft und der sich daraus ergebenden Analysierbarkeit prospektiv kaum möglich. Wohl aber lassen sich die persönlichkeitsrechtlichen Risiken beim Umgang mit genetischen Daten durch den geschickten Einsatz von Pseudonymen und die abgeschottete und kontrollierte Verarbeitung der Daten maßgeblich reduzieren.[498]

Häufig lässt sich das wissenschaftliche Potenzial von Gesundheitsdaten nur durch eine einrichtungsübergreifende (möglicherweise weltweite) Zusammenführung der Daten angemessen ausschöpfen, insbesondere bei der Erforschung seltener Erkran-

493 Graf von Kielmansegg in TMF, 97

494 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DS-GVO v. 04.04.2019; EDPS 2020, 19; Dierks 2019, 57f.; siehe hierzu den „Mustertext zur Patienteneinwilligung" der Medizininformatik-Initiative, www.medizininformatik-initiative.de; gebilligt von den Landesdatenschutzaufsichtsbehörden am 16.04.2020; Beschluss der DSK vom 15.04.2020 zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung.

495 Pohle/Ghaffari CR 2017, 490.

496 EuGH 01.10.2019 – C-673/17 (Planet 49) Rn. 62–65, NJW 2019, 3433.

497 RfII, 4.

498 Weichert/Krawczak MIBE 2019, Vol. 15(1), 4f./8.

kungen. Eine solche Zusammenführung ist bereits heute leicht über Forschungsnetzwerke oder Krankheitsregister[499] realisierbar. Allerdings gibt es hierfür, abgesehen von den Spezialfällen der Krebsregistergesetze[500] und des Implantateregisters[501], keine expliziten gesetzlichen Grundlagen. Die Rechtmäßigkeit der Datennutzung gründet vielmehr allein auf der Einwilligung der Betroffenen, jedoch mit dem Vorbehalt, dass zum Zeitpunkt der Einwilligung Art und Umfang der **Datenzusammenführung meist völlig unbekannt** sind.[502]

Ein weiteres grundsätzliches Problem bei der Einholung von Einwilligungen im medizinischen Bereich betrifft die **Freiwilligkeit**. Diese ist unabdingbare Voraussetzung für die Wirksamkeit einer selbstbestimmten Erklärung. Wird die Einwilligung für Forschungszwecke im räumlichen, personellen und zeitlichen Zusammenhang mit der ärztlichen Beratung und Behandlung eingeholt, so kann dadurch die Selbstbestimmung des Patienten eingeschränkt sein. Der Patient kann den Eindruck haben, dass eine Verweigerung seiner Einwilligung einen Einfluss auf die Qualität der ärztlichen Leistung hat. Zugleich kann die Anforderung einer Einwilligung das Vertrauensverhältnis zwischen Arzt und Patient beeinträchtigen, wenn der Patient den Eindruck hat, dass nicht die Behandlung, sondern die Forschung für den Arzt handlungsbestimmend ist.[503]

Angesichts der bestehenden nationalen gesetzlichen Regelungen, die einen Vorrang der Einwilligung festlegen, und der praktischen Anforderungen an die Durchführung medizinischer Forschung wurden mit Datum vom 16.04.2020 von der **Medizininformatik-Initiative** (MII) national harmonisierte Einwilligungsdokumente zusammen mit einer „Handreichung zur Anwendung der national harmonisierten Patienteninformations- und Einwilligungsdokumente zur Sekundärnutzung" vorgelegt. Mithilfe dieser Dokumente wird an den Universitätskliniken in Deutschland eine nicht projekt- und stellengebundene „breite Einwilligung" (broad consent) als Grundlage für eine Forschungsnutzung von Patientendaten umgesetzt, die flankiert wird von Prozessen und Regularien, mit denen ergänzend Garantien für die Wahrung der Betroffenenrechte geschaffen werden.[504] Die deutsche Datenschutzkonferenz (DSK) hat hierzu am 21.04.2020 einstimmig beschlossen, dass unter den vorgelegten Rahmenbedingungen „keine Bedenken" gegen die Verarbeitung von genetischen und Gesundheits-Daten bestehen.[505] Eine Feststellung der formellen Rechtmäßigkeit ist mit dem Beschluss nicht verbunden. Über die vorgesehenen umfassenden Garantien kann in

499 Bizer, 371ff.; Sachverständigenrat, 214ff., 246ff.; Zenker/Krawczak/Semler in TMF, 34ff.

500 Bizer, 377ff.

501 BfDI, TB 2020, Kap. 7.3 (S. 68f.).

502 Zur Einwilligungsproblematik ebenso Weichert/Krawczak MIBE 2019, Vol. 15(1), 4/8.

503 Dochow, 718–735; Schneider 2015, 113.

504 AG Consent des Nationalen Steuerungsgremiums der MII des BMBF, 16.04.2020, https://www.datenschutzkonferenz-online.de/media/pm/MII_AG-Consent_Handreichung_v0.9d.pdf; siehe zur medizinwissenschaftlichen, ethischen und rechtlichen Begründung TMF.

505 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung, 15.04.2020, https://www.datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf, zugehörige Pressemitteilung der Konferenz https://www.datenschutzkonferenz-online.de/media/pm/20200427_Einwilligungsdokumente_der_Medizininformatik-Initiative.pdf.

der Praxis ein Rahmen geschaffen werden, der den materiellen Schutz der Gesundheitsdaten sichert.[506]

Die obigen Erwägungen zeigen, dass eine Einwilligung für die medizinische Forschung eine valide Grundlage für die Datenverarbeitung sein kann. Es gibt aber eine Vielzahl von Fallgestaltungen, in denen ein öffentliches Interesse und ein überwiegendes berechtigtes Interesse an einer Forschungsnutzung bestehen können und eine **informierte Einwilligung nicht möglich** ist, weil sie nicht eingeholt oder auch nicht gefordert werden kann.[507]

7.3 Einwilligung versus gesetzliche Rechtsgrundlage

Datenschutzrechtlich ungeklärt und umstritten ist die Frage, inwieweit Rechtsgrundlagen für eine Datenverarbeitung ausgetauscht werden dürfen. Diese Frage wird insbesondere relevant, wenn eine Datenverarbeitung auf eine Einwilligung gegründet wurde und diese sich **nachträglich als nicht** (**mehr**) **gültig erweist**. Diese Ungültigkeit kann ihren Grund darin haben, dass die Einwilligung von Anfang an unwirksam war oder dass der einwilligende Betroffene seine Einwilligung widerruft. Gerade bei komplexen Datenverarbeitungsvorgängen, wie sie gerade auch in der Forschung vorkommen können, kann die Wirksamkeit der Einwilligung an der geforderten Freiwilligkeit und Informiertheit scheitern.[508] In solchen Fällen kann die Verarbeitung möglicherweise durch eine sonstige Rechtsgrundlage gestützt sein, die zur Datenverarbeitung verpflichtet oder zumindest hierzu – nach einer Interessenabwägung – berechtigt. Mit einem solchen Wechsel der Rechtsgrundlage wird das Vertrauen des Betroffenen, über die Verarbeitung seiner selbst bestimmen zu können, tendenziell beeinträchtigt.[509]

Art. 6 Abs. 1 UAbs. 1 DSGVO verlangt für die Rechtmäßigkeit einer Verarbeitung, dass *„mindestens eine der nachstehenden Bedingungen erfüllt ist"*, und zählt dann nebeneinander die Einwilligung (lit. a) sowie gesetzliche Verarbeitungsbefugnisse auf, u.a. die Wahrnehmung einer Aufgabe im öffentlichen Interesse (lit. e) und die Verarbeitung auf der Grundlage einer Interessenabwägung (lit. f). Gemäß Art. 17 Abs. 1 lit. b DSGVO ist ein Anspruch auf Löschung nur begründet, wenn es *„an **einer anderen Rechtsgrundlage** für die Verarbeitung fehlt"*.

Die Einwilligung ist in besonderem Maße Ausdruck informationeller Selbstbestimmung. Der Betroffene erklärt in Ausübung seines Bestimmungsrechts, wer welche Daten über ihn zu welchem Zweck wie verarbeiten darf. Um dieses Bestimmungsrecht zu wahren, steht es dem Betroffenen frei, seine Einwilligung mit Wirkung für die Zukunft zu widerrufen (Art. 7 Abs. 3 S. 1 DSGVO). Ein solcher Widerruf ist gemäß der Regelung im Grunde jederzeit möglich, auch wenn dadurch die Interessen des Verantwortlichen, etwa eines Forschenden, beeinträchtigt werden. Art. 7 DSGVO lässt **für eine Interessenabwägung keinen Raum**.[510]

506 Netzwerk Datenschutzexpertise, 7f.
507 In Bezug auf klinische Studien EDSA, 8f. (Rn. 25–28).
508 Kollmar/El-Auwad K&R 2021, 75ff.
509 Dochow, 705ff. m.w.N.
510 Klement in SHS Art. 7 Rn. 91; LNK § 2 Rn. 14; Wybitul ZD 2016, 205.

Vor Wirksamwerden der DSGVO hat das BAG demgegenüber geurteilt, dass ein Einwilligungswiderruf im Arbeitsverhältnis nicht gegen Treuepflichten verstoßen dürfe und wegen § 241 Abs. 2 BGB (vgl. auch § 242 BGB) im Einzelfall eine Interessenabwägung vorzunehmen sei.[511] Diese Entscheidung ist zwar auf den Widerruf einer Forschungseinwilligung nach der DSGVO nicht direkt übertragbar, da ein Rückgriff auf nationale Regelung nicht mehr möglich ist. Doch ist auch nach europäischem Recht bei der Datenverarbeitung der **Grundsatz von Treu und Glauben** gemäß Art. 8 Abs. 2 S. 1 GRCh sowie Art. 5 Abs. 1 lit. a DSGVO anzuwenden.[512] Dieser Grundsatz richtet sich vorrangig an die Daten verarbeitende Stelle, doch ist nicht erkennbar, dass eine Verpflichtung des Betroffenen durch und eine Berufung des Verantwortlichen auf den Grundsatz von Treu und Glauben ausgeschlossen ist.[513]

Das Urteil des BAG bezieht sich auf ein vertragliches Treueverhältnis, wie es zwischen Arbeitgeber und Arbeitnehmer besteht. Eine solche vertragliche Beziehung besteht im Verhältnis eines Betroffenen gegenüber einer forschenden Stelle i.d.R. nicht. Als treuwidrig oder „unfair" sind Verhaltensweisen zu bewerten, die ein Vertrauen missbrauchen. Dies schützt einerseits das Vertrauen des Einwilligenden, dass die Datenverarbeitung in Falle eines Widerrufs künftig unterbleibt, zumal auf die Widerspruchsmöglichkeit gemäß Art. 7 Abs. 3 S. 3 DSGVO ausdrücklich hinzuweisen ist.[514] Dies schließt andererseits aber nicht aus, dass der Hinweis mit einer auf Fairnesserwägungen basierenden Einschränkung verknüpft wird, in der auch auf das Vertrauen des Verantwortlichen verwiesen wird. Ein solches **Vertrauen von Forschenden** wird gerade in der DSGVO durch die dort enthaltenen Privilegierungen besonders geschützt.

Dem kann entgegengehalten werden, dass mit einem Wechseln der Rechtsgrundlage das Vertrauen des Betroffenen missbraucht wird. Suggeriert der Verantwortliche dem Betroffenen, es sei dessen Entscheidung, ob eine Verarbeitung erfolgt oder nicht, und missachtet er danach diese Entscheidung, so verhält sich der Verantwortliche **widersprüchlich und treuwidrig**, was für die Unzulässigkeit eines Wechsels spricht.[515] Der Verantwortliche muss sich grundsätzlich auf eine Rechtsgrundlage festlegen.[516] Zudem ist nach Ansicht der Art.-29-Arbeitsgruppe der in Art. 17 Abs. 1 lit. b DSGVO geregelte Fall nicht auf einen Wechsel der Rechtsgrundlage anzuwenden, sondern auf die Verarbeitung zu unterschiedlichen Zwecken auf der Grundlage von unterschiedlichen Rechtsgrundlagen.[517]

Eine Lösung des Konfliktes zwischen den Erwartungshaltungen des Betroffenen und eines forschenden Verantwortlichen kann darin liegen, dass ausdrücklich darauf hingewiesen wird, dass für den Fall eines Einwilligungswiderrufs der Rückgriff auf eine andere **Rechtsgrundlage** möglich ist.[518] Dieses **Hinweiserfordernis** ergibt sich

511 BAG 11.12.2014 – 8 AZR 1010/13, Rn. 39; BAGE 150, 195 = NJW 2015, 2140 = MDR 2015, 1082 = NZA 2015, 604 = BB 2015, 1203 u. 1276 = DB 2015, 1296 = K&R 2015, 433 = afp 2015, 358 = JR 2016, 479.

512 Weichert in DWWS, Art. 5 Rn. 18.

513 Wolff in Schantz/Wolff, Rn. 393; a.A. wohl Heberlein in Ehmann/Selmayr, Art. 5 Rn. 9f.

514 Roßnagel in SHS, Art. 5 Rn. 47.

515 Buchner/Petri in Kühling/Buchner, Art. 6 Rn. 23; Uecker ZD 2019, 248; EDPB, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, 30; Artikel 29-Datenschutzgruppe, WP 259 rev. 01 v. 10.04.2018, 27; Graf von Kielmansegg in TMF, 109f.

516 Artikel 29-Datenschutzgruppe, WP 259 rev. 01 v. 10.04.2018, 28.

517 Artikel 29-Datenschutzgruppe, WP 259 rev. 01 v. 10.04.2018, 26.

518 EuGH 01.10.2015 – C-201/14 (Weltimmo), Rn. 32, ZD 2015, 578 = NVwZ 2016, 375.

auch aus Art. 13 Abs. 1 lit. c bzw. Art. 14 Abs. 1 lit. c DSGVO, wonach die Betroffenen über die Rechtsgrundlage für die Verarbeitung zu informieren sind. Zwar ändert sich hier nicht der Zweck, wohl aber die Rechtsgrundlage. Ein Verweis auf Art. 6 DSGVO genügt nicht.[519] Vielmehr müssen die konkreten rechtlichen Normen, auf welche eine Verarbeitung gestützt werden soll, benannt werden. Im Fall einer auf Interessenabwägung basierenden Rechtfertigung muss der Verantwortliche vor der Datenverarbeitung über seine berechtigten Interessen informieren. Art. 13 Abs. 2 lit. c DSGVO und Art. 14 Abs. 2 lit. d DSGVO verpflichten, nicht nur auf die Möglichkeit eines Einwilligungswiderrufs, sondern auch auf die damit verbundenen Folgen hinzuweisen. Eine Hinweispflicht besteht auch in Bezug auf ein Widerspruchsrecht nach Art. 21 DSGVO (Art. 13 Abs. 2 lit. b, 14 Abs. 2 lit. c DSGVO).

Gegen eine solche Informationslösung wird eingewandt, dass der Betroffene mit **widersprüchlichen Informationen** zu einer Datenverarbeitung konfrontiert werde, was diesem nicht zuzumuten sei und letztlich auf eine Täuschung oder zumindest eine Verwirrung hinauslaufe. Der Betroffene werde entmutigt, nachträglich eine neue entgegenstehende Entscheidung (Opt-out) zu treffen, weil er befürchten müsse, dass diese nicht beachtet werde. Eine Widersprüchlichkeit und damit einhergehende Täuschungen oder Verwirrungen können durch die Art der erteilten Informationen vermieden werden. Eine Entmutigung des Betroffenen zur Wahrnehmung seiner Rechte kann durch die Zusage verhindert werden, dass für den Fall eines Wechsels zu einer abwägenden Rechtsgrundlage von ihm vorgebrachte Interessen Berücksichtigung finden.

Schließlich wird darauf hingewiesen, dass unterschiedliche Rechtsgrundlagen in Bezug auf die **Datenübertragbarkeit** unterschiedliche Rechtsfolgen haben. Im Fall einer Einwilligung besteht ein Anspruch nach Art. 20 DSGVO, bei einer abwägungsbasierten Verarbeitung dagegen nicht.[520] Diese gesetzlich vorgesehene, in der Praxis derzeit wenig relevante Rechtsfolge kann eine grundsätzlich rechtmäßige Datenverarbeitung nicht zu einer unzulässigen Verarbeitung machen.

Im Ergebnis kommt es für die Frage der Auswechselbarkeit der Rechtsgrundlagen auf den **konkreten Einzelfall** an. Entscheidend ist, ob und inwieweit Treu und Glauben einen Rechtsgrundwechsel ausschließen. Ein „Befugnis-Hopping" darf es nicht geben. Umgekehrt kann auch der Forschende sich möglicherweise auf Treu und Glauben berufen. Die Angabe mehrerer einschlägiger Rechtsgrundlagen ist rechtlich nicht ausgeschlossen.[521] Den Hinweis- und Informationspflichten nach den Art. 13f. DSGVO kann umfassend Rechnung getragen werden, wozu auch die Information über eine Widerspruchsmöglichkeit und deren Wirkung gehört. Auf Verlangen ist dem Betroffenen der Wechsel der Rechtsgrundlage zu erläutern.[522]

Je nach den Umständen kann eine auf einer Abwägung basierende Legitimation ausnahmsweise möglich sein (vgl. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO). Im Anwendungsbereich des Art. 9 DSGVO bedarf es dabei regelmäßig einer diese Abwägung präzisierenden nationalen Regelung. Entsprechendes gilt aber nicht für eine alternative Rechtsgrundlage bei einer Verarbeitung durch Behörden (Art. 6 Abs. 1 UAbs. 2

519 Eßer in Auernhammer, Art. 13 Rn. 21.
520 Roßnagel, Review des vorliegenden Rechtsgutachtens v. 02.02.2020, 13.
521 Schwartmann/Schneider in SJTK, Art. 13 Rn. 39; Knyrim in Ehmann/Selmayr, Art. 13 Rn. 38.
522 Bäcker in Kühling/Buchner, Art. 13 Rn. 26.

DSGVO). Ein pauschaler Rückgriff auf die andere Rechtsgrundlage ist jedenfalls unzulässig. Vielmehr bedarf es – unabhängig von der alternativen Rechtsgrundlage – einer **Abwägung im Einzelfall**, wobei von Betroffenen vorgetragene Interessen und Belange umfassend berücksichtigt werden müssen. Dabei sind die jeweiligen Vertrauenserwartungen zu berücksichtigen. Als weitere Abwägungsaspekte sind die Sensitivität für den Betroffenen und die Bedeutung des einzelnen Datums für das Forschungsprojekt zu berücksichtigen.[523]

Wird also eine Forschungseinwilligung widerrufen, so entfällt die Legitimation der Datenverarbeitung nach Art. 6 Abs. 1 lit. a, 7 DSGVO. Kommt man im konkreten Fall zu dem Ergebnis, dass wegen des Wegfalls eine Weiterverarbeitung unzulässig ist, so muss diese unterbleiben. Jedoch können durch die bisherige Verarbeitung ausgelöste weitere Verarbeitungsvorgänge, die auf anderen Rechtsgrundlagen basieren, weiterhin zulässig sein. Dies gilt etwa für Dokumentationspflichten der Forschenden sowie für **gesetzliche Aufbewahrungspflichten** aus Sicherheitsgründen.[524]

7.4 Einwilligung nach nationalem Recht

Die Regelungen des BDSG sowie der LDSG erwähnen die **Einwilligung als Legitimation** für die Verarbeitung von Daten für Forschungszwecke nicht.[525] Dies ist konsequent, da als Rechtsgrund direkt auf Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO zurückgegriffen werden kann und EU-Recht vorgeht. Es gilt in Bezug auf europäische Regelungen für die nationalen Gesetzgeber ein Normwiederholungsverbot.[526] Anders als § 27 BDSG, der deshalb die Einwilligung unerwähnt lässt, weisen einige Landesregelungen darauf hin, dass Daten für Forschungszwecke „ohne Einwilligung" verarbeitet werden dürfen.[527] Diese Formulierungen sind unschädlich und haben keine eigenständige normative Bedeutung.

Art. 9 Abs. 2 lit. a DSGVO erlaubt es dem nationalen Gesetzgeber, Gesetze zu erlassen, die eine Legitimation einer sensitiven Datenverarbeitung auf Einwilligungsbasis ausschließt. Dem nationalen Gesetzgeber ist es damit auch erlaubt, **zusätzliche Anforderungen** an eine Einwilligung zu stellen, etwa in Bezug auf die Form der Einwilligung, die Bedenkzeit oder die Art und den Umfang der nötigen Aufklärung oder Beratung.[528]

Es gibt aber auch nationale Regelungen, die eine Datenverarbeitung ohne Einwilligung für unzulässig erklären. In diese Richtung geht im **Sozialrecht** die allgemeine Regelung zur Datenweitergabe für Forschungszwecke in § 75 Abs. 1 S. 2 SGB X:

> *„Eine Übermittlung ohne Einwilligung der betroffenen Person ist nicht zulässig, soweit es zumutbar ist, ihre Einwilligung einzuholen."*

523 Im Ergebnis ähnlich Schulz in Gola, Art. 4 Rn. 11–13.
524 EDSA, 8 (Rn. 24).
525 Siehe dazu den Überblick im Anhang bei Bernhardt/Ruhmann/Weichert.
526 Selmayr/Ehmann in Ehmann/Selmayr, Einführung Rn. 80, 90; Hornung/Spiecker in SHS, Einl. Rn. 233; Bieresborn, NZS 2017, 888f.
527 So § 17 Abs. 1 BlnDSG, § 25 Abs. 1 S. 1 BbgDSG, § 11 Abs. 1 S. 1 HmbDSG, § 9 Abs. 1 DSG M–V,
528 Dochow GesR 2016, 405; Greve in Aauernhammer, Art. 9 Rn. 19; Weichert in Kühling/Buchner, Art. 9 Rn. 48; Petri in SHS, Art. 9 Rn. 36; Jaspers/Schwartmann/Mühlenbeck in SJTK, Art. 9 Rn. 119; a.A. Schiff in Ehmann/Selmayr, Art. 9 Rn. 36.

Die Regelung ist auch für Zweckänderungen innerhalb des Verantwortlichen zugunsten einer Forschungsnutzung anzuwenden (§ 67c Abs. 2 Nr. 2 SGB X).[529] Über die Zumutbarkeitsformel besteht kein ausnahmsloses Einwilligungserfordernis. Es erfolgt auch keine inhaltliche Ausgestaltung der Einwilligung in die Verarbeitung von personenbezogenen Daten allgemein, die in der DSGVO abschließend geregelt ist. Die Frage nach der Zumutbarkeit muss aber im Lichte der Forschungsprivilegierung i.S.v. Art. 5 Abs. 1 lit. b DSGVO ausgelegt werden.

Eine weitere Sonderregelung zur Forschungsdatenverarbeitung enthält § 67b Abs. 3 SGB X:

> *„Die Einwilligung zur Verarbeitung personenbezogener Daten zu Forschungszwecken kann für ein bestimmtes Vorhaben oder für bestimmte Bereiche der wissenschaftlichen Forschung erteilt werden. Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne des Absatzes 2 Satz 2 auch dann vor, wenn durch die Einholung einer schriftlichen oder elektronischen Einwilligung der Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind die Gründe, aus denen sich die erhebliche Beeinträchtigung des Forschungszweckes ergibt, schriftlich festzuhalten."*

Abs. 2 S. 2 erlaubt den besonders zu begründenden **Verzicht auf eine schriftliche oder elektronische Einwilligung**. Trotz der möglichen vorgesehenen inhaltlichen Weite der Einwilligung steht diese Regelung mit der DSGVO in Einklang, zumal sie die gleiche Funktion wie die in der DSGVO geregelte Privilegierung verfolgt.[530]

Eine Sonderregelung zur Einwilligung und zu deren Widerrufbarkeit enthält das **Arzneimittelgesetz** (AMG). § 40 Abs. 1 Nr. 3 AMG stellt qualifizierte Anforderungen an die Betroffeneneinwilligung bei der Teilnahme an klinischer Forschung (Volljährigkeit, besondere Einsichtsfähigkeit, Aufklärung, Schriftlichkeit der Erklärung). Nach § 40 Abs. 2a S. 2 Nr. 2 AMG darf – in Einklang mit Art. 7 Abs. 3 S. 1 DSGVO – der Betroffene *„die Einwilligung nach Absatz 1 Satz 3 Nummer 3 Buchstabe c jederzeit widerrufen"*. In Nr. 3 ist dann aber vorgesehen, dass weiterhin

> *„3. im Falle eines Widerrufs der nach Absatz 1 Satz 3 Nummer 3 Buchstabe b oder Buchstabe c erklärten Einwilligung die gespeicherten Daten weiterhin verarbeitet werden dürfen, soweit dies erforderlich ist, um*
>
> *a) Wirkungen des zu prüfenden Arzneimittels festzustellen,*
>
> *b) sicherzustellen, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden,*
>
> *c) der Pflicht zur Vorlage vollständiger Zulassungsunterlagen zu genügen.*
>
> *4. die Daten bei den genannten Stellen für die auf Grund des § 42 Abs. 3 bestimmten Fristen gespeichert werden."*

Weiterhin wird in den Sätzen 4–6 das Vorgehen im **Fall eines Widerrufs der Einwilligung** beschrieben. Danach „haben die verantwortlichen Stellen unverzüglich zu prüfen, inwieweit die gespeicherten Daten für die in Satz 2 Nr. 3 genannten Zwecke

529 Dierks in Dierks/Roßnagel, 39.
530 Dierks in Dierks/Roßnagel, 47f.

noch erforderlich sein können. Nicht mehr benötigte Daten sind unverzüglich zu löschen. Im Übrigen sind die erhobenen personenbezogenen Daten nach Ablauf der auf Grund des § 42 Abs. 3 bestimmten Fristen zu löschen, soweit nicht gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen."[531] Gemäß § 42 Abs. 3 AMG kann in einer Rechtsverordnung die Aufbewahrungsfrist der Forschungsunterlagen näher festgelegt werden. Diese Regelungen sind durch die Öffnungsklauseln der DSGVO gedeckt.[532]

531 Zur Widerruflichkeit der Einwilligung nach AMG Bischoff/Wiencke ZD 2019, 9.
532 Bischoff/Wiencke ZD 2019, 8ff.

8 Zweckbindung, Zweckänderung

Das Erfordernis einer Zweckbindung bei der Verarbeitung personenbezogener Daten ergibt sich aus Art. 8 Abs. 2 S. 1 GRCh, wonach solche „Daten nur nach Treu und Glauben für festgelegte Zwecke" verarbeitet werden dürfen. Im deutschen Recht wird dieser Grundsatz für Sozialdaten in § 67c SGB X bekräftigt.[533] Der Zweckbindungsgrundsatz wird nun in Art. 5 Abs. 1 lit. b DSGVO bestätigt, verbunden mit der Ergänzung, dass eine Unvereinbarkeit mit dem Erhebungszweck nicht anzunehmen ist, wenn die Verarbeitung für wissenschaftliche Forschungszwecke gemäß Art. 89 Abs. 1 DSGVO erfolgt.[534] Forschung und Statistik sind also hinsichtlich der Zweckfestlegung **grundsätzlich privilegiert** (Fiktion der Zweckidentität)[535]; ob eine Nutzung erfolgen darf, ist abhängig von entsprechenden Garantien.

8.1 Privilegierung

Nicht eindeutig ist, welches die **Begründung für die Privilegierung** von (Archiv,) Forschung und Statistik ist. Diese Zweckverfolgung hat nicht in jedem Fall, aber typischerweise zur Folge, dass zwar die Ausgangsdaten, aber die Ergebnisse nicht personenbezogen sind.[536] Es kann auch nicht behauptet werden, dass die genannten

533 Bieresborn NZS 2017, 928f.

534 Albrecht/Jotzo, Teil 3 Rn. 55; Weichert ZD 2020, 21; Werkmeister/Schwaab CR 2019, 88: Es bedarf keines Kompatibilitätstests.

535 Roßnagel in SHS, Art. 5 Rn. 103; Paal/Pauly-Frenzel, Art. 5 Rn. 32; Kühling/Buchner-Herbst, Art. 5 Rn. 50.

536 Roßnagel in SHS, Art. 5 Rn. 104.

Zwecke höherrangig als die des Datenschutzes wären. Vielmehr kann der Grund der Privilegierung nur in dem spezifischen öffentlichen Interesse an (Archiv,) Forschung und Statistik liegen.[537]

Es ist aber umstritten, ob bei einer privilegierten Zweckänderung für Forschungs- und Statistikzwecke ein **öffentliches Interesse** bestehen muss. Art. 5 Abs. 1 lit. b und Art. 89 Abs. 1 DSGVO fordern dies ausdrücklich nur für Archivzwecke.[538] In ErwGr 159 S. 4 wird hinsichtlich der Medizinforschung auf das öffentliche Interesse hingewiesen:

> *„Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden."*

Unbestreitbar ist, dass die Privilegierung öffentliche wie private Stellen für sich in Anspruch nehmen können. Für eine die Privilegierung rechtfertigende Datennutzung muss aber insbesondere auch bei privaten Forschenden ein überwiegendes Allgemeininteresse vorliegen.[539] Ein rein privates Forschungsinteresse kann den sehr weitgehenden Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen nicht legitimieren, der mit einer rechtlich privilegierten Forschungsnutzung verbunden sein kann. Der Verzicht auf den Hinweis auf ein öffentliches Interesse bei Forschung und Statistik in der DSGVO mag damit zu erklären sein, dass der Gesetzgeber davon ausging, dass bei Forschung und Statistik schon begrifflich in jedem Fall ein öffentliches Interesse besteht.

Eine **enge Zweckbindung** von Forschungsdaten ist die zwangsläufige Konsequenz daraus, dass diese privilegiert genutzt werden dürfen: Könnten Daten aus einem Forschungszusammenhang – ähnlich wie sonstige Daten – auf der Grundlage eines einfachen berechtigten (vgl. Art. 6 Abs. 1 lit. f DSGVO) oder eines sonstigen öffentlichen Interesses (vgl. Art. 6 Abs. 1 lit. e DSGVO) weiterverwendet werden, so würde über den Umweg einer Forschungsnutzung einer missbräuchlichen Weiterverwendung die Tür geöffnet (Flucht in die Privilegierung). Die wissenschaftliche Datennutzung stellt ein berechtigtes Interesse dar.[540] Dies rechtfertigt aber noch nicht eine generelle Vorrangbehandlung dieser Nutzungsart. Ähnlich wie auch Statistikdaten[541], für die es ein spezifisches Statistikgeheimnis gibt (§ 16 BStatG), muss es für eine Verwendung von Forschungsdaten entweder ein vollständiges Verbot oder aber eine besonders hohe rechtliche Hürde bei einer Nutzung zu anderen als Forschungszwecken geben. Anderenfalls würde das Vertrauen der Betroffenen wie der Gesellschaft generell in einen verantwortungsvollen Umgang mit den anvertrauten Daten beeinträch-

537 Caspar in SHS, Art. 89 Rn. 6; Paal/Pauly-, Art. 89 Rn. 3; Kühling/Buchner-Herbst, Art. 5 Rn. 52; Weichert in HHJ, 429.

538 EDPS 2020, 23; Weichert in DWWS, Art. 89 Rn. 10; a.A. Albrecht/Jotzo, Teil 3 Rn. 71; Buchner/Tinnefeld in Kühling/Buchner, Art. 89 Rn. 9; Werkmeister/Schwaab CR 2019, 86.

539 Unstreitig seit BVerfG 15.12.1983 – 1 BvR 209/83 u.a., LS 2, Rn. 100, NJW 1984, 422; zur Forschung schon OLG Hamm 28.11.1995 – 1 VAs 38/94, NJW 1996, 941 = JR 1997, 172; aktuell ebenso Datenethikkommission, 124, 139 (These 16); DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, März 2019, 14, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf; so schon OLG Hamm JR 1997, 172; missverständlich Martini/Hohmann NJW 2020, 3576.

540 Golla in Specht/Mantz, § 23 Rn. 42, 44.

541 BVerfG 15.12.1984 – 1 BvR 209/83 u.a., NJW 1984, 423; Weichert in HHJ, 431f.

tigt. Dieses Vertrauen ist eine Grundvoraussetzung für die Durchführung von Forschung.[542]

Das Fehlen einer strengen gesetzlichen Zweckbindung auf nationaler Ebene kann nicht dazu führen, dass privilegiert verarbeitete Forschungsdaten in Deutschland für nicht-wissenschaftliche Zwecke genutzt werden dürfen. Eine **nachträgliche weitere Datenverarbeitung** für Zwecke außerhalb des Anwendungsbereichs des Art. 89 DSGVO würde zu einem Verstoß gegen Art. 89 DSGVO führen, da die in Abs. 1 S. 1 geforderten Garantien nicht bestehen und die in Abs. 4 für die Zulässigkeit der privilegierten Nutzung geforderte Zweckbeschränkung nicht beachtet wird.[543] Die zweckwidrige Weiterverarbeitung hat die Folge, dass die Privilegierung in Bezug auf die Beschränkung der Betroffenenrechte nicht in Anspruch genommen werden kann.[544] Sie hat aber regelmäßig auch zur Folge, dass die Weiterverarbeitung der Forschungsdaten regelmäßig unzulässig ist, soweit nicht eine Betroffeneneinwilligung vorliegt.[545] Etwas anderes kann nur gelten, wenn das nationale Recht eine ausdrückliche Zweckänderung von Forschungsdaten zulässt, bei der der in Art. 89 Abs. 1 S. 1 DSGVO geforderte Betroffenenschutz gewahrt bleibt. Letztlich wird so durch Art. 89 Abs. 4 DSGVO ein Forschungsgeheimnis vorgegeben, das bei der Verarbeitung von Forschungsdaten zu beachten ist (s.u. Kap. 8.4).

Die Annahme der Wissenschaftlichkeit der Verarbeitung personenbezogener Daten setzt deren Zweckbindung voraus. Es muss ein **wissenschaftliches Erkenntnisinteresse** verfolgt werden, wobei dieses nicht auf ein eng definiertes Forschungsprojekt beschränkt sein muss (s.o. Kap. 3.2).[546] Der Zweck jeder Forschungsdatenverarbeitung muss aber gesondert festgelegt werden.

Die Privilegierung durch die grundsätzlich bestehende Zweckvereinbarkeit (Art. 5 Abs. 1 lit. b DSGVO) gilt auch, wenn die **Forschung der Primärzweck** der Daten ist.[547] Daten können zwischen Projekten, in Forschungsverbünden, wissenschaftlichen Netzwerken und Registern ausgetauscht und weiterverwendet werden, wenn hierbei die Rechte und Freiheiten der Betroffenen durch Garantien hinreichend gewahrt bleiben (Art. 5 Abs. 1 lit. b i.V.m. Art. 89 Abs. 1 DSGVO).

Streitig ist, wie sich die **Regelung des Art. 6 Abs. 4 DSGVO** zur Forschungsprivilegierung verhält. Diese Regelung gibt Kriterien dafür vor, wann Zwecke miteinander vereinbar sind. Dies bedeutet jedoch nicht, dass in Art. 6 Abs. 4 DSGVO eine eigenständige Befugnis zur Zweckänderung zu sehen ist (s.o. Kap. 4.4).[548] Die Regelung benennt nur, welche Kriterien für die Zulässigkeit einer Zweckänderung beachtet werden müssen: Verhältnis zwischen Primär- und Sekundärzweck (a), Verhältnis zwischen Verantwortlichem und Betroffenen (b), Sensibilität der Daten (c), Risiken für die Betroffenen (d) und Schutzmaßnahmen (e). Diese Aspekte sind bei Zweckänderungen zu berücksichtigen, beinhalten aber keine eigenständige Zweckänderungserlaubnis. Insofern gelten die Rahmenbedingungen, die durch Art. 6 und für beson-

542 Golla in Specht/Mantz, § 23 Rn. 9; Britz in Dreier, Art. 5 III (Wissenschaft), Rn. 37; Bizer, 229.
543 Caspar in SHS, Art. 89 Rn. 68; Raum in Ehmann/Selmayr, Art. 89 Rn. 53.
544 Caspar in SHS, Art. 89 Rn. 68; Greve in Auernhammer, Art. 89 Rn. 15.
545 So wohl auch Raum in Ehmann/Selmayr, Art. 89 Rn. 53.
546 Noch anders die frühere herrschende Meinung, Bizer, 230.
547 Roßnagel ZD 2019, 162.
548 So Gola-Schulz, Art. 6 Rn. 185; Roßnagel in SHS, Art. 6 Abs. 4 Rn. 12; wohl auch Kühling/Martini u.a., 38.

dere Datenkategorien ergänzend durch Art. 9 DSGVO gesetzt werden.[549] Es ist kein Grund dafür ersichtlich, dass die Kriterien des Art. 6 Abs. 4 DSGVO nicht für Zweckänderungen bei privilegierter Forschung anwendbar sein sollten.[550] Die dort genannten Aspekte können und müssen bei der Risikobewertung und bei der Bestimmung der nötigen Garantien einfließen.

Die **Nachweispflicht** für das Vorliegen der Voraussetzungen für die Privilegierung liegt beim Verantwortlichen (Art. 5 Abs. 2 DSGVO). Es gehört nicht zu den Pflichten der Betroffenen, deren Nichtvorliegen zu begründen.[551] Die Betroffenen haben i.d.R. keine genauere Kenntnis vom konkreten Zweck der sie betreffenden Forschungsprojekte, geschweige denn vom konkreten Vorliegen der Voraussetzungen der in Art. 89 DSGVO geforderten Garantien.

Die privilegierte Zweckänderung bezieht sich zunächst auf die Verarbeitung durch den Verantwortlichen. Erlaubt wird also zunächst die **interne Nutzung**, die Eigenforschung durch den Verantwortlichen.[552]

Die Regelung des Art. 5 Abs. 1 lit. b DSGVO beschränkt sich aber nicht hierauf; vielmehr erlaubt sie die Zweckänderung ohne Beschränkung auf bestimmte Verantwortliche. Sie muss so interpretiert werden, dass damit auch zweckändernde **Übermittlungen privilegiert** sein sollen (zum Erfordernis einer eigenständigen Rechtsgrundlage s.o. Kap. 4.4), soweit die sonstigen Voraussetzungen für die Übermittlung vorliegen. Bei einem anderen Verständnis würde die Regelung praktisch leerlaufen, da moderne Forschung regelmäßig mit großen Datenbeständen von mehr als einem Verantwortlichen und unter der Verantwortung einer auf Forschung spezialisierten Stelle erfolgen muss, die zumeist nicht mit der primär datenverarbeitenden Stelle identisch sein kann. Einschränkungen für Übermittlungen können sich aus der Notwendigkeit angemessener Garantien ergeben (Art. 89 Abs. 1 DSGVO).

8.2 Zweckfestlegung

Hinsichtlich der **Zweckfestlegung** bestätigt ErwGr 33 S. 1, dass bei einer Datenerhebung für Forschungszwecke die konkreten Zwecke oft nicht vollständig angegeben werden können, da relevante Fragestellungen sich erst während der Durchführung eines Projektes oder zu einem noch späteren Zeitpunkt ergeben. Zugleich lässt sich aus ErwGr 33 S. 2, 3 ableiten, dass Art. 89 DSGVO keine übergeordnete und umfassende Zweckfestlegung beabsichtigt und eine Eingrenzung erforderlich ist. Zu unbestimmt ist daher z.B. folgende Formulierung: „Wir können Ihre personenbezogenen Daten zu Forschungszwecken verwenden".[553] Dies gilt nicht nur für die einwilligungsbasierte Forschung, sondern auch für die Zweckfestlegung, wenn Forschung auf gesetzlicher Grundlage durchgeführt wird. Wie weit diese Eingrenzung erfolgt, soll von der Einhaltung von Standards abhängen, wobei hier nicht nur anerkannte ethische

549 Schantz, NJW 2016, 1844; Albrecht, CR 2016, 92; Ehmann/Selmayr-Schiff, Art. 9 Rn. 11; Ehmann/Selmayr-Heberlein, Art. 6 Rn. 53.

550 Roßnagel in SHS, Art. 6 Abs. 4, Rn. 41; Ehmann/Selmayr-Heberlein, Art. 6 Rn. 53; Kühling/Buchner-Buchner/Petri, Art. 6 Rn. 192.

551 So aber Roßnagel in SHS, Art. 5 Rn. 110; Paal/Pauly-Frenzel, Art. 5 Rn. 32.

552 Zur früheren Rechtslage Bizer, 266ff.; Metschke/Wellbrock, 40.

553 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 10.

Standards ausschlaggebend sein können, sondern auch normative Festlegungen sowie technisch-organisatorische Vorkehrungen.[554] Die Erwägungen in ErwGr 33 gelten für öffentliche und private Stellen, also für öffentlich-rechtliche Forschungsinstitute wie für kommerzielle Forschungsunternehmen gleichermaßen, soweit die Anforderungen an eine privilegierte Forschungseinrichtung erfüllt sind (s.o. Kap. 8.1).

Soll eine Weiternutzung von Daten für **Forschungsprojekte** erfolgen, so müssen die Zwecke vorab möglichst präzise festgelegt werden.[555] Ohne diese konkrete Zielvorgabe ist eine Abwägung mit den Betroffeneninteressen nicht möglich.[556] Die von der DSGVO vorgesehene Nutzungsprivilegierung erlaubt eine erleichterte Zweckänderung, also die Festlegung des möglichst präzise zu benennenden Sekundärzwecks. Sie ermöglicht – bei hinreichenden Garantien – eine Flexibilisierung bei der Festlegung.[557]

Hier nicht weiter vertieft, aber angesprochen werden soll die Nutzung von individuellen Forschungserkenntnissen für **therapeutische Zwecke**. Lange Zeit war die Nutzung von Behandlungsdaten für Forschungszwecke eine Einbahnstraße. Dass Forschungsdaten für individuelle Behandlungszwecke genutzt werden können, ist eine relativ neue Entwicklung, die mit der zunehmenden Personalisierung in der Therapie auf der Grundlage der Erkenntnis insbesondere von genetischen Krankheitsursachen absehbar immer mehr von Bedeutung sein wird.[558] Ein solcher Erkenntnisrückfluss aus der Forschung in die Behandlung ist auf Grundlage einer informierten Einwilligung schon heute möglich. Dabei sind aber hohe Anforderungen an die Informiertheit der Betroffenen zu stellen; das Recht auf Nichtwissen (s.u. Kap. 12.3) ist zu beachten.

8.3 Zweckfestlegung durch Einwilligung

Basiert eine personenbezogene Datenverarbeitung nicht auf einer gesetzlichen Grundlage, sondern auf einer Einwilligung (Art. 6 Abs. 1 lit. a, 9 Abs. 2 lit. a DSGVO), so wird der Zweck der Datenverarbeitung durch die **Einwilligungserklärung** festgelegt. Der Betroffene kann die Tragweite seiner Einwilligungserklärung nur beurteilen, wenn er weiß, zu welchem Nutzen eine Datenverarbeitung erfolgen soll.[559] Die Zweckbestimmung muss bei der Einwilligungserteilung so präzise wie möglich erfolgen, um sicherzustellen, dass personenbezogene Daten nicht für Zwecke verarbeitet werden, mit denen der Betroffene nicht rechnet.[560] Allerdings muss sich die Einwilligung nicht auf einen Zweck beschränken, es ist möglich, eine Einwilligung *„für einen oder mehrere bestimmte Zwecke“* zu erteilen (Art. 6 Abs. 1 lit. a DSGVO). Die Bestimmtheit der Einwilligung ist Voraussetzung für deren Informiertheit.

554 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ in Erwägungsgrund 33 der DS-GVO v. 03.04.2019.

555 Missverständlich daher die Aussage von Geminn, DuD 2018, 641, die Privilegierung bedeute eine Aufweichung dieser Vorgabe.

556 Schneider, 99; OLG Hamm 28.11.1995 – 1 VAs 38/94, NJW 1996, 941 = JR 1997, 172.

557 Johannes/Richter, DuD 2017, 301; Geminn, DuD 2018, 641; zur Frage, welche Rechtsgrundlage nötig ist s.o. Kap. 4.4.

558 Deutscher Ethikrat, 53.

559 Klement in SHS, Art. 7 Rn. 70.

560 Buchner/Kühling in Kühling/Buchner, Art. 7 Rn. 61.

Die Einwilligung muss im Hinblick auf den Zweck hinreichend bestimmt sein. Nicht ausreichend sind Blanko- oder Pauschalerlaubnisse mit generalklauselartigen Zweckbeschreibungen.[561] Kontrovers diskutiert wird, welche **Bestimmtheit** bei der Einwilligung in die Datenverarbeitung für wissenschaftliche Forschungszwecke zu verlangen ist. Oft lässt sich bei der Forschung zum Zeitpunkt der Einwilligung wegen der Offenheit der möglichen Zielsetzungen bei der Auswertung ein konkreter Forschungszweck nicht festlegen. Dem trägt ErwGr 33 S. 2 DSGVO Rechnung (s.o. Kap. 8.2). Für die Bestimmtheit gibt es im Forschungsbereich keine eindeutigen Grenzen. Vielmehr ist anerkannt, dass Einwilligungen „breiter" formuliert werden können, wenn kompensatorische Maßnahmen zum Schutz der Betroffenen bestehen (sog. broad consent, s.o. Kap. 7.2).[562]

8.4 Gesetzliche Regelungen im deutschen Recht

Das allgemeine (und weitgehend auch das spezifische) **deutsche Datenschutzrecht** wurde formell an die Vorgaben der DSGVO angepasst. Die Privilegierung der Forschung bei der Zweckänderung gemäß der DSGVO spiegelt sich aber darin inhaltlich nicht bzw. nur begrenzt wider. Teilweise wird in den Gesetzen ein erhebliches Überwiegen des Forschungszwecks gefordert (so z.B. § 27 Abs. 1 BDSG), teilweise, dass der Zweck nicht auf andere Weise erreicht werden kann oder dass die schutzwürdigen Betroffeneninteressen nicht beeinträchtigt werden.[563] Diese Formulierungen sind mit den Wertungen der DSGVO, Forschung grundsätzlich zu ermöglichen, nicht vereinbar und lassen sich allenfalls über eine europarechtsfreundliche Auslegung mit den Vorgaben der DSGVO in Einklang bringen.[564]

Besonders problematisch ist die enge Zweckbeschreibung einer **Übermittlung** von Sozialdaten nach § 75 Abs. 1 S. 1 SGB X, die beschränkt ist auf *„ein bestimmtes Vorhaben 1. der wissenschaftlichen Forschung im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder 2. der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben."*

Eine entsprechende Regelung enthält § 67c Abs. 5 SGB X für die Verwendung von Sozialdaten durch **Sozialleistungsträger**:

„Für Zwecke der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich erhobene oder gespeicherte Sozialdaten dürfen von den in § 35 des Ersten Buches genannten Stellen nur für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der Planung im Sozialleistungsbereich verändert oder genutzt werden. Die Sozialdaten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Planungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können.

561 Klement in SHS, Art. 7 Rn. 70; Dochow, 736–738.

562 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DS-GVO v. 03.04.2019; Buchner/Kühling, Art. 7 Rn. 64; Schneider, 119f.; zu den Problemen beim Broad Consent: Dierks 2019, 57f.; s.a. Kap. 7.2.

563 Bernhardt/Ruhmann/Weichert, 6.

564 Bernhardt/Ruhmann/Weichert, 9; a.A. wohl Golla in Specht/Mantz, § 23 Rn. 31.

Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Planungszweck dies erfordert."[565]

Solche **absoluten Zweckbegrenzungen** sind mit der offenen Regelung des Art. 5 Abs. 1 lit. b DSGVO nicht in Einklang zu bringen. Die Zweckbegrenzungen werden damit gerechtfertigt, dass es dem nationalen Gesetzgeber nach Art. 6 Abs. 3 lit. b DSGVO freistünde, die Zwecke bei der Offenlegung gegenüber Dritten wie bei der Eigennutzung festzulegen, unabhängig davon, ob es sich um sensitive Daten handelt oder nicht.[566] Zudem wird vorgebracht, dass gemäß Art. 9 Abs. 4 DSGVO bei Gesundheitsdaten der Schutzstandard durch die Mitgliedstaaten erhöht werden darf.[567] Art. 6 Abs. 3 lit. b S. 3 DSGVO verlangt jedoch, dass eine Abwägung erfolgt, also dass Verarbeitungs- und Schutzinteressen in einem „angemessenen Verhältnis" zu stehen haben. Diese geforderte Abwägung hat der deutsche Gesetzgeber hier unterlassen. Auch Art. 9 Abs. 4 DSGVO setzt voraus, dass eine nationale Regelung geeignet, erforderlich und angemessen ist.[568] Ein völliges Abweichen von einem Grundsatz des Art. 5 DSGVO kann damit nicht legitimiert werden.[569] Auch eine Rechtfertigung als geeignete Garantie nach Art. 89 Abs. 1 DSGVO kommt nicht in Betracht, da eine solche Pauschaleinschränkung zum Schutz der Betroffenenrechte nicht erforderlich ist. Dies gilt unabhängig davon, ob medizinische oder auch nichtmedizinische Fragestellungen verfolgt werden.[570] Zwar rühmt sich der Gesetzgeber der besonderen Forschungsfreundlichkeit.[571] Dies mag im Verhältnis zum zuvor geltenden Recht zutreffen. Er ist aber nicht forschungsfreundlich genug, um den DSGVO-Vorgaben zu genügen.

Der Verstoß des § 75 Abs. 1 S. 1 SGB X gegen Art. 5 Abs. 1 lit. b DSGVO wird auch nicht dadurch kompensiert, dass in § 75 Abs. 2 und 4a S. 1 SGB X eine Nutzung der Sozialdaten für Forschungsfragen erlaubt wird, die mit dem ursprünglichen Vorhaben „**in einem inhaltlichen Zusammenhang**" steht. Auch diese Zweckeingrenzung geht über die offene und generelle Privilegierung der DSGVO hinaus. Sie geht auch über die Vereinbarkeitskriterien des Art. 6 Abs. 4 DSGVO hinaus. Diese Bewertung gilt auch für die Regelung des § 67c Abs. 2 Nr. 2 SGB X, der der verantwortlichen Stelle eine Zweckänderung (nur) erlaubt, wenn *„es zur Durchführung eines bestimmten Vorhabens der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich erforderlich ist und die Voraussetzungen des § 75 Absatz 1, 2 oder 4a Satz 1 vorliegen."*

In § 40 BDSGaF war anstelle von verantwortlicher Stelle von „Forschungseinrichtung" die Rede. Damit wurde zum Ausdruck gebracht, dass eine Trennung zwischen der Datennutzung für Forschungszwecke von der Verarbeitung der weiteren Einheiten der Stelle für andere Zwecke geboten ist. Auch wenn diese Formulierung im nunmehr geltenden Recht nicht mehr auftaucht, hat sich an dem **Trennungsgebot** nichts ge-

565 Dazu Dierks in Dierks/Roßnagel, 39ff.; zum Begriff „Forschung im Sozialleistungsbereich" 58.
566 Bieresborn NZS 2017, 929.
567 So in Bezug auf § 287 SGB V Dierks in Dierks/Roßnagel, 35.
568 Es ist streitig, ob Art. 9 Abs. 4 DSGVO nur weitere Beschränkungen einer Datenverarbeitung erlaubt, so Bischoff/Wiencke ZD 2019, 9f., Schiff in Ehmann/Selmayr, Art. 9 Rn. 64, Petri in SHS, Art. 9 Rn. 101, oder ob auch erweiternden gesetzliche Bedingungen zulässig sind, so Dochow GesR 2016, 407; Weichert in Kühling/Buchner, Art. 9 Rn. 150; Kampert in Sydow Art. 9 Rn. 59.
569 Dierks 2019, 31f.
570 Zu dieser Fragestellung in Bezug auf die Auslegung des § 287 SGB V Dierks in Dierks/Roßnagel, 26ff.
571 BT-Drs. 18/12611, 113; dazu Bieresborn NZS 2017, 931.

ändert, das auf die forschungsspezifische Zweckbindung zurückgeht. Das Trennungsgebot bezieht sich auf den spezifischen Umgang mit den Forschungsdaten und erfasst nicht die Organisationsstruktur des Verantwortlichen.[572]

Die Nutzung von Forschungsdaten für andere als Forschungszwecke ist grundsätzlich verboten; insofern kann von einem **Forschungsgeheimnis** (bzw. Forschungsdatengeheimnis) gesprochen werden.[573] Ein Verbot der Verwendung von Forschungsdaten für nichtwissenschaftliche Zwecke, also ein Zweckentfremdungsverbot, war in § 40 Abs. 1 BDSGaF vorgesehen.[574] Dieses schloss insbesondere aus, dass unter Beibehaltung des Personenbezugs Geschäfts- oder Verwaltungszwecke verfolgt werden.[575] Derartige Zwecke sind nicht miteinander vereinbar.[576] Ein gewisses Forschungsgeheimnis ergibt sich nun aus Art. 89 Abs. 4 DSGVO, wonach die Forschungsprivilegierung nicht greifen soll, wenn „gleichzeitig" ein weiterer Zweck verfolgt wird.[577] Die Norm ist aber nicht eindeutig und schließt z.B. eine spätere Zweckänderung der Forschungsdaten nicht zwingend aus. Deshalb kann und sollte dessen konkrete Umsetzung in einem expliziten Gesetz erfolgen.[578] Ein effektives Forschungsgeheimnis müsste ein Beschlagnahmeverbot bei dem und ein Zeugnisverweigerungsrecht für den Forschenden gewährleisten. Damit würde den Probanden das nötige Vertrauen gegeben, dass bereitgestellte Daten nicht zu deren Nachteil in behördliche Verfahren einfließen.[579]

572 Geminn, DuD 2018, 643; Buchner/Tinnefeld in Kühling/Buchner, Art. 85 Rn. 22.

573 Zur früheren Debatte hierüber Bizer, 229; Bochnik, MedR 1994, 398ff.; ders., MedR 1996, 262ff., und Weichert, MedR 1996, 258ff.; Kilian NJW 1998, 788; Greitemann, Das Forschungsgeheimnis, 2001.

574 Schneider, 100f.

575 Weichert in DKWW, § 40 Rn. 6f.

576 Vgl. Art. 6 Abs. 4 sowie die analogen Ausführungen des BVerfG zur Statistik BVerfG NJW 1984, 423ff.

577 Schantz/Wolff-Schantz, Rn. 1346; Werkmeister/Schwaab CR 2019, 86.

578 Ehmann/Selmayr-Raum, Art. 89 Rn. 17, 19.

579 So schon Albrecht CuR 1986, 100; Bizer, 230–234; Deutsche Forschungsgemeinschaft, Forschungsfreiheit – ein Plädoyer der DFG für bessere Rahmenbedingungen der Forschung in Deutschland, 1996, 72; Weichert DANA 4/1997, 7; Greitemann, Das Forschungsgeheimnis, 2001, 290f.; Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik, Wege zu einer besseren informationellen Infrastruktur, 2001, 285.

9 Technisch-organisatorische Vorkehrungen

Das Datenschutzrecht sieht eine Vielzahl von **Vorkehrungen** vor, die im Rahmen von Forschungsprojekten zum Einsatz kommen können. Nur bei einem am Risiko der Verarbeitung orientierten Einsatz der genannten Maßnahmen kann die datenschutzrechtliche Privilegierung für Forschungszwecke zur Anwendung kommen (Art. 89 Abs. 1 DSGVO, vgl. § 27 Abs. 1 S. 3 BDSG). Normativ genannt werden folgende Maßnahmen:[580]

- Datenverschlüsselung (Art. 32 Abs. 1 lit. a DSGVO, § 22 Abs. 2 Nr. 6 BDSG),
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitung sicherzustellen (Art. 32 Abs. 1 lit. b DSGVO, § 22 Abs. 2 Nr. 8 BDSG),
- Fähigkeit, die Verfügbarkeit und den Zugang zu Daten herzustellen (Art. 32 Abs. 1 lit. c DSGVO, § 22 Abs. 2 Nr. 8 BDSG),
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO, § 22 Abs. 2 Nr. 9 BDSG),
- Protokollierung (§ 22 Abs. 2 Nr. 2 BDSG),
- Sensibilisierung der an der Verarbeitung Beteiligten (§ 22 Abs. 2 Nr. 3 BDSG),

580 Roßnagel ZD 2019, 161; Dierks 2020, 8f.; kritisch zum Verweis auf § 22 Abs. 1 in § 27 Abs. 1 S. 2 BDSG wegen des fehlenden Bezugs zur Forschung Golla in Specht/Mantz, § 23 Rn. 32.

Benennung bzw. Einbeziehung eines Datenschutzbeauftragten (§ 22 Abs. 2 Nr. 4 BDSG)[581],

- Zugangsbeschränkungen (§ 22 Abs. 2 Nr. 5 BDSG),

spezifische Verfahrensregelungen bei Übermittlung oder Zweckänderung (§ 22 Abs. 2 Nr. 10 BDSG)[582],

- Genehmigungsvorbehalte (§ 75 Abs. 4, 4a SGB X),
- Anzeigepflichten (§ 80 Abs. 1 SGB X),

Einbeziehung einer Ethikkommission (§ 15 MBOÄ),[583]

- weitere technisch-organisatorische Maßnahmen zur Wahrung der Datenschutzkonformität (§ 22 Abs. 2 Nr. 1 BDSG).

Hinsichtlich dieser Anforderungen besteht durch die Aufsichtsbehörden, deren Zusammenschlüsse und insbesondere den Europäischen Datenschutzausschuss die Möglichkeit der Konkretisierung.[584] Insbesondere **bei einer wenig bestimmten Zweckbindung** von für Forschungszwecke verarbeiteten Daten verlangt die Konferenz der deutschen Datenschutzaufsichtsbehörden kompensatorische Maßnahmen im Interesse von Transparenz (A.), Vertrauensbildung (B.) und Datensicherheit (C.):[585]

A. Transparenz

- *„Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren Forschungsplanes, der die geplanten Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet*
- *Ausarbeitung und Dokumentation im Hinblick auf das konkrete Forschungsprojekt, wieso in diesem Fall eine nähere Konkretisierung der Forschungszwecke nicht möglich ist*
- *Einrichten einer Internetpräsenz, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden"*

B. Vertrauensbildung

- *„Positives Votum eines Ethikgremiums vor der Nutzung für weitere Forschungszwecke*
- *Prüfung, ob das Arbeiten mit einem dynamic consent möglich ist, bzw. Einräumung einer Widerspruchsmöglichkeit vor der Verwendung der Daten für neue Forschungsfragen"*

C. Datensicherheit

- *„Keine Datenweitergabe in Drittländer mit geringerem Datenschutzniveau*
- *Gesonderte Zusagen zur Datenminimierung, Verschlüsselung, Anonymisierung oder Pseudonymisierung*
- *Spezifische Vorschriften für die Begrenzung des Zugriffs auf die erhobenen Daten"*

581 Roßnagel ZD 2019, 162.
582 Nachweise zum Landesrecht bei Bernhardt/Ruhmann/Weichert, 8.
583 Zur Geschichte ethischer Standards, zu „informed consent" und Kontrolle EDPS 2020, 13.
584 Martini/Hohmann NJW 2020, 3577.
585 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DS-GVO v. 03.04.2019; ähnlich zu Rahmenbedingungen des Broad Consent TMF, 98ff.

Bei der Verarbeitung von Sozialdaten gilt § 22 BDSG entsprechend (§ 67b Abs. 1 S. 4 SGB X). Bei den genannten Maßnahmen fällt auf, dass diese zumeist nicht nur im Forschungsbereich bzw. bei sensitiven Daten, sondern generell zur Pflicht gemacht werden.[586] Die spezifische Erwähnung verpflichtet zu einer **erhöhten Prüftiefe** und zu spezifischen, dem Risiko angemessenen Maßnahmen.

Die Feststellung, welche der genannten Maßnahmen zu ergreifen sind, erfolgt unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen (**Risikoorientierung** – vgl. § 22 Abs. 2 S. 2 i.V.m. § 27 Abs. 1 S. 2 BDSG).[587] Die Art und der Umfang der Garantien hängen also im Forschungsbereich vom jeweiligen Projekt und den damit verbundenen Risiken ab.[588]

Aus dem oben Ausgeführten kann abgeleitet werden, dass bei jedem privilegierten Forschungsprojekt, bei dem in erheblichem Umfang mit personenbezogenen Daten gearbeitet wird, ein **Datenschutzkonzept** erstellt werden muss, in dem die angemessenen Garantiemaßnahmen aufgeführt werden (ausdrücklich z.B. § 24 Abs. 1 S. 2 HDSIG).[589] Diese Pflicht ergibt sich zudem indirekt aus der nach Art. 35 Abs. 3 lit. b DSGVO bestehenden Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (s.u. Kap. 11.4).[590]

586 Johannes/Richter, DuD 2017, 302f.
587 Zum risikobasierten Ansatz Schröder ZD 2019, 503ff.
588 Johannes/Richter, DuD 2017, 302.
589 Roßnagel ZD 2019, 161.
590 DWWS-Wedde, § 22 Rn. 21; Roßnagel ZD 2019, 163.

10 Datenminimierung

Wissenschaftliche Forschung zielt regelmäßig auf das **Erkennen von allgemeinen Gesetzmäßigkeiten**, nicht auf die Beschreibung einer bestimmten Person. Das Forschungsergebnis soll möglichst vom Einzelfall unabhängig sein, d.h. anonym und verallgemeinerungsfähig.

Kein datenschutzrechtlicher Eingriff ist gegeben, wenn vor der Erhebung oder der Weitergabe personenbezogener Daten an die Forschungsstelle eine **Anonymisierung** erfolgt. Erfolgte eine personenbezogene Erhebung, so sind zum frühestmöglichen Zeitpunkt Maßnahmen zur Datenminimierung zu ergreifen (Art. 5 Abs. 1 lit. c DSGVO).

Gemäß Art. 89 Abs. 1, 2 DSGVO ist die Privilegierung der Datenverarbeitung für Forschungszwecke vom Bestehen bestimmter **geeigneter Bedingungen und Garantien** abhängig. Über diese Garantien soll ein Ausgleich zwischen den tangierten Grundrechten, insbesondere der Forschungsfreiheit und dem Grundrecht auf Datenschutz, hergestellt werden. Art. 89 Abs. 1 S. 2–4 DSGVO nennt als vorrangige Garantie *„die Achtung des Grundsatzes der Datenminimierung"*. Prominent wird die Pseudonymisierung genannt, *„sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen"*.

Eine Verbesserung des kontrollierten Zugangs zu ursprünglich personenbezogenen Daten kann durch die Entwicklung von **Verfahren und Standards** der Anonymisierung und der Pseudonymisierung erreicht werden, die geeignete Betroffenengarantien sicherstellen.[591]

591 Datenethikkommission, 21 (These 20), zu den Methoden 129ff.; Health Ethics Policy Lab, 74, 78.

10.1 Biomaterial und Personenbezug

Für die Anwendung des Datenschutzrechtes ist Voraussetzung, dass die personenbezogenen Daten *„in einem Dateisystem gespeichert sind oder gespeichert werden sollen"* (Art. 2 Abs. 1 DSGVO). Was ein **Dateisystem** ist, wird in Art. 4 Nr. 6 DSGVO definiert:

> *„[…] jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird."*

Biomaterialproben sind durch biotechnische Verfahren analysierbar. Die darin enthaltenen Daten sind geordnet und strukturiert erfassbar. Zwar fehlt es für die Annahme eines Dateisystems bei reinen Proben daran, dass es für deren Analyse zusätzlicher technischer Verfahren bedarf.[592] Doch genügt es für die Anwendung der DSGVO, dass die Verarbeitung **in einem Dateisystem geplant** ist. Diese Voraussetzung ist bei Biomaterialproben gegeben, die für Zwecke der Forschung genutzt werden sollen. Es kommt insofern darauf an, zu welchem Zeitpunkt die Entscheidung getroffen wird, dass Biomaterial analysiert und dateimäßig gespeichert werden soll. Ein zielgerichtetes Verhalten ist nicht erforderlich. Es genügt die Aussicht, dass die Daten in ein Dateisystem aufgenommen werden, dass nach den Umständen und der Lebenserfahrung im Regelfall mit einer Aufnahme in ein Dateisystem zu rechnen ist.[593] Die Art des Speichermediums ist unerheblich. Die DSGVO ist darauf angelegt, so weit wie möglich technologieneutral zu sein (ErwGr 15 S. 1). Als Datenträger kommen auch Biomaterialien in Betracht.[594]

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO Informationen einer **identifizierten oder identifizierbaren natürlichen Person** – des Betroffenen. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden können, sollen **alle objektiven Faktoren**, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (ErwGr 26 S. 4). Subjektive Faktoren, also z. B. die Motivation oder Intention, sich die Mittel zur Identifizierung zu verschaffen, sind unbeachtlich.[595] Für den Schutzzweck nach der DSGVO kommt es also nicht darauf an, wann ein Datenträger unter welchen Umständen entstanden ist. Relevant ist ausschließlich, dass personenbezogene Daten verarbeitet werden. Der Personenbezug kann somit vom **aktuellen technischen Stand** der Verarbeitungsmöglichkeiten abhängen.[596]

592 Weichert in DWWS, Art. 4 Rn. 84.
593 Roßnagel in SHS, Art. 2 Rn. 16; Dammann/Simitis, Art. 3 Rn. 5; Weichert in DWWS, Art. 2 Rn. 13.
594 Weichert DuD 2002, 134; Weichert in DKWW, § 3 Rn. 16.
595 Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 23.
596 Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 24.

Identifizierbarkeit ist weit auszulegen. Es muss kein direkter Personenbezug bestehen; es genügt, wenn dieser, u.U. über mehrere Zwischenschritte, hergestellt werden kann. Das ist der Fall, wenn im Umfeld der verantwortlichen Stelle Zusatzwissen vorhanden ist, das abgefragt werden könnte. Verfügt die speichernde Stelle nicht über die Zuordnungsmöglichkeit zu einem Pseudonym (s.u. Kap. 10.2), wohl aber eine andere Stelle, sind die pseudonymisierten Daten personenbezogen, wenn es nicht völlig unrealistisch ist, dass die andere Stelle ihre Kenntnisse zur Verfügung stellt. Die Möglichkeiten der Zuordnung **von Datenbeständen** zwecks Identifizierung nehmen mit der technischen Entwicklung immer weiter zu. Ein Personenbezug wird nur dann nicht angenommen, wenn Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeit einer natürlichen Person zugeordnet werden können und damit als anonym behandelt werden können (ErwGr 26 S. 5). Eine Rechtsänderung hat sich insofern mit der DSGVO nicht ergeben, wohl aber eine gewisse Klärung.

Sind von Altproben keine direkt identifizierenden Daten einzelner Personen mehr greifbar oder gespeichert, so kommt es für die Frage der Anwendbarkeit des Datenschutzrechts darauf an, wie groß der Aufwand ist, um eine Identifizierung vorzunehmen. Nach dem Willen des Gesetzgebers soll relevant sein, ob der Einsatz der Mittel zur Identifizierung nach ***„allgemeinem Ermessen wahrscheinlich"*** ist (ErwGr 26 S. 4). Daraus lässt sich ableiten, dass das Wissen eines beliebigen Dritten bzw. das gesamte „Weltwissen" nicht zugrunde gelegt werden können.[597] Es ist aber auch nicht nötig, dass die Individualisierung aufgrund einer Informationsquelle tatsächlich erfolgt. Entscheidend ist, über welches Zusatzwissen der Verantwortliche verfügen könnte.[598] Berücksichtigt werden müssen auch Informationen aus unterschiedlichen Quellen, die in ihrem Zusammenspiel die Identifizierung ermöglichen.[599]

Waren also Biomaterialproben nach früherer Ansicht als anonym anzusehen und haben sich inzwischen die **technischen Möglichkeiten weiterentwickelt**, sodass Biomaterialproben einer natürlichen Person zugeordnet werden können, dann sind diese als personenbezogen anzusehen mit der Folge, dass die DSGVO sowie das BDSG zur Anwendung kommen. Damit sind sie aber der Forschung nicht entzogen. Vielmehr kommt dann die Privilegierung für Forschungszwecke zur Anwendung mit der Folge, dass eine Weiternutzung erlaubt ist, wenn geeignete Garantien nach Art. 89 Abs. 1 DSGVO bestehen (s.o. Kap. 9). Geeignete Maßnahmen können auch solche einer weitergehenden Datenminimierung sein (s. in vorliegendem Kapitel).

Entsprechendes gilt, wenn Biomaterialproben aus einem Land stammen, in dem nach dem dort geltenden Recht ein **weiteres Verständnis von Anonymität** gilt und die Proben in Europa verarbeitet werden (s.u. Kap. 13.6).

Dies hat zur Folge, dass eindeutig identifizierende biometrische Merkmale, wie sie bei genetisch analysierbaren Biomaterialproben erlangt werden können, grundsätzlich zu einem Personenbezug führen, da z.B. über den genetischen Code generell eine Zuordnung zu einer natürlichen Person möglich ist.[600] Durch die weltweite Verfügbarkeit von genetischen Zuordnungsmöglichkeiten eröffnen sich in immer stärkerem

597 Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 24; weitergehend Klabunde in Ehmann/Selmayr, Art. 4 Rn. 17.
598 Mit ausführlicher Herleitung Roßnagel/Geminn in Dierks/Roßnagel, 157ff.
599 Karg in SHS, Art. 4 Nr. 1 Rn. 52.
600 So Karg in SHS, Art. 4 Nr. 1 Rn. 71.

Maße die Möglichkeiten zur Identifizierung eines Probengebers. Kein Personenbezug ist anzunehmen, wenn im konkreten Fall die **Identifizierung sehr unwahrscheinlich** ist.

10.2 Anonymisierung

Am wirksamsten wird die Datenminimierung durch Anonymisierung umgesetzt (ErwGr 26). Diese führt dazu, dass ein **Personenbezug vollständig beseitigt** wird und dann keine weiteren datenschutzrechtlichen Restriktionen bei der Verarbeitung beachtet werden müssen. Anonymisieren bedeutet das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (s.o. Kap. 10.1).[601]

Anders als zur Pseudonymisierung (s.u. Kap. 10.3) wird der Begriff der Anonymisierung im Normtext der **DSGVO** nicht verwendet oder definiert.[602] auf. In ErwGr 26 S. 5, 6 DSGVO wird im Rahmen der Definition von „personenbezogene Daten" darauf hingewiesen, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, also *„für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."*

Anonymisierung wird vereinzelt im allgemeinen deutschen Datenschutzrecht in den Forschungsklauseln definiert.[603] Eine explizite **Anonymisierungspflicht**, „sobald dies nach dem Forschungszweck möglich ist", gilt teilweise für alle Forschungsdaten,[604] teilweise explizit nur für solche sensitiven Daten.[605] Auf Bundesebene gilt § 27 Abs. 3 S. 1 **BDSG**:

> *„Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert."*

601 So § 3 Abs. 6 BDSGaF.
602 Hansen in SHS, Art. 4 Nr. 5 Rn. 11; Roßnagel/Geminn in Dierks/Roßnagel, 166; Weichert in DWWS, Art. 4 Rn. 74.
603 § 9 Abs. 2 S. 1 DSG M-V, § 28 Abs. 3 S. 1 ThürDSG, dazu Weichert in DWWS § 27 Rn. 28f.
604 Art. 25 Abs. 2 S. 1 BayDSG, § 25 Abs. 2 S. 1 BbgDSG, § 9 Abs. 2 S. 1 DSG M–V, § 13 Abs. 2 S. 1 NDSG, § 17 Abs. 3 S. 1 DSG NRW, § 23 Abs. 1 S. 2 DSG Saar, § 13 Abs. 2 S. 1 LDSG SH, § 28 Abs. 3 S. 1 ThürDSG.
605 § 27 Abs. 2 S. 1 BDSG, § 13 Abs. 2 S. 1 LDSG BW, § 24 Abs. 3 S. 1 HDSIG, § 17 Abs. 2 S. 2 DSG NRW, § 22 Abs. 4 S. 1 LDSG RP.

Das Anonymisieren von personenbezogenen Daten ist als eine **besondere Form der Datenverarbeitung** anzusehen und bedarf daher einer rechtlichen Grundlage.[606] Diese kann in der Einwilligung des Betroffenen erfolgen. Bei einer Anonymisierung, die das Ziel verfolgt, mit den anonymisierten Daten einen anderen Zweck, etwa Forschungszwecke, zu verfolgen, liegt die Rechtsgrundlage in der ursprünglichen Rechtsgrundlage in Verbindung mit Art. 6 Abs. 4 DSGVO.[607]

Eine Forschungsverarbeitung von personenbezogenen Daten ist unzulässig, wenn deren Zweck mit anonymen Daten erreicht werden kann.[608] Die **Erforderlichkeit einer personenbeziehbaren Verarbeitung** ist zu dokumentieren.[609]

Ob eine Anonymisierung wirksam ist, hängt von den Erkenntnisquellen ab, die der speichernden Stelle als **Zusatzwissen** zur personenbezogenen Zuordnung direkt oder indirekt zur Verfügung stehen bzw. stehen können.[610] Für die **Verfügbarkeit des Zusatzwissens** genügt die theoretische Möglichkeit. Relevant ist, ob das Zusatzwissen vernünftigerweise bei einer Einheit der verarbeitenden Stelle verfügbar sein kann.[611] Nicht beachtlich ist, dass diese Möglichkeit nicht in Anspruch genommen werden soll oder will (s.o. Kap. 10.1). Oft genügen einige Merkmalsdaten, um eine Zuordnung von Datensätzen zu konkreten Personen zu ermöglichen, selbst wenn deren Stammdaten gelöscht sind.[612] Eine absolute Anonymisierung ist bei hochkomplexen und umfangreichen Datensätzen zumeist praktisch nicht möglich. Wenn das Zusatzwissen nur unter einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann, genügt dies für die Anonymisierung. Es ist ein objektiver Maßstab anzulegen; nicht beachtlich ist, wenn der Aufwand nur für die speichernde Stelle unverhältnismäßig ist; auch das Interesse der Stelle ist nicht erheblich.[613]

Bei einer Vielzahl von Datenkategorien, die insbesondere im medizinischen Forschungsbereich von Relevanz sind, ist eine **vollständige Anonymisierung nicht möglich**.[614] Auf eine Anonymisierung kann verzichtet werden, wenn dies für eine privilegierte Zweckverfolgung gem. Art. 9 Abs. 2 DSGVO zwingend erforderlich ist. Dies muss einschränkend in die Regelung mit hineingelesen werden.[615] Eine personen-

606 Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 8.

607 BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 20.06.2020, 6ff. m.w.N; gemäß S. 8f. ist bei einer Pflicht zur Löschung die Rechtsgrundlage Art. 6 Abs. 1 i.V.m. Art. 17 Abs. 1 DSGVO.

608 Roßnagel in SHS, Art. 5 Rn. 108; Golla in Specht/Mantz, § 23 Rn. 29, 48, 53; Albrecht/Jotzo, Teil 3 Rn. 74; Paal/Pauly, Art. 89 Rn. 12; Johannes in Roßnagel 2017, § 4 Rn. 93.

609 Werkmeister/Schwaab CR 2019, 86; zur Erforderlichkeit generell Graf von Kielmansegg in TMF, 104ff.

610 Anders noch BFH, NJW 1994, 2247 = RDV 1995, 32, der meinte, dass Re-Identifizierung durch Branchenkenntnisse für eine Behandlung von Daten unschädlich ist.

611 Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 10; Dierks in Dierks/Roßnagel, 29f.; zu einem „modifizierten Verständnis der Anonymisierung S. 30ff. m.w.N., wobei es sich dabei um eine Pseudonymisierung handelt. Die Anonymisierungspflicht in § 287 Abs. 2 SGB V muss in europarechtskonformer Auslegung als Pseudonymisierungspflicht verstanden werden.

612 Hurtz, Von wegen anonym, SZ 29.07.2019, 1 mit Verweis auf Rocher/Hendrickx/de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications Vol. 10, Art. Nr. 3069 (2019), Kauß (Fn. 56), 594ff.

613 Roßnagel/Geminn in Dierks/Roßnagel, 164–167; Kühling/Buchner/Klar, Art. 4 Nr. 1 Rn. 32; Weichert in DWWS, Art. 4 Rn. 75; Schaar ZD 2016, 225; a.A. Gola/Schomerus, § 3 Rn. 44; Gola in Gola, Art. 2 Rn. 11.

614 Schaar ZD 2016, 225; Riechert DANA 2019, 211; Weichert in Kühling/Buchner, Art. 4 Nr. 13 Rn. 5 m.w.N.; zu den Methoden Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 13ff.

615 A.A. Johannes/Richter, DuD 2017, 304, die darin eine Verordnungswidrigkeit der Regelung sehen.

beziehbare Verarbeitung kann z.B. erforderlich sein zum Schutz lebenswichtiger Interessen des Betroffenen (Art. 9 Abs. 2 lit. c DSGVO).[616] Eine wirksame Anonymisierung ist oft bei Biomaterialproben, Bilddaten oder Stimmaufnahmen nicht möglich. Ist eine vollständige Anonymisierung nicht möglich oder auch nicht gewünscht, weil z.B. eine spätere Zuordnung von Datensätzen erfolgen muss, hat eine **Pseudonymisierung** zu erfolgen (s.u. Kap. 10.2).

Bei der Pflicht zur Anonymisierung und Pseudonymisierung müssen nicht sämtliche hierfür bestehenden Mittel eingesetzt werden, sondern nur solche, die dem aktuellen **Stand der Technik** entsprechen. Sind die Methoden der Datenminimierung für den Forscher nicht zugänglich und ist ihm deren Einsatz nicht zuzumuten, so kann der Einsatz dieser Methoden auch nicht gefordert werden.[617]

Mit einer Anonymisierung kann ein forschungsrelevanter **Informationsverlust** verbunden sein. Dies gilt z.B. für eine Aggregierung von Datensätzen, bei der Einzelangaben zusammengeführt werden (sog. K-Anonymität). Auch bei anderen Methoden der Anonymisierung, etwa der Verschleierung, der Merkmalsaggregierung, durch das gezielte Einführen von Merkmalsfehlern (z.B. Hinzufügung von Dummy-Datensätzen) oder das Vertauschen von Daten[618] können Inhaltsverluste entstehen, die die Wertigkeit des Forschungsergebnisses beeinträchtigen können.[619]

Von einer Anonymisierung kann abgesehen werden, wenn berechtigte **Interessen der betroffenen Personen** dies erfordern. Dies kann dann der Fall sein, wenn der Betroffene ein individuelles Interesse an den Resultaten hat, die z.B. im medizinischen Bereich in eine Behandlung einfließen sollen. Ein Betroffeneninteresse kann auch darin bestehen, dass die Rechtmäßigkeit der Verarbeitung zur eigenen Person überprüft werden soll. In solchen Fällen ist regelmäßig eine Pseudonymisierung mit File-Trennung angezeigt.

10.3 Pseudonymisierung

Um Inhaltsverluste zu vermeiden, wird bei Forschungsprojekten anstelle einer Anonymisierung oft die **Pseudonymisierung** gewählt. Diese Datenveränderung im Interesse der Datenminimierung wird in Art. 4 Nr. 5 DSGVO definiert. Danach ist

„Pseudonymisierung" 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."[620]

616 Johannes/Richter, DuD 2017, 304.
617 Weichert in DWWS, § 27 BDSG Rn. 31.
618 Wiebe 534; 23. TB LDI NRW 2017, Kap. 13.2 (S. 100); zur sog. K-Anonymität 23. TB LDI NRW 2017, Kap. 13.2 (S. 100); Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 19ff.
619 Weichert in DWWS, Art. 4 Rn. 77; Schäfer in Kipker/Voskamp, 343ff.
620 Zur Begriffsdefinition und zu den Unterschieden zwischen Art. 4 Nr. 5 und ErwGr 26, S. 2 DSGVO Roßnagel/Geminn in Dierks/Roßnagel, 175ff.

Die Pseudonymisierung wird sowohl in der DSGVO (Art. 6 Abs. 4 lit. e, 25 Abs. 1, 32 Abs. 1 lit. a, 40 Abs. 2 lit. d, 89 Abs. 1 S. 3)[621] als auch im BDSG (§ 22 Abs. 2 Nr. 6) als eine wichtige Garantiemaßnahme aufgeführt.[622] Wegen der Definition in der DSGVO verzichtet das deutsche Datenschutzrecht auf eine eigene Begriffsbestimmung. Ist eine Pseudonymisierung möglich, ohne dass die Erreichung des Forschungszwecks beeinträchtigt wird, so muss sie – als Ergebnis der Risikobewertung – grundsätzlich auch vorgenommen werden.[623] Eine gängige Form der Pseudonymisierung bei Forschungsprojekten besteht darin, dass die eine natürliche Person identifizierenden Daten (Stammdaten) durch ein per **Zuordnungsfunktion** definiertes Merkmal (Pseudonym) ersetzt werden und bei der Auswertung für Forschungszwecke statt der Stammdaten ausschließlich das Pseudonym verwendet wird.

Eine **Pseudonymisierung von Einzeldatensätzen** ermöglicht bei Langzeitstudien das Verfolgen von Einzelfällen. Mit dieser Methode können auch Daten zu einer Person aus unterschiedlichen Quellen zu unterschiedlichen Zeiten in einem geschützten Raum verarbeitet werden. Der Einsatz von Pseudonymen mit der Möglichkeit der Reidentifizierung von Einzelfällen ist dann geboten, wenn Forschungsergebnisse, z.B. bei medizinischen Spätfolgen, im Nachhinein überprüft werden können müssen. Durch die Pseudonymisierung soll ermöglicht werden, dass trotz Verzicht auf einen direkten Personenbezug keine falschen Datensatzzuordnungen und Verwechslungen erfolgen.

Pseudonymisierung gemäß der DSGVO muss ein bestimmtes Maß an **Qualität** vorweisen.[624] Soll die Pseudonymisierung eine Zuordnung für Dritte ausschließen, sodass sie für diese als anonym behandelt werden können, dann muss eine Identifizierung der Betroffenen für diese nach allgemeinem Ermessen ausgeschlossen sein. Dabei ist neben dem Ersetzen der identifizierenden Daten darauf zu achten, dass mit den Merkmalsdaten im Datensatz keine Reidentifizierung durch den Dritten möglich ist.[625] Dient dagegen die Pseudonymisierung zur Risikominimierung als Garantie für den Betroffenen, so bleiben sie für den Verantwortlichen personenbezogene Daten.[626]

Die Zuordnung der Datensätze kann technisch (z.B. Einwegverschlüsselung) oder über Pseudonymlisten vorgenommen werden. Im letztgenannten Fall sind gemäß § 27 Abs. 3 S. 3 u. 4 BDSG die **identifizierenden Angaben gesondert aufzubewahren**. Durch diese technisch-organisatorische Maßnahme soll vermieden werden, dass bei der Auswertung ein Personenbezug hergestellt wird (**File-Trennung**). Eine solche File-Trennung war im alten BDSG (§ 30a Abs. 3 S. 2) für die Markt- und Meinungsforschung vorgesehen.[627] Eine Reidentifizierung ist nur in Ausnahmefällen (wenn für Forschungszweck erforderlich, § 27 Abs. 2 S. 3 BDSG; bei Wahrnehmung von Betroffenenrechten) zulässig. Referenzlisten können beim Verantwortlichen gesondert oder bei einem Datentreuhänder (s.u. Kap. 10.4) gespeichert werden. Die Trennung erfolgt im Statistikrecht durch die Unterscheidung zwischen Hilfs- und Erhebungsmerk-

621 Roßnagel/Geminn in Dierks/Roßnagel, 174.
622 Überblick über die Landesdatenschutzgesetze bei Bernhardt/Ruhmann/Weichert, 8.
623 Johannes/Richter, DuD 2017, 302.
624 Roßnagel/Geminn in Dierks/Roßnagel, 174; Marnau DuD 2016, 430; zu den Methoden Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 24ff.
625 Roßnagel/Geminn in Dierks/Roßnagel, 182f.; Graf von Kielmansegg in TMF, 91.
626 Roßnagel/Geminn in Dierks/Roßnagel, 183f.
627 Hornung/Hofmann ZD-Beilage 4/2017, 10.

malen (vgl. § 10 BStatG). Die Trennung zwischen identifizierenden Daten und Merkmalsdaten ist in vielen Krebsregistergesetzen sowie im Arzneimittelrecht[628] gesetzlich konkretisiert. Die Identifizierungsmerkmale dürfen nur genutzt werden, soweit dies für den Forschungs- oder Statistikzweck erforderlich ist. Ist eine Individualisierung oder eine individuelle Zuordnung der Forschungsdatensätze nicht mehr nötig, sind die identifizierenden Referenzdaten zu löschen.[629]

Mit einer wirksamen Verschlüsselung oder einer Pseudonymisierung liegt keine Offenbarung von **Berufsgeheimnissen** vor, wenn die Stelle, die die Daten erhält, keine Möglichkeit zur Entschlüsselung bzw. zur Reidentifizierung hat (s.o. Kap. 6.7 am Ende).[630]

10.4 Datentreuhänderschaft u.a.

Die Pseudonyme mit den Merkmalsdaten und die Zuordnung der Pseudonyme zu den Stammdaten sind grundsätzlich getrennt zu halten (sog. **File-Trennung**). Über die Zuordnungsfunktion können die Stammdaten und das Pseudonym zusammengeführt werden (vgl. § 27 Abs. 3 S. 2 BDSG). Dadurch besteht die Möglichkeit, Datensätze aus unterschiedlichen Quellen oder aus unterschiedlichen Entstehungszeiten für Forschungszwecke ohne Namensnennung für Forschungszwecke zusammenzuführen und gemeinsam auszuwerten. Möglich ist es auch, in definierten Fällen den pseudonymisierten (Forschungs-)Datensatz wieder den Stammdaten zuzuordnen. Dies kann z.B. sinnvoll bzw. nötig sein, wenn sich aus Forschungserkenntnissen medizinische Behandlungsmöglichkeiten für eine konkrete Person ergeben und diese Daten in die Behandlung wieder eingeführt werden sollen.[631] Eine weitere Funktion eines Treuhänders bzw. einer Vertrauensstelle kann darin bestehen, Forschungsdaten treuhänderisch zu verwalten oder Einwilligungserklärungen von Betroffenen zu verwalten und deren Beachtung sicherzustellen.[632] Durch die Unabhängigkeit des Treuhänders wird gewährleistet, dass bei der Zuordnung pseudonymisierter Daten eine – idealerweise unabhängige – Drittkontrolle stattfindet.

Eine Verstärkung der Pseudonymisierungsmaßnahmen kann bei Forschungsprojekten dadurch erfolgen, dass bei **Verarbeitungsketten** für einzelne Verarbeitungsstadien (Erhebung, Speicherung, Zusammenführung, Nutzung) jeweils separate Pseudonyme genutzt werden. Dies kann notwendig sein bei hoch sensiblen Daten, die für unterschiedliche Zwecke und langfristig genutzt werden sollen, so wie dies z.B. bei Biobanken oft der Fall ist.[633]

628 Bischoff/Wiencke ZD 2019, 12.
629 Weichert in DWWS, § 27 Rn. 32.
630 Fechtner/Haßdenteufel CR 2017, 357f.; Dierks in Dierks/Roßnagel, 64; unsicher Graf von Kielmansegg in TMF, 115.
631 Weichert in DWWS, Art. 4 Rn. 67f.
632 Datenethikkommission, 127, 135; RfII, 13; Roßnagel ZD 2019, 161; Wiebe,550; Sachverständigenrat, 233f.; Martini/Hohmann NJW 2020, 3575; Metschke/Wellbrock, 44.
633 ULD, Datentreuhänderschaft in der Biobank-Forschung, Schlussbericht, Teilprojekt 2, 30.04.2009, 52ff., https://www.datenschutzzentrum.de/uploads/projekte/bdc/1-20090630-datentreuhaender-biobankenforschung-endbericht.pdf; Weichert 2018, Kap. 10.9; Wiebe, 535f.

Zu den Maßnahmen der Datenminimierung gehört es auch, dass Daten zum frühestmöglichen Zeitpunkt gelöscht oder anonymisiert werden (**Speicherbegrenzung**, Art. 5 Abs. 1 lit. e DSGVO).[634] Diese Maßnahme kommt in Betracht, wenn für Forschungszwecke von einem bestimmten Zeitpunkt an die Identifizierung von Datensätzen nicht mehr benötigt wird (Art. 89 Abs. 1 S. 4 DSGVO).[635] Eventuell genügt es, dass lediglich die Pseudonyme oder die Zuordnungsfunktionen gelöscht werden.

Mit der Einschaltung eines Treuhänders wird eine **informationelle Gewaltenteilung** erreicht. Das BVerfG hat anlässlich des Volkszählungsurteils 1983 festgestellt, dass eine solche informationelle Gewaltenteilung „unerlässlich" ist bei der Verarbeitung von Statistikdaten im kommunalen Bereich.[636] Demgemäß ist eine organisatorische Abschottung zur Wahrung der spezifischen statistischen Zweckbindung gefordert.

Diese nach nationalem Verfassungsrecht entwickelten Grundsätze lassen sich uneingeschränkt auf den europäischen Rechtsrahmen übertragen.[637] Die Notwendigkeit einer informationellen Gewaltenteilung kann auch aus der Definition der Pseudonymisierung in Art. 4 Nr. 5 DSGVO und den Grundsätzen der Datenminimierung und der Speicherbegrenzung des Art. 5 Abs. 1 lit. c und e DSGVO abgeleitet werden. Die Daten minimierende „Pseudonymisierung" erfolgt 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"*. Informationelle Gewaltenteilung lässt sich also durch **technisch-organisatorische Maßnahmen** umsetzen.[638]

Informationelle Gewaltenteilung kann auch **räumlich und personell** realisiert werden.[639] Die Notwendigkeit informationeller Gewaltenteilung besteht im öffentlichen wie im privaten Bereich.[640] Die allgemeinen Feststellungen gelten auch für die Umsetzung der Zweckbindung im Forschungsbereich. Es ist wünschenswert, dass insofern weitere gesetzliche Konkretisierungen erfolgen (s.u. Kap. 15.2).

Informationelle Gewaltenteilung ist von besonderer Bedeutung bei Treuhändern als Organisationsteil einer verantwortlichen Stelle, die auch die Forschung selbst durchführt. Dabei ist darauf zu achten, dass keine **Interessenkonflikte** zwischen der Treuhänderfunktion und weiteren Aufgaben bestehen. So darf der Treuhänder selbst keine Forschung mit den anvertrauten Daten durchführen.[641]

Derartige Interessenkonflikte können z.B. auch beim **Datenschutzbeauftragten** (s.u. Kap. 11.1) bestehen, dessen zentralen Aufgaben die Datenschutzkontrolle und die Beratung sind (Art. 39 DSGVO). Art. 38 Abs. 6 S. 2 DSGVO verbietet ihm die Wahr-

634 Weichert in DWWS, Art. 5 Rn. 46.
635 Siehe aber den Hinweis von Roßnagel ZD 2019, 162 auf die Notwendigkeit der Nachprüfbarkeit der Forschungsergebnisse.
636 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Rn. 153, NJW 1984, 428.
637 Von Lewinski in Auernhammer, Einl. BDSG Rn. 38.
638 Roßnagel, Review zum vorliegenden Gutachten, 30.
639 Vgl. § 290 Abs. 2 S. 2 SGB V zur Vertrauensstelle bzgl. der Krankenversicherungsnummer sowie § 303a Abs. 2 S. 1 SGB V zur Vertrauensstelle bei der „Datentransparenz"; Weichert DANA 2020, 21f.
640 Simitis/Hornung/Spiecker in SHS, Einl. Rn. 37; Bizer, 197.
641 Böhm/Wagner CR 1997, 625.

nehmung zusätzlicher Aufgaben und Pflichten, die zu einem Interessenkonflikt führen. Zwar sind sowohl Treuhänder wie auch Datenschutzbeauftragter unabhängig hinsichtlich der konkreten Durchführung ihrer Aufgaben im Rahmen des Forschungsvorhabens. Auch dient die Unabhängigkeit in beiden Fällen der Wahrung des Datenschutzes. Doch kann ein Datenschutzbeauftragter seine gesetzlich definierten Aufgaben der Beratung und Kontrolle nicht gegenüber sich selbst wahrnehmen. Die vertraglich definierten Aufgaben des Treuhänders liegen in der von anderen Beteiligten unabhängigen Datenverarbeitung in besonders sensiblen Bereichen. Nähme er zugleich die Aufgaben des Datenschutzbeauftragten wahr, so müsste er sich in einer zentralen Rolle bei der Datenverarbeitung selbst kontrollieren.[642]

Die Benennung eines Datenschutzbeauftragten ist unter bestimmten Voraussetzungen **gesetzliche Pflicht**, insbesondere für öffentliche Stellen sowie für nicht-öffentliche Stellen, bei denen mindestens 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind, bei denen eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO Pflicht ist, sowie bei solchen, deren Kerntätigkeit die umfangreiche Verarbeitung sensitiver Daten ist (Art. 37 DSGVO, § 38 Abs. 1 BDSG, s.u. Kap. 11.1). Besteht keine solche Benennungspflicht, so steht es einer Stelle frei, einen Datenschutzbeauftragten zu benennen (Art. 37 Abs. 4 DSGVO).[643] Eine solche Benennung ist eine organisatorische Maßnahme i.S.v. Art. 89 Abs. 1 S. 2 DSGVO.[644]

Ebenso wie in Art. 38 Abs. 6 S. 1 DSGVO ist in § 7 Abs. 2 S. 1 BDSG ausdrücklich für **öffentliche Stellen des Bundes** geregelt, dass der Datenschutzbeauftragte neben seiner Funktion gemäß der DSGVO andere Aufgaben und Pflichten wahrnehmen kann. In Satz 2 wird ausdrücklich Folgendes geregelt:

> *„Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen."*

Wird ein Datenschutzbeauftragter auf **freiwilliger Basis** ernannt, so ist streitig, ob dieser die gleichen Rechte und Pflichten wie ein obligatorisch zu benennender Datenschutzbeauftragter hat.[645] Da insofern keine verpflichtende gesetzliche Regelung besteht, kann es auch keinen rechtlichen Hinderungsgrund dafür geben, die Modalitäten bei einer freiwilligen Benennung selbst zu bestimmen.[646] Dies gilt in jedem Fall für die personellen Voraussetzungen eines Datenschutzbeauftragten, wozu auch die Frage nach der Unabhängigkeit und nach möglichen Interessenkonflikten, etwa zu einer Datentreuhänderschaft, gehört.[647]

Der zwischen den Funktionen des Treuhänders und des Datenschutzbeauftragten entstehende **Interessenkonflikt kann dadurch verringert** werden, dass der Treu-

642 Allgemein dazu Däubler in DWWS, Art. 37 Rn. 19; Drewes in SHS, Art. 38 Rn. 55f.; Heberlein in Ehmann/Selmayr, Art. 38 Rn. 21; Bergt in Kühling/Buchner, Art. 38 Rn. 40; Paal in Paal/Pauly, Art. 38 Rn. 14; Raum in Auernhammer, Art. 38 Rn. 49, 52, 54ff.; Jaspers/Reif in SJTK, Art. 38 Rn. 26f.

643 Jaspers/Reif RDV 2016, 62; Däubler in DWWS, § 38 Rn. 8; Drewes in SHS, Art. 37 Rn. 37.

644 Vgl. Heberlein in Ehmann/Selmayr, Art. 37 Rn. 32, 35.

645 Dafür: Artikel 29-Datenschutzgruppe, WP 243 rev. 01 v. 0504.2017, 24; Raum in Auernhammer, Art. 37 Rn. 67; Heberlein in Ehmann/Selmayr, Art. 11, 37; Jaspers/Reif in SJTK, Art. 37 Rn. 38; unklar: Bergt in Kühling/Buchner, Art. 37 Rn. 26; differenzierend: Drewes in SHS, Art. 37 Rn. 37; dagegen: Däubler in DSSW, § 38 Rn. 8.

646 Däubler in DSSW § 38 Rn. 8.

647 Bergt in Kühling/Buchner, Art. 37 Rn. 26.

händer hinsichtlich seiner Aufgaben besonderen Rechenschaftspflichten und Kontrollen unterworfen wird. Die Art. 37–39 DSGVO sehen allerdings nicht vor, dass ein Datenschutzbeauftragter nur für Teile einer Stelle zuständig sein kann. Deshalb ist eine separate Datenschutzaufsicht des Treuhänders rechtlich nur bei einer externen Datentreuhänderschaft möglich. In seiner Treuhänderfunktion kann ein Datenschutzbeauftragter zudem nicht die gesetzliche Unabhängigkeit nach Art. 38 Abs. 3 DSGVO für sich in Anspruch nehmen.

10.5 Keine personenbezogene Veröffentlichung

Durch die Veröffentlichung der Forschungsergebnisse werden diese einem nicht mehr überschaubaren Empfängerkreis zugänglich gemacht mit der Folge, dass die Einhaltung von Zweckbindungsregelungen praktisch nicht mehr durchsetzbar ist. Da gerade im Forschungsbereich besonders hohe Anforderungen an die Zweckbindung bestehen, muss bei der Veröffentlichung grundsätzlich gewährleistet werden, dass diese **keine personenbezogenen Daten** enthält.

Dieser Grundsatz kann nicht eingehalten werden, wenn ein Forschungsvorhaben sich **auf eine konkrete Person** bezieht und der Schutz personenbezogener Daten mit dem Öffentlichkeitsgrundsatz der Forschung in Kollision gerät. Kommt es bei der Veröffentlichung nicht auf die Identität des Probanden an, so muss eine Veröffentlichung anonymisiert oder mit einer starken Pseudonymisierung erfolgen (s.o. Kap. 10.1, Kap. 10.2). Bei medizinischen Einzelfallstudien lässt sich manchmal eine auf eine natürliche Person bezogene Veröffentlichung nicht vermeiden. Die DSGVO enthält keine explizite Regelung zu dem Fall, dass eine Verschleierung der Probandenidentität im konkreten Fall nicht möglich ist. Es kann aber auf die Öffnungsklausel des Art. 85 Abs. 1 DSGVO zurückgegriffen werden, der die wissenschaftliche Kommunikation privilegiert (s.o. Kap. 4.4).[648] Dies aufgreifend regelt § 27 Abs. 4 BDSG:

> *„Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist."*

Die Forschungsklauseln der meisten Landesdatenschutzgesetze enthalten entsprechende Regelungen.[649] Entsprechendes gilt für Landeskrankenhausgesetze.[650] Einige dieser Gesetze sind offener, wenn die Veröffentlichung davon abhängig gemacht wird, dass die *„schutzwürdigen Interessen der betroffenen Person"* nicht überwiegen[651] bzw. nicht „erheblich" überwiegen.[652] Bei medizinischer Forschung geht es regelmäßig nicht um Ereignisse der Zeitgeschichte.[653]

648 Weichert in DWWS, § 27 Rn. 34.
649 § 13 Abs. 3 LDSG BW, Art. 25 Abs. 3 BayDSG, § 25 Abs. 3 BbgDSG, § 11 Abs. 3 HmbDSG, § 24 Abs. 4 HDSIG, § 9 Abs. 3 DSG M–V, § 13 Abs. 3 NDSG, § 13 Abs. 4 LDSG SH, § 28 Abs. 4 ThürDSG.
650 Dierks 2019, 62; zu den Regelungen vor Wirksamwerden der DSGVO Schneider 2015, 123ff.
651 § 17 Abs. 3 BlnDSG, § 12 Abs. 4 SächsDSDG, ähnlich § 22 Abs. 5 LDSG RP, § 23 Abs. 3 SDSG.
652 § 17 Abs. 4 DSG NRW.
653 Dazu Weichert in DWWS, § 27 Rn. 34.

11 Datenschutzmanagement

Zwar kennt die DSGVO den Begriff des Datenschutzmanagements nicht, doch enthält sie mehrere Regelungen, die unter diesem Begriff zusammengefasst werden können. Zweck des Datenschutzmanagements ist es, die **datenschutzrelevanten Prozesse** so zu organisieren und zu dokumentieren (Art. 5 Abs. 2 DSGVO), dass sämtlichen Datenschutz-Anforderungen zu jeder Zeit genügt werden kann.[654] Das Datenschutzmanagement obliegt dem Verantwortlichen. Damit ist es letztlich die Aufgabe der jeweiligen Stellenleitung, darauf zu achten; dass alle datenschutzrechtlich geforderten Maßnahmen umgesetzt werden. Dem Datenschutzbeauftragten (s.u. Kap. 11.1) sind insofern spezielle Aufgaben übertragen. Dies ändert aber an der Letztverantwortung der Stellenleitung nichts. Im Rahmen der vorliegenden Ausarbeitung kann zum Datenschutzmanagement keine umfassende Darstellung erfolgen. Wohl aber sollen die Aspekte behandelt werden, die im Rahmen von medizinischen Forschungsprojekten von besonderer praktischer Relevanz sind. Dabei handelt es sich um die Benennung eines Datenschutzbeauftragten, die Erstellung von Verarbeitungsverzeichnissen, die Durchführung einer Datenschutz-Folgenabschätzung sowie die Notwendigkeit eines umfassenden Datenschutzkonzepts.

654 Roßnagel in SHS, Art. 5 Rn. 101, 176.

11.1 Datenschutzbeauftragter

Nach Art. 37 Abs. 1 DSGVO besteht in jedem Fall die **Verpflichtung zur Benennung** eines Datenschutzbeauftragten für öffentliche Stellen (lit. a). Bei nicht-öffentlichen Stellen besteht die Verpflichtung, wenn deren Kerntätigkeit in der systematischen Überwachung von Betroffenen (lit. b) oder in der umfangreichen Verarbeitung sensitiver Daten nach Art. 9 DSGVO (lit. c) besteht. Weiterhin besteht die Verpflichtung zu einer solchen Benennung bei nicht-öffentlichen Stellen gemäß § 38 Abs. 1 S. 1 BDSG, soweit *„in der Regel mindestens zwanzig Personen mit der automatisierten Verarbeitung personenbezogener Daten"* beschäftigt werden.[655]

Die Benennungspflicht besteht für den Verantwortlichen oder Auftragsverarbeiter und damit regelmäßig für die jeweilige **juristische Person**. Werden von dieser neben Aufgaben der (medizinischen) Forschung weitere Aufgaben wahrgenommen, so kommt es auf die Gesamtsicht an. Eine spezifische Benennung von nur für die Forschungsdatenverarbeitung zuständigen Datenschutzbeauftragten ist nicht vorgesehen. Vielmehr ist der Datenschutzbeauftragte z.B. auch für Fragen der Verarbeitung von Beschäftigtendaten oder von Daten aus dem Verwaltungs- und dem Produktionsbereich zuständig.

Datenschutzbeauftragter kann sowohl eine natürliche Person wie auch eine (externe) juristische Person sein (Art. 37 Abs. 6 DSGVO).[656] Es ist – insbesondere bei größeren Stellen – möglich, dass ein Datenschutzbeauftragter nachgeordnete Mitarbeiter mit spezialisierten Zuständigkeitsbereichen hat, d.h., dass besondere Mitarbeiter ausschließlich für den (medizinischen) Forschungsbereich zuständig sind. Die Letztverantwortung für die Aufgabenwahrnehmung bleibt aber beim Datenschutzbeauftragten (zu möglichen Interessenkonflikten s.o. Kap. 10.4).

Erfolgt die Forschungstätigkeit im organisatorischen Rahmen einer **öffentlichen Stelle**, so ist in jedem Fall ein Datenschutzbeauftragter zu benennen (Art. 37 Abs. 1 lit. a DSGVO). Dies ist der Fall bei öffentlich-rechtlichen Forschungseinrichtungen, Universitäten, Universitätskliniken, Kommunen, bei denen in Gesundheitsämtern geforscht wird, Kliniken der Bundeswehr sowie Kliniken unter Landes- oder kommunaler Verantwortung sowie bei sonstigen öffentlichen Körperschaften, Stiftungen oder Anstalten.

Der in Art. 37 DSGVO verwendete Begriff der **Kerntätigkeit** bezieht sich auf die Haupttätigkeit einer Stelle und umfasst auch solche Aufgaben, die mit einer Haupttätigkeit untrennbar verbunden sind.[657] Bei medizinischen Forschungseinrichtungen liegt in der Verarbeitung von Gesundheitsdaten deren Kerntätigkeit. Die Forschungstätigkeit von Universitätskliniken gehört zu deren Kerntätigkeit. Entsprechendes kann auch für Medizinprodukteherstellen und für Pharmaunternehmen gelten.

Eine Benennungspflicht besteht auch bei einer **systematischen Überwachung von Betroffenen** (Art. 37 Abs. 1 lit. b DSGVO). Diese knüpft an der Kritikalität der Datenverarbeitung an und basiert auf der Risikoorientierung, die der gesamten DSGVO zu

655 Geändert durch das 2. DSAnpUG-EU v. 20.11.2019, BGBl. I S. 1626, zuvor 10 Personen.
656 Jaspers/Reif in SJTK, Art. 37 Rn. 45; zweifelnd Bergt in Kühling/Buchner, Art. 37 Rn. 36 m.w.N.
657 Drewes in SHS, Art. 37 Rn. 16.

Grunde liegt.[658] Systematische Überwachung erfordert ein gezieltes, planmäßiges Vorgehen mit einer größeren Zahl von Betroffenen oder einer umfangreicheren räumlichen Ausdehnung.[659] Die Intention der Überwachung spielt keine Rolle; erfasst wird auch eine Überwachung zu Forschungszwecken, etwa im Rahmen der „NAKO-Gesundheitsstudie". Ebenso können durch diese Regelung Krankheitsregister oder Biodatenbanken erfasst sein.

Eine **umfangreiche sensitive Datenverarbeitung** begründet ebenso eine Benennungspflicht (Art. 37 Abs. 1 lit. c DSGVO). Die Verarbeitung von Daten zur Gesundheit, zu genetischen Anlagen oder zur sexuellen Disposition sind derartige sensitive Daten (Art. 9 Abs. 1 DSGVO). Der große Umfang lässt sich an der Zahl der Betroffenen festmachen, an der Größe der jeweiligen Datensätze sowie an der Verarbeitungstiefe.[660] Das reine Führen einer Patientendokumentation in einer kleineren Arztpraxis soll nicht genügen (ErwGr. 91 S. 4); verpflichtet sein sollen dagegen größere medizinische Labors und Arztpraxen, Krankenhäuser oder Beratungsstellen wie Familienhilfevereine.[661]

11.2 Verarbeitungsverzeichnis

Art. 30 DSGVO verpflichtet verarbeitende Stellen zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten, in das Angaben zu **Verantwortlichen und Auftragsverarbeitern**, zu den Zwecken, Datenkategorien, Empfängern und – wenn möglich – zu Löschfristen und technisch-organisatorischen Maßnahmen aufzunehmen sind.[662] Dies ist Teil der Dokumentationspflichten gemäß Art. 5 Abs. 2, 24 DSGVO. Das Verzeichnis soll den Aufsichtsbehörden bei Kontrollen dienlich sein, es dient aber auch der jeweiligen Stelle selbst zur Wahrnehmung von deren datenschutzrechtlichen Pflichten. Es ist zudem geeignet als Grundlage für die Erarbeitung einer Datenschutz-Folgenabschätzung und eines projektbezogenen Datenschutzkonzepts.

Zentrales Ordnungskriterium des Verarbeitungsverzeichnisses ist der **Zweck der Datenverarbeitung**. Dieser ist so präzise wie möglich zu benennen, er muss eindeutig und aussagekräftig sein; bei medizinischen Forschungsvorhaben ist also deren Fragestellung aufzuführen (s.o. Kap. 8.2).[663] Das Verzeichnis ist laufend auf dem aktuellen Stand zu halten.[664] Eine Änderung der wissenschaftlichen Fragestellung muss sich im Verzeichnis ebenso widerspiegeln wie Änderungen beim Datenumfang, bei den Betroffenen oder den Empfängern.

658 Drewes in SHS, Art. 37 Rn. 12.
659 Drewes in SHS, Art. 37 Rn. 26f.
660 Drewes in SHS, Art. 37 Rn. 23.
661 Bergt in Kühling/Buchner, Art. 37 Rn. 24; Klug ZD 2016, 317; Paal in Paal/Pauly, Art. 37 Rn.
662 DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, Stand Februar 2018, https://www.datenschutzzentrum.de/uploads/dsgvo/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf.
663 Hartung in Kühling/Buchner, Art. 30 Rn. 18.
664 Hartung in Kühling/Buchner, Art. 30 Rn. 31.

11.3 Datenschutz-Folgenabschätzung

Darüber hinausgehende Anforderungen stellt Art. 35 DSGVO, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein besonders hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Der Verantwortliche muss in diesem Fall eine Datenschutz-Folgenabschätzung[665] durchführen. Gemäß Art. 35 Abs. 3 DSGVO ist ein **besonders hohes Risiko** insbesondere anzunehmen bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, wenn automatisierte Entscheidungen (Art. 22 DSGVO) erfolgen sollen (lit. a), sowie bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO. Mit der Regelung zur Datenschutz-Folgenabschätzung wird der Risikoansatz konkretisiert, der der gesamten DSGVO zugrunde liegt.[666]

Da medizinische Forschungsvorhaben regelmäßig nicht auf **konkrete Entscheidungen** abzielen, ist Art. 22 DSGVO nicht anwendbar (Art. 35 Abs. 3 lit. a DSGVO). Etwas anderes gilt, wenn ein Forschungsprojekt so in eine medizinische Behandlung integriert ist, dass die über die automatisierte Datenverarbeitung erlangten Erkenntnisse, etwa über maschinenlernende Systeme, direkt in die Therapie einfließen.

Wenn bei medizinischen Forschungsprojekten in einem großen Umfang **Gesundheitsdaten** verarbeitet werden, was regelmäßig der Fall ist, besteht die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.[667] Entsprechendes gilt für die forschende Verarbeitung von biometrischen und genetischen Daten, Daten zum Sexualleben oder zur sexuellen Orientierung oder Daten zu bestimmten Einstellungen oder zur rassischen oder ethnischen Herkunft.[668]

Umfangreich ist eine Verarbeitung, wenn eine große Zahl von Betroffenen und eine große räumliche Verbreitung gegeben ist (ErwGr 91 S. 1). Ebenso ist von einem großen Umfang auszugehen, wenn eine Datensammlung über einen längeren Zeitraum hinweg erfolgt sowie wenn zu jeder Person eine Vielzahl von Merkmalen erfasst wird. Keine Pflicht besteht aber, wenn sich dabei die Verarbeitung auf Einzelfälle beschränkt.[669] Die Verarbeitung durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs ist nicht umfangreich (ErwGr 91 S. 4). Bei der Speicherung von Metadaten zum Zweck des Forschungsdatenmanagements kann eine Folgenabschätzung auch dadurch nötig werden, dass über die Forschenden umfassende Profile erstellt werden können.[670] Big-Data-Anwendungen können für Forschungszwecke zulässig sein, bedürfen aber regelmäßig einer umfassenden Folgenabschätzung.[671]

Gemäß Art. 35 Abs. 4, 5 DSGVO wird **von den Aufsichtsbehörden aufgelistet**, wann eine Folgenabschätzung nötig ist und wann nicht. Diese Liste findet sich im Inter-

665 Zum Begriff Friedewald u.a., 7.
666 Friedewald u.a., 17f.
667 Zu klinischen Prüfungen Bischoff/Wiencke ZD 2019, 13.
668 Roßnagel ZD 2018, 163.
669 Wedde in DWWS, Art. 35 Rn. 50; siehe aber nächster Absatz.
670 Syckor/Strufe/Lauber-Rönsberg ZD 2019, 393.
671 Raum in Ehmann/Selmayr, Art. 89 Rn. 44.

net.[672] Darin wird klargestellt, dass auch bei einer umfangreichen Verarbeitung von Sozial- und Berufsgeheimnissen eine Folgenabschätzung durchzuführen ist (dort Nr. 3). Unter Nr. 15 wird als weiterer Anwendungsfall aufgeführt:

> *„Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte".*

Unter ausdrücklicher Nennung von „Telemedizin-Lösungen" wird unter Nr. 16 als Regelbeispiel aufgeführt:

> *„Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO – auch wenn sie nicht als ‚umfangreich' im Sinne des Art. 35 Abs. 3 lit. b) anzusehen ist – sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden."*

Nicht ausdrücklich aufgeführt wird in der Liste die **Verarbeitung für Forschungszwecke**. Die dabei geltende enge Zweckbindung kann zu einem geringeren Risiko führen als bei einer Verarbeitung mit einer operativen Zielsetzung. Insbesondere bei sensitiven Daten sowie einer umfangreichen Verarbeitung bleibt aber weiterhin technisch-organisatorisch wie auch personell ein hohes Risiko bestehen. Daher kann für eine Forschungsverarbeitung in Bezug auf Art. 35 DSGVO grundsätzlich keine rechtliche Freistellung angenommen werden.[673] Dies gilt umso mehr, als die in der DSGVO vorgesehenen Privilegierungen hinsichtlich der Zweckänderung und der Betroffenenrechte normativ die DSGVO-Schutzstandards zweckbedingt reduzieren. ErwGr. 91 S. 1 nennt als einen Anlass für eine Folgenabschätzung, wenn die *„Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren"*.

Folgende **Risikoindikatoren** können im Forschungsbereich besonders relevant sein: Sensitivität und Höchstpersönlichkeit der Daten, Verletzlichkeit der Betroffenen, der Umfang der Daten bzw. die Komplexität und der Umfang der Datenverarbeitung, die systematische Beobachtung von Betroffenen, die Neuartigkeit der eingesetzten Technik, die individuelle Bewertung von Betroffenen, die Art der Datenverknüpfung, der Einsatz automatisierter Entscheidungsverfahren oder der Einsatz sog. Künstlicher Intelligenz.[674]

Bei der Durchführung der Datenschutz-Folgenabschätzung hat der Verantwortliche den **Rat des Datenschutzbeauftragten** (s.o. Kap. 11.1) einzuholen, sofern ein solcher benannt wurde (Art. 35 Abs. 2 DSGVO).[675]

Art. 35 Abs. 9 DSGVO legt dem Verantwortlichen nahe, *„den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge einzuholen."* Die-

672 DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, https://www.datenschutzzentrum.de/uploads/dsgvo/2018_10_17_DSK_DSFA-Liste-1_1.pdf.
673 Friedewald u.a., 26.
674 EDPS 2020, 24; Martin/Mester/Schiering/Friedewald/Hallinan DuD 2020, 152.
675 Jandt in Kühling/Buchner, Art. 35 Rn, 18; Martin/Schiering/Friedewald DuD 2020, 156.

ser **Standpunkt der betroffenen Personen** kann durch Patienteninitiativen oder durch Verbraucherschutzorganisationen vertreten werden.[676]

Art. 35 Abs. 7 DSGVO beschreibt die **Inhalte**, die zumindest in eine Folgenabschätzung aufgenommen werden müssen:

> *„a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*
>
> *b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;*
>
> *c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und*
>
> *d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird."*

Die in Abs. 7 genannten unabdingbaren Inhalte a) bis d) bauen aufeinander auf und sind demgemäß auch so darzustellen.[677] Die **systematische Beschreibung** kann an das Verarbeitungsverzeichnis nach Art. 30 DSGVO anknüpfen[678], darf sich jedoch nicht hierauf beschränken, da es zusätzlich auf die Systematik der Verarbeitungsschritte ankommt. Es geht also nicht nur um die Beschreibung der einzelnen zum Einsatz kommenden Verfahren, sondern um eine ablauf- bzw. prozessorientierte Gesamtschau unter Einbeziehung der Hardware, der Software, der Vernetzung, der Schnittstellen und der Rollen der Anwendenden.[679]

Ergeben sich wesentliche Änderungen in Bezug auf die Datenverarbeitung oder die Risiken, so ist eine **Fortschreibung** der Folgenabschätzung nötig.[680]

Hinsichtlich der **Form** gibt es keine expliziten normativen Vorgaben. Da die Dokumentation aber verfügbar sein und auf Nachfrage vorlegt werden können muss, bedarf es einer textlichen Darstellung, die analog oder digital vorgehalten werden kann.[681]

11.4 Datenschutzkonzept

Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen, die Rechtmäßigkeit der von ihm veranlassten Datenverarbeitung nachzuweisen. Im Rahmen dieser Gesamtver-

676 Wedde in DWWS, Art. 35 Rn. 104f.
677 Baumgartner in Ehmann/Selmayr, Art. 35 Rn. 48, Roßnagel ZD 2019, 163f.; zum Gesamtprozess Friedewald u.a., 19ff.
678 Baumgartner in Ehmann/Selmayr, Art. 35 Rn. 51; Goosen/Schramm ZD 2017, 11; Ferik in SJTK, Art. 35 Rn. 164.
679 Karg in SHS, Art. 35 Rn. 76.
680 Friedewald u.a., 33.
681 Piltz K&R 2016, 716; Sassenberg/Schwendemann in Sydow, Art. 35 Rn. 37; Ferik in SJTK, Art. 35 Rn. 163; Raum in Auernhammer, Art. 35 Rn. 39; a.A. Baumgartner in Ehmann/Selmayr, Art. 35 Rn. 49: schriftlich.

antwortung hat er vor Beginn der Verarbeitung Risikoanalysen und Datenschutz-Folgenabschätzungen vorzunehmen (s.o. Kap. 11.3) und ein Verarbeitungsverzeichnis (s.o. Kap. 11.2) zu erstellen. Weitere **zu dokumentierende Umstände** sind die technisch-organisatorischen Maßnahmen (Art. 32 DSGVO) sowie im Fall von „Verletzungen des Schutzes personenbezogener Daten", also von Datenlecks, Meldungen an die Aufsichtsbehörde sowie evtl. an die Betroffenen (Art. 33, 34 DSGVO).

Eine **ausdrückliche Verpflichtung** zur Erstellung eines umfassenden Datenschutzkonzeptes enthält die DSGVO nicht.[682] Etwas anderes gilt für die Durchführung von Forschungsprojekten durch öffentliche Stellen in Hessen, wo § 24 Abs. 1 S. 2 HDSIG Folgendes regelt:

> *„Vor dem Beginn des Forschungsvorhabens ist ein Datenschutzkonzept zu erstellen, das der zuständigen Aufsichtsbehörde auf Nachfrage vorzulegen ist."*

Eine weitergehende Regelung enthält § 75 Abs. 1 S. 4 SGB X. Danach ist im Fall einer Übermittlung von Sozialdaten für Forschungszwecke *„der nach Absatz 4 Satz 1 zuständigen Behörde [...] ein Datenschutzkonzept vorzulegen. Zuständige Behörde ist nach Abs. 4 S. 1 die oberste Bundes- oder Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist."* Dabei handelt es sich regelmäßig um das jeweilige Sozialministerium, welches die Datenübermittlung gemäß Abs. 4 S. 1 zu genehmigen hat. In dem Datenschutzkonzept soll der Antragsteller, also der forschende Verantwortliche, darlegen, dass er die technischen und organisatorischen Anforderungen des Datenschutzes sowie des Grundsatzes der Datenminimierung erfüllt.[683] Dabei wird auf Art. 32 DSGVO sowie § 22 Abs. 2 BDSG Bezug genommen.

Auch wenn es eine ausdrückliche Regelung nicht gibt, vertreten die deutschen Datenschutzbehörden die Ansicht, dass die für ein Forschungsprojekt Verantwortlichen den *„zur Prüfung der ethischen und datenschutzrechtlichen Vereinbarkeit zuständigen Stellen"* ein **„Forschungskonzept"** vorlegen müssen gemeinsam mit der Prüfung der Vereinbarkeit mit dem Datenschutzrecht, einschließlich der *„zugrunde liegenden Beweggründe sowie die Sicherstellung der o.g. Sicherheitsmaßnahmen"*.[684] Eine entsprechende Dokumentationspflicht kann mit Art. 5 Abs. 2 DSGVO begründet werden, der den Verantwortlichen dazu verpflichtet, die Einhaltung der in Art. 5 Abs. 1 DSGVO geregelten Datenschutzgrundsätze nachweisen zu können einschließlich der in Art. 89 DSGVO auferlegten Garantien.

Eine präzise Umschreibung dessen, was ein Datenschutzkonzept enthalten muss, ist den Regelungen nicht zu entnehmen. Wohl aber ergibt sich aus einer Gesamtschau der rechtlichen Vorgaben, dass die **Inhalte des Datenschutzkonzeptes** eine umfassende Darstellung der Datenverarbeitung enthalten müssen, aus der sich deren Rechtmäßigkeit ableiten lässt. Erfasst werden damit

- das Verarbeitungsverzeichnis (s.o. Kap. 11.2),
- die Darstellung der technisch-organisatorischen Maßnahmen (s.o. Kap. 9) und
- die Datenschutz-Folgenabschätzung (s.o. Kap. 11.3).

682 Bischoff/Wiencke ZD 2019, 13: Empfehlung; Weichert in Kühling/Buchner § 22 Rn. 43.

683 BT-Drs. 18/12611, 109.

684 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DS-GVO v. 03.04.2019; Weichert ZD 2020, 23; als Empfehlung bei klinischen Prüfungen Bischoff/Wiencke ZD 2019, 13.

Nimmt eine Stelle die Privilegierungen bei der Zweckbindung (s.o. Kap. 8.1) sowie hinsichtlich der Einschränkung der Betroffenenrechte (s.u. Kap. 12) in Anspruch, so sind hierfür geeignete Garantien vorzusehen, die zu dokumentieren sind ebenso wie die Abwägung der Interessen der forschenden Stelle mit den Betroffeneninteressen. Letztlich handelt es sich bei diesen vorzunehmenden **Abwägungen** um zu dokumentierende Bestandteile der Datenschutz-Folgenabschätzung.[685]

Es bestehen keine Vorgaben für die Form der o.g. Dokumente. Insbesondere das Verarbeitungsverzeichnis und die Folgenabschätzung können in separate Dokumente aufgenommen werden. Es empfiehlt sich jedoch, diese in **ein umfassendes Dokument** aufzunehmen, das allen Anforderungen genügt. Dieses Dokument sollte in einer Weise strukturiert sein, dass es zeitlich fortgeschrieben werden kann.

685 Karg in SHS, Art. 35 Rn. 13.

12 Betroffenenrechte

Betroffene haben nach den Regelungen der DSGVO (Art. 12–22) sehr weit gehende Rechte. Diese sind jedoch zugunsten der Forschung durch die DSGVO sowie durch Regelungen der Mitgliedstaaten nach Art. 89 Abs. 2 DSGVO **eingeschränkt oder gar ausgeschlossen**.

Gemäß Art. 12 Abs. 1 S. 1 DSGVO trifft der Verantwortliche geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Regelung zielt darauf ab, die Betroffenenrechte so einfach wie möglich durchsetzbar zu machen. Zu diesem Zweck soll für die Betroffenen **größtmögliche Transparenz** hergestellt werden und sind Maßnahmen verpflichtend, mit denen die konkrete Inanspruchnahme der Rechte erleichtert wird.[686]

Die Betroffenenrechte, insbesondere das Auskunftsrecht (s.u. Kap. 12.3), bestehen, wenn der Betroffene und dessen Daten **eindeutig identifiziert** sind. Personenbeziehbarkeit genügt (Art. 4 Nr. 1 DSGVO). Gemäß Art. 12 Abs. 2 S. 2 DSGVO darf der Verantwortliche die Wahrnehmung der Betroffenenrechte nur verweigern, *„wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren."* Bei Zweifeln an der Identität ist Art. 12 Abs. 6 DSGVO anwendbar:

686 Däubler in DWWS, Art. 12 Rn. 1.

> *„Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er unbeschadet des Artikels 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.“*

Für die eindeutige Identifizierung bedarf es nicht der Namensnennung. Wurde dem Betroffenen ein **Pseudonym** zugeordnet, so können die Betroffenenrechte auch über die Verwendung des Pseudonyms in Anspruch genommen werden.[687] Bei medizinischen Forschungsprojekten dürfte der Betroffene selbst ein ihm zugeordnetes Pseudonym selten kennen. In diesen Fällen hängt die Wahrnehmung der Betroffenenrechte davon ab, ob die vom Betroffenen genannten Klardaten im Rahmen des Forschungsvorhabens einem Pseudonym und hierüber erschlossenen Daten zugeordnet werden können.

12.1 Informationspflichten

Die DSGVO und auch das sonstige Datenschutzrecht sieht eine Vielzahl von Informationspflichten vor. Transparenz über die Datenverarbeitung *„in einer für die betroffene Person nachvollziehbaren Weise“* ist die grundlegende Bedingung dafür, dass die Betroffenen ihre informationelle Selbstbestimmung wahrnehmen können. Transparenz ist ein wesentliches Element des Grundsatzes, dass personenbezogene Daten *„nach **Treu und Glauben**“* zu verarbeiten sind (Art. 5 Abs. 1 lit. a DSGVO).[688]

Bei den Transparenzvorschriften kann unterschieden werden. Zum einen gibt es Pflichten, denen auf Initiative des Betroffenen entsprochen werden muss (sog. **Pull-Hinweise**). Hier ist in erster Linie der Auskunftsanspruch nach Art. 15 zu benennen (s.u. Kap. 12.3). Daneben gibt es Informationspflichten, die an bestimmte Situationen anknüpfen mit *„komplexen, technischen oder unerwarteten Verarbeitungsvorgängen“*[689], etwa an eine gemeinsame Verantwortlichkeit (Art. 26 Abs. 2 S. 2 DSGVO, s.o. Kap. 5.4) oder an eine Verletzung des Schutzes durch ein Datenleck (Breach Notification, Art. 34 DSGVO). Daneben gibt es generell geltende, allein von einer personenbezogenen Datenverarbeitung abhängig gemachte Informationspflichten. Diese sind in den Art. 12–14 DSGVO geregelt. Bei unabhängig von einem Tätigwerden des Betroffenen bestehenden Transparenzpflichten spricht man von **„Push-Hinweisen“**.[690]

Hinsichtlich der **Form der Information** gibt es im Datenschutzrecht generell keine zwingenden Vorgaben. Diese können analog, also z.B. über Hinweisblätter, oder digital erfolgen. Bei einer digitalen Präsentation bietet sich bei komplexen Sachverhalten eine Mehrebenen-Vorgehensweise an. Weitere mögliche elektronische Formen sind kontextbezogene „Just-in-time-Pop-up-Hinweise“, 3D-Touch- oder Hover-over-Hinweise sowie Datenschutz-Dashboards[691]. Als ergänzende, nicht-schriftliche For-

687 Dix in SHS, Art. 12 Rn. 36.
688 Artikel 29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 01 v. 11.04.2018, 8.
689 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 5, 8.
690 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 25.
691 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 25.

men können Videos, Smartphone- oder IoT-Sprachmeldungen hinzutreten, ebenso Bildgeschichten, Infografiken oder Ablaufdiagramme.[692]

Um den Betroffenen die Erfüllung der Transparenzpflicht klar und einfach zu vermitteln, bedarf es einer verständlichen **Bezeichnung der Information**. Zu empfehlen sind Begriffe wie „Datenschutzhinweis", „Datenschutzbestimmungen" oder „Datenschutzerklärung".[693]

Die Erteilung der geforderten Information sollte grundsätzlich gemäß den berechtigten Erwartungen und dem Grundsatz von Treu und Glauben zum frühestmöglichen **Zeitpunkt** erfolgen (Art. 12 Abs. 3, 13 Abs. 1 3, Art. 14 Abs. 4 DSGVO).[694] Dies gilt insbesondere für eine Verarbeitung für Forschungszwecke, bei denen die Betroffenen keine Überraschung in Bezug auf die Verarbeitung erleben sollten.[695]

Im Interesse einer gesicherten **Dokumentation** beim Betroffenen sollte eine Form gewählt werden, bei der der Betroffene die Möglichkeit hat, die erlangte Information mit nach Hause zu nehmen, auszudrucken oder abzuspeichern. Gerade bei langfristigen Speicherungen und Datennutzungen, wie sie im Forschungsbereich oft erfolgen, sollte den Betroffenen dauerhaft der Zugang zur Information gesichert sein.[696] Auf Wunsch des Betroffenen kann eine mündliche Erläuterung erfolgen. Aushänge oder ausschließlich mündliche Informationen genügen nur, wenn eine Zuordnung zum Betroffenen hinreichend dokumentiert ist (Art. 12 Abs. 1 S. 2 DSGVO).[697] Die beim Verantwortlichen liegenden Dokumentations- und Rechenschaftspflichten müssen beachtet werden (Art. 5 Abs. 2 DSGVO).[698]

Art. 13 Abs. 1 und 14 Abs. 1 DSGVO verpflichten den Verantwortlichen, die Betroffenen **zu informieren über** den Namen und die Kontaktdaten des Verantwortlichen, den Datenschutzbeauftragten, die Verarbeitungszwecke, die berechtigten Interessen und die Rechtsgrundlage, die verarbeiteten Daten, die Empfänger sowie über eine etwaig geplante Übermittlung ins Drittausland[699]. Gemäß Art. 13 Abs. 2 und 14 Abs. 2 DSGVO sind zusätzlich folgende Informationen zur Verfügung zu stellen: die Speicherdauer, Angaben zu den Betroffenenrechten einschließlich des Beschwerderechts bei einer Aufsichtsbehörde sowie das Widerrufsrecht im Fall einer Einwilligung sowie bei automatisierten Entscheidungen Informationen über die involvierte Logik und über deren Tragweite. Im Fall einer Erhebung bei einer dritten Stelle ist zudem die Information über die Datenherkunft zu erteilen (Art. 14 Abs. 2 lit. f DSGVO). Die in den Absätzen 1 und 2 genannten Informationspflichten bestehen kumulativ und ohne Einschränkungen.[700]

Bei der Information der Betroffenen sollten, ähnlich wie vor einem „informed consent", also einer Einwilligung in ein medizinisches Forschungsprojekt, neben dem Zweck **zudem folgende Aspekte** dargestellt werden: die zum Einsatz kommenden

692 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 14.
693 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 17.
694 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 17 f., 21, 30.
695 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 28 f.
696 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 22.
697 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 15.
698 Roßnagel in SHS Art. 5 Rn. 183; Weichert in DWWS, Art. 5 Rn. 72.
699 Zur Informationspflicht bei EU-Schweiz-Kooperationen Mausbach ZD 2019, 454.
700 Däubler in DWWS, Art. 13 Rn. 17; Bäcker in Kühling/Buchner, Art. 13 Rn. 20; Dix in SHS, Art. 13 Rn. 13.

Methoden, die erwarteten Ergebnisse, mit dem Projekt verknüpfte Interessen und Erwartungen sowie mögliche Unannehmlichkeiten und Risiken für die Teilnehmenden.[701]

Bei der **Benennung des Zwecks** genügt nicht die Angabe „für medizinische Forschungszwecke". Vielmehr muss der verfolgte Zweck bzw. müssen die verfolgten Zwecke zwar knapp, aber so präzise wie möglich benannt werden (s.o. Kap. 8.2). Nur so ist es dem Betroffenen möglich zu überprüfen, ob und inwieweit eine Verarbeitung sich im Rahmen des vorgegebenen Zwecks hält.[702] Im medizinischen Bereich wird mit einer Verarbeitung oft eine Vielzahl von Zwecken verfolgt. In Art. 9 Abs. 2 DSGVO werden typische Zwecke aufgeführt: Gesundheitsvorsorge, Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich, Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich (lit. h), Schutz vor Gesundheitsgefahren, Gewährleistung hoher Qualitäts- und Sicherheitsstandards, bei der Versorgung, bei Arzneimitteln oder Medizinprodukten (lit. i) oder Forschungszwecke (lit. j).

Die Zwecke sollten so präzise wie möglich benannt werden.[703] Dabei kann sich die Information auf die **primären Zwecke** beschränken. Sekundäre Zwecke, die aufgrund von gesetzlichen Regelungen typischerweise mit verfolgt werden (z.B. Abrechnung mit Krankenkassen bzw. -versicherungen, Qualitätssicherung, Wirtschaftlichkeitskontrolle) müssen nicht aufgeführt werden (vgl. Art. 14 Abs. 5 lit. c DSGVO).[704] Dies würde gerade im medizinischen Bereich den Umfang der Information sprengen und zugleich die Betroffenen überfordern. Gesetzliche Zwecke ergeben sich zwangsläufig und können von den Betroffenen zumeist unabhängig von der konkreten Datenerhebung durch ein Studium der einschlägigen Gesetze erkannt werden.

Ist absehbar, dass Daten für medizinische **Forschungszwecke** genutzt werden sollen, ohne dass geklärt ist, für welche Art der Forschung, dann muss dies in dieser offenen Weise dargestellt werden. Im Interesse ausreichender Transparenz sollte zudem ein Hinweis darauf gegeben werden, wie die Betroffenen aktuelle nähere Informationen über die Forschungsnutzung erhalten können. Die Konferenz der Datenschutzbehörden führt folgende *„zusätzliche Sicherungsmaßnahmen zur Gewährleistung von Transparenz"* auf:

- *„Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren **Forschungsplanes**, der die geplante Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet*
- *Ausarbeitung und **Dokumentation** im Hinblick auf das konkrete Forschungsprojekt, wieso in diesem Fall eine nähere Konkretisierung nicht möglich ist*

*Einrichtung einer **Internetpräsenz**, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden"*[705]

701 EDPS 2020, 20.

702 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 10; Däubler in DWWS, Art. 13 Rn. 9; Bäcker in Kühling/Buchner, Art. 13 Rn. 25; Ingold in Sydow, Art. 13 Rn. 15.

703 Däubler in DWWS, Art. 13 Rn. 9; Dix in SHS Art. 13 Rn. 8.

704 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 39f.

705 DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DS-GVO v. 03.04.2019.

Erfolgt später eine **Zweckänderung**, so muss die Information vor der Verwendung für den neuen Zweck und darf nicht später erfolgen (Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO).[706] Entsprechendes gilt auch, wenn eine Forschungsnutzung in einem weiteren Umfang erfolgen soll, als dies ursprünglich mitgeteilt worden ist. Der Betroffene muss nicht neu über schon erteilte Informationen unterrichtet werden, also z.B. über den Verantwortlichen oder den Datenschutzbeauftragten.[707] Soweit eine Änderung erfolgt, also insbesondere über den neuen Zweck oder über eine neue Rechtsgrundlage (s.o. Kap. 7.3), ist eine Information aber nötig.[708] Bei einem nachträglichen Wechsel von einer Einwilligung zu einer gesetzlichen Rechtsgrundlage, die nur ausnahmsweise zulässig ist (s.o. Kap. 7.3), muss hierauf ausdrücklich hingewiesen werden.[709]

Dem Betroffenen muss in jedem Fall die **Rechtsgrundlage** mitgeteilt werden (Art. 13 Abs. 1 lit. c, 14 Abs. 1 lit. c DSGVO).

Die DSGVO unterscheidet bei den Informationspflichten danach, ob die Daten direkt **bei dem Betroffenen erhoben** werden (dann Art. 13) oder nicht (dann Art. 14).[710]

Begrifflich ist eine Erhebung beim Betroffenen nach Art. 13 DSGVO auch gegeben, wenn dieser vom Erhebungsvorgang **keine Kenntnis** hat, etwa weil die Erhebung verdeckt erfolgt. Die Art. 13, 14 DSGVO sollen sicherstellen, dass in jedem Fall die für die Wahrnehmung des Rechts auf informationelle Selbstbestimmung nötige Transparenz hergestellt wird.[711]

Bei einer **Erhebung beim Betroffenen** nach Art. 13 DSGVO ist es für die Informationsverpflichtung unerheblich, auf welcher Rechtsgrundlage diese erfolgt. Grundlage kann eine informierte Einwilligung sein (Art. 9 Abs. 2 lit. a, Art. 7 DSGVO). Diese ist regelmäßig einzuholen, wenn vom Betroffenen im Rahmen eines medizinischen Forschungsprojektes gezielt Gesundheitsdaten erfasst werden. Eine Datenerhebung beim Betroffenen kann auch im Rahmen einer medizinischen Behandlung erfolgen, wenn der Behandelnde die Daten auch für Forschungszwecke nutzt. Rechtsgrundlage für die Datenerhebung ist dann regelmäßig ein Behandlungsvertrag (Art. 6 Abs. 1 lit. b, Art. 9 Abs. 2 lit. h DSGVO i.V.m. § 630a BGB) und evtl. eine ergänzende Einwilligung (Art. 9 Abs. 2 lit. a DSGVO). Art. 13 DSGVO ist auch anwendbar, wenn die Erhebung auf gesetzlicher Grundlage erfolgt und die erhebende Stelle selbst die Weiterverarbeitung für Forschungszwecke vornimmt (Art. 6 Abs. 1 lit. c, e, Art. 9 Abs. 2 DSGVO).

Werden mit einer Datenerhebung vorrangig Behandlungszwecke verfolgt und ist eine Sekundärnutzung der Daten für Forschungszwecke von Anfang an geplant, so ist schon bei der Erhebung auf beide Zwecke hinzuweisen.[712] Erfolgt die Entscheidung über die Sekundärnutzung später, so ist die Information spätestens vor der Weiterverarbeitung zu geben (Art. 13 Abs. 3 DSGVO). Derartige Sekundärnutzungen werden

706 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 20; Dix in SHS, Art. 13 Rn. 20.
707 Dix in SHS, Art. 13 Rn. 21.
708 Franck in Gola, Art. 13 Rn. 30.
709 A.A. Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 16: verstößt in jedem Fall gegen Treu und Glauben.
710 Generell zu Problemen bei der Datenerhebung für Forschungszwecke Tinnefeld/Schrempf RDV 1997, 241ff.
711 Dix in SHS, Art. 13 Rn. 6.
712 Dix in SHS, Art. 13 Rn. 20; Artikel 29-Datenschutzgruppe WP 260 rev. 01, 17f., 21, 30.

in **Krankenhausgesetzen** ausdrücklich erlaubt.[713] Eine Information gegenüber den Patienten kann z.B. wie folgt formuliert sein: „Wir verarbeiten Daten über Ihre Person, Ihre Erreichbarkeit, Ihre Krankenversicherung sowie im Rahmen der Behandlung Informationen über Ihre Gesundheit. Diese Daten werden, soweit hierfür erforderlich, für Abrechnungszwecke (bei gesetzlich Versicherten gemäß SGB V verarbeitet. Zudem können Ihre Gesundheitsdaten gemäß § xyz Krankenhausgesetz für Forschungszwecke in pseudonymisierter Form (durch das behandelnde Krankenhaus/die Fachabteilung des Krankenhauses, in einem Krankheitsregister) verarbeitet werden. Für nähere Informationen können Sie sich an den Datenschutzbeauftragten des Krankenhauses wenden: xyz".

Anders als bei anderen Betroffenenrechten (s.u. Kap. 12.2 sowie Kap. 12.3–12.5, Kap. 12.7 u. Kap. 8) besteht hinsichtlich der Informationspflicht bei einer Datenerhebung beim Betroffenen **keine Sonderregelung** beim Verfolgen von Forschungszwecken.[714] Dies ist angemessen, da in diesen Fällen keine Gründe erkennbar sind, aus denen durch die Information der Forschungszweck beeinträchtigt werden könnte. Erfolgt die Erhebung beim Betroffenen, so muss die Information zu diesem Zeitpunkt gegeben werden.

Erfolgt die **Datenerhebung bei einem Dritten**, so muss gemäß Art. 14 Abs. 3 DSGVO die Information der Betroffenen erteilt werden

> *„a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,*
>
> *b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder*
>
> *c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung."*

Bei einer Erhebung bei Dritten ist eine Information des Betroffenen gemäß Art. 14 Abs. 5 lit. b DSGVO nicht erforderlich, wenn und soweit *„die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit."*

Die Feststellung der **Unmöglichkeit** einer Benachrichtigung erfordert ein klares Ja oder Nein. Möchte der Verantwortliche diese Ausnahme geltend machen, so muss er die Faktoren darlegen, die ihn tatsächlich daran hindern, die Informationen zu über-

713 Graf von Kielmansegg in TMF, 108; Überblicke über die Regelungen in Landes-Krankenhausgesetzen finden sich bei Schneider, 310ff. (Stand 2015); Dierks 2019, 37ff.

714 Werkmeister/Schwaab CR 2019, 87, Rn. 18.

mitteln. Sofern die Faktoren, welche diese Unmöglichkeit begründen, später wegfallen, sollte der Verantwortliche die Information dann unverzüglich veranlassen.[715]

Für einen **unverhältnismäßigen Aufwand** können folgende Anhaltspunkte beachtlich sein: *„die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien"* (ErwGr 62 S. 2, 3).[716] Der Ausnahmetatbestand kann bei der Auswertung öffentlich zugänglicher Daten einschlägig sein oder wenn eine Erhebung durch Dritte erfolgt, die mit den Forschenden in keiner Verbindung stehen.[717] Wegen des Ausnahmecharakters soll eine enge Auslegung erfolgen.[718] Unverhältnismäßigkeit kann dadurch gegeben sein, dass eine herangezogene Datenquelle alt ist und der Versuch, die Betroffenen ausfindig zu machen, einen hohen Aufwand verursachen würde.[719] An die Stelle einer individuellen Benachrichtigung kann bei einem unverhältnismäßigen Aufwand eine allgemeine Veröffentlichung treten (ähnlich Art. 34 Abs. 3 lit. c für eine Breach Notification). Eine Pflicht hierzu besteht nicht generell, sondern nur im Rahmen einer Verhältnismäßigkeitsprüfung als geeignete Garantie.[720] Eine angemessene Garantie kann in einer weitgehenden Datenminimierung liegen (s.o. Kap. 10).[721]

Eine **Gefährdung der Forschungsziele** kann eine Ausnahme für die Informationspflicht begründen. So kann ein vorläufiges Zurückhalten der Informationen geboten sein, wenn nur durch verdeckte Nachforschungen die erforderlichen Informationen gewonnen werden können.[722] Die gezielte Täuschung von Betroffenen steht im Widerspruch zu den Informationspflichten der DSGVO. Sie kann aber ausnahmsweise nötig sein, wenn bestimmte Informationen eine Voreingenommenheit der Probanden zur Folge hätten und dadurch die Forschungsergebnisse verfälscht würden. In derartigen Fällen bedarf es zusätzlicher Sicherungsmaßnahmen, etwa eines positiven Votums einer Ethikkommission, sowie einer nachträglichen Information.[723]

12.2 Betroffenenrechtseinschränkung bei privilegierten Forschungszwecken

Eine Einschränkung von Betroffenenrechten ist in Art. 89 Abs. 2 DSGVO vorgesehen, wenn Daten u.a. für Forschungszwecke verarbeitet werden:

> *„Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, können vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1 des vorliegenden Artikels im Unionsrecht oder im Recht der Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäß der Artikel 15, 16, 18 und 21 vor-*

715 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 35.
716 Knyrim in Ehmann/Selmayr, Art. 14 Rn. 45.
717 Werkmeister/Schwaab CR 2019, 87, Rn. 17.
718 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 37.
719 Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 38.
720 Bäcker in Kühling/Buchner, Art. 14 Rn. 62; Werkmeister/Schwaab CR 2019, 87, Rn. 1; anders wohl Knyrim in Ehmann/Selmayr, Art. 14 Rn. 56 mit dem Argument, bei den vorliegenden Zwecken sei das Informationsinteresse der Betroffenen generell als gering zu veranschlagen.
721 Dix in SHS, Art. 14 Rn. 23.
722 Vgl. Bäcker in Kühling/Buchner, Art. 14 Rn. 59; Artikel 29-Datenschutzgruppe, WP 260 rev. 01 v. 11.04.2018, 39.
723 EDPS 2020, 21 mit dem Hinweis, dass hierüber eine weitere Klärung nötig ist.

gesehen werden, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.“

Die Regelung enthält eine **Öffnungsklausel** für den nationalen oder europäischen Gesetzgeber im Hinblick auf Forschungs- und Statistikzwecke, bei denen **Ausnahmen von den strengen Regeln** der DSGVO zugelassen werden im Hinblick auf das Auskunftsrecht der Betroffenen (Art. 15), das Recht auf Berichtigung (Art. 16), das Recht auf Einschränkung der Verarbeitung (Art. 18) und das Recht auf Widerspruch (Art. 21), vorausgesetzt, dass in den Gesetzen kompensierende Garantien vorgesehen sind.

Diese Regelung ist nicht wegen **Art. 85 Abs. 2 DSGVO** überflüssig, der eine weitergehende Öffnungsklausel enthält.[724] Art. 89 Abs. 2 DSGVO verfolgt nicht den Schutz der Meinungs- und Informationsfreiheit, sondern ausschließlich den Schutz der Forschungsfreiheit (s.o. Kap. 4.4).[725]

Bei sämtlichen Ausnahmen ist eine **prognostische Verhältnismäßigkeitsprüfung** vorzunehmen. Dabei können Wirtschaftlichkeits- und Praktikabilitätsaspekte berücksichtigt werden. Die Wahrnehmung der Betroffenenrechte soll die Durchführung privilegierter Forschung nicht verkomplizieren, unwirtschaftlich oder gar unmöglich machen. Es darf dabei aber keine unverhältnismäßige Rechtsverkürzung für die Betroffenen erfolgen.[726]

Die Privilegierung hinsichtlich der Betroffenenrechte kann – parallel zur Privilegierung des Zwecks – nur für solche Forschungsvorhaben gelten, an denen ein **öffentliches Interesse** besteht.[727] Ein intransparente oder ausschließlich private Interessen verfolgendes Forschungsprojekt kann im Rahmen der Grundrechtsabwägung nicht die in Art. 89 Abs. 2 DSGVO vorgesehene Vorrangregelung für die Forschung rechtfertigen (s.o. Kap. 3.3 u. Kap. 3.4). Die Ausführungen zur erleichterten Zweckänderung (s.o. Kap. 8.1) gelten auch für die Beschränkung der Betroffenenrechte. Diese Auslegung ist – trotz des grundsätzlich weit auszulegenden Forschungsbegriffs (s.o. Kap. 3.2) – zwingend wegen der mit der Beschränkung der Betroffenenrechte verbundenen Grundrechtseingriffe.

Die Einschränkung der genannten Betroffenenrechte muss „**notwendig**“ sein. Es muss eine qualifizierte Erforderlichkeitsprüfung erfolgen.[728] Bei der Auslegung dieses Begriffs ist weder eine enge noch eine weite Auslegung angesagt, da hier zwei Grundrechte miteinander in Ausgleich gebracht werden müssen. Eine prognostische Unsicherheit muss in Kauf genommen werden. Dies eröffnet aber keinen diffusen Beurteilungsspielraum.[729] Abgestellt werden muss auf das Forschungsvorhaben im Einzelfall.[730] Im Rahmen des jeweiligen Forschungsprojektes kann aber eine abstrakte, also generalisierende pauschale Abwägung stattfinden, wenn schon mit einer Prü-

724 So aber Pötters in Gola, Art. 89 Rn. 12f.; so wohl auch Greve in Auernhammer, Art. 89 Rn. 13; Hense in Sydow, Art. 89 Rn. 13.
725 Buchner/Tinnefeld in Kühling/Buchner, Art. 89 Rn. 24.
726 Pauly in Paal/Pauly, Art. 89 Rn. 14; Greve in Auernhammer, Art. 89 Rn. 12.
727 So wohl auch BMH, Art. 89 Rn. 36 vgl. EDPS 2020, 2, mit Verweis auf das EU-Urheberrecht, 11.
728 Caspar in SHS, Art. 89 Rn. 64; generell Bizer, 190ff.; a.A. zur Markt- und Meinungsforschung, soweit diese überhaupt privilegiert ist, Hornung/Hofmann, ZD-Beilage 4/2017, 11.
729 So aber Krohm in Gola/Heckmann, § 27 Rn. 37.
730 Hense in Sydow, DSGVO, Art. 89 Rn. 14.

fung zu einzelnen Datensätzen eine ernsthafte Beeinträchtigung des Forschungsprojektes verbunden wäre.[731]

Soweit möglich, sind Umsetzungsdefizite der Datenschutzgrundsätze (Art. 5 Abs. 1) durch **geeignete Garantien** gemäß Art. 89 Abs. 1 DSGVO zu kompensieren.[732] Mit der Regelung muss also nicht in jedem Einzelfall eine Interessenabwägung sichergestellt werden. Es genügt, wenn im Regelfall (voraussichtlich, typischerweise) die Betroffenenrechte die Realisierung des Forschungsvorhabens verhindern.[733]

Der Europäische Datenschutzbeauftragte meint, dass **zusätzliche Kosten** allein eine Verweigerung der Betroffenenansprüche nicht rechtfertigten.[734] Diese Ansicht ignoriert, dass der Gesetzestext eine Verhältnismäßigkeitsprüfung fordert und hierbei Aufwandserwägungen nicht ausschließt. Richtig ist aber, dass der Ausschluss der Betroffenenrechte nur bei unverhältnismäßig hohen Kosten gerechtfertigt sein kann. Es bedarf einer Abwägung zwischen dem öffentlichen Forschungsinteresse und den Betroffenenrechten. Bei der Abwägung besteht für den Verantwortlichen kein Abwägungsspielraum; seine Entscheidung ist voll überprüfbar.[735] Über die geeigneten Garantien muss in jedem Fall sichergestellt werden, dass ein vollständiger Ausschluss der Wahrnehmung der Betroffenenrechte verhindert wird.[736]

In Umsetzung der Öffnungsklausel des Art. 89 Abs. 2 DSGVO enthält **§ 27 Abs. 2 S. 1 BDSG** unter fast wörtlicher Wiederholung[737] folgende Regelung:

> *„Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist."*

Entsprechende Regelungen finden sich auch in den **Landesdatenschutzgesetzen**: § 13 Abs. 4 S. 1 LDSG BW, § 17 Abs. 4 S. 1 Bln DSG, § 11 Abs. 4 HmbDSG, § 24 Abs. 2 S. 1 HDSIG, § 13 Abs. 5 NDSG, § 17 Abs. 5 DSG NRW, § 23 Abs. 4 DSG Saar, § 12 Abs. 5 SächsDSDG, § 13 Abs. 5 LDSG SH, § 28 Abs. 5 ThürDSG, ähnlich Art. 25 Abs. 4 BayDSG, § 9 Abs. 5 DSG M-V. In Brandenburg ist auch ein „unverhältnismäßiger Aufwand" generell bei Betroffenenrechten als Ausnahmetatbestand vorgesehen.[738]

Die Einschränkung der Betroffenenrechte in § 27 Abs. 2 BDSG gilt (anders als § 27 Abs. 1 BDSG) für alle Kategorien personenbezogener Daten, nicht nur für sensitive Daten gemäß Art. 9 Abs. 1 DSGVO. Voraussetzung für die Einschränkung der Betroffenenrechte ist, dass deren Wahrnehmung die Forschungs- und Statistikzwecke **unmöglich macht oder ernsthaft beeinträchtigt**. Zu beachten ist, dass mit modernen technischen Instrumenten Arbeitserleichterungen möglich sind. Deren Potential ist vor einem Rechtsverzicht voll auszuschöpfen. Hierfür bedarf es in jedem Fall im Rahmen

731 So wohl auch Pötters in Gola, Art. 89 Rn. 20.
732 Pauly in Paal/Pauly, Art. 89 Rn. 15.
733 Kühling/Buchner/Tinnefeld, Art. 89 Rn. 24.
734 EDPS 2020, 21.
735 A.A. Gola/Heckmann-Krohm § 27 Rn. 37.
736 So wohl auch Caspar in SHS, Art. 89 Rn. 64f.
737 Johannes/Richter DuD 2017, 303.
738 § 25 Abs. 5 BbgDSG; s.a. Bernhardt/Ruhmann/Weichert, 7.

des Datenschutzkonzeptes des Forschungsvorhabens einer dokumentierten Begründung (s.o. Kap. 11.4). Eine Einschränkung ist nicht bei jeder Unmöglichkeit oder ernsthaften Beeinträchtigung zulässig.

Die Einschränkungen gelten für jeden Einzelfall der Wahrnehmung der Betroffenenrechte. Da das Vorliegen der Gründe für die Verweigerung der Betroffenenrechte aber nicht vom Einzelfall abhängt, sondern zumeist dem jeweiligen konkreten Forschungsprojekt strukturell immanent ist, empfiehlt es sich, bei der Erarbeitung des Datenschutzkonzepts zu dem Forschungsprojekt grundsätzlich überprüfbare, **generell geltende Aussagen** zur Einschränkung der Betroffenenrechte und zu deren Begründung aufzunehmen (s.o. Kap. 11.4).[739] Das Geltendmachen der Betroffenenrechte bedingt, dass der Betroffene von der Verarbeitung seiner Daten überhaupt Kenntnis erlangt. Durch die Einschränkung des Auskunftsanspruchs wird deshalb auch eine Beeinträchtigung der weiteren Betroffenenrechte bewirkt.

Wenn bei der Grundrechtsabwägung zwischen Forschungsfreiheit und Datenschutz **Aufwandsaspekte** im Vordergrund stehen, kommt es zumeist auf die Zahl der Betroffenen und deren Zuordenbarkeit an. Ist nur eine Person Gegenstand der Forschung oder sind es nur wenige Personen, deren Daten eindeutig zugeordnet werden können, so kann der Aufwand eine Verweigerung der Betroffenenrechte nicht rechtfertigen.[740]

Unmöglichkeit ist dann gegeben, wenn die Wahrnehmung der Betroffenenrechte die Durchführung des Projektes und das Gewinnen der angestrebten Erkenntnisse unmöglich macht oder wenn die Umsetzung der Betroffenenrechte praktisch nicht möglich ist. Letzteres ist gegeben, wenn die Zuordenbarkeit der Betroffenendaten nicht besteht ist und deshalb keine Kontaktaufnahme erfolgen kann (vgl. Art. 11 Abs. 2 DSGVO).[741]

12.3 Auskunftsanspruch

Der Auskunftsanspruch des Betroffenen ist in Art. 15 DSGVO geregelt:

> *„(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:*
>
> *a) die Verarbeitungszwecke;*
>
> *b) die Kategorien personenbezogener Daten, die verarbeitet werden;*
>
> *c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;*

739 Weichert in DWWS, § 27 BDSG Rn. 19.
740 Weichert in DWWS, § 27 BDSG Rn. 17.
741 Weichert in DWWS, § 27 BDSG Rn. 20.

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen."

Der Auskunftsanspruch des Betroffenen erstreckt sich auf **alle Einzeldaten** eines Betroffenen. Dies schließt auch personenbezogene oder personenbeziehbare Daten mit ein, die in Auswertung der ursprünglich vorhandenen Daten gewonnen wurden. Ausschlaggebend ist, dass die Daten zum Zeitpunkt des Auskunftsbegehrens vorhanden und dem Betroffenen zuzuordnen sind.[742]

Hat der europäische oder der nationale Gesetzgeber Gebrauch von der Öffnungsklausel in Art. 89 Abs. 2 DSGVO Gebrauch gemacht, so besteht keine Auskunftspflicht, wenn die Auskunftserteilung die Forschung **unmöglich machen oder ernsthaft beinträchtigen** würde. Ob und in welchem Stadium des Forschungsprojektes dies im Einzelfall anzunehmen ist, hängt vom Einzelfall ab. Relevant ist, dass die Daten noch als Einzeldatensatz vorhanden und nicht aggregiert sind. Bei aggregierten Daten fehlt in der Regel der Personenbezug.

In der Gesetzesbegründung zu § 27 BDSG wird als Beispiel dafür, dass eine umfassende Auskunft einen Forschungszweck **unmöglich machen** würde, genannt, dass die zuständige Ethikkommission zum Schutz des Betroffenen eine Durchführung des Forschungsprojektes für diesen Fall untersagen würde.[743] Setzte eine Forschungsfragestellung die Unkenntnis des Betroffenen in Bezug auf bestimmte Angaben zu

742 Däubler in DWWS, Art. 15 Rn. 8; Bäcker in Kühling/Buchner, Art. 15 Rn. 8f.; Dix in SHS, Art. 15 Rn. 13.
743 BT-Drs. 18/11325, 99.

seiner Person voraus, so würde insofern eine Auskunftserteilung die Durchführung des Projektes insgesamt vereiteln.

Das Recht auf Auskunft kann z.B. im Bereich der Verhaltensforschung eine **methodische Hürde** darstellen, wenn und solange der Betroffene zur Durchführung über den Verlauf im Unklaren gehalten werden muss, um das Forschungsziel zu erreichen.[744]

Ist ein Einzeldatensatz vorhanden und lässt sich dieser beim Verantwortlichen selbst, bei dessen Auftragsverarbeiter oder bei einem Dritten (z.B. gemeinsam Verantwortlichen) über ein **Pseudonym eindeutig zuordnen**, so ist die Auskunft nicht unmöglich. Dies ist insbesondere der Fall, wenn zu den betroffenen Probanden oder Patienten eine Zuordnungsliste vorliegt. Je größer der Zuordnungsaufwand ist, umso ernsthafter kann eine Beeinträchtigung vorliegen. Fehlt es an einem Zuordnungspseudonym und wäre eine Identifizierung des Betroffenen lediglich noch über Merkmalsdaten möglich, so ist i.d.R. eine Zuordnung nur noch mit einem unverhältnismäßigen Aufwand möglich, was zur Auskunftsverweigerung berechtigt.

Erfolgt die **Zuordnung über eine dritte Stelle**, etwa einen Treuhänder, nicht durch die forschende Einrichtung selbst, so verfügt diese nicht mehr über die zur Auskunftserteilung nötigen Informationen. Gemäß Art. 11 Abs. 1 DSGVO ist ein Verantwortlicher *„nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren."* Zur „Einhaltung dieser Verordnung" gehört auch die Umsetzung der Betroffenenrechte in den Art. 12ff. DSGVO.[745] Im Interesse der Datensparsamkeit ist eine Stelle verpflichtet, Daten zum frühestmöglichen Zeitpunkt zu pseudonymisieren. Art. 11 DSGVO entbindet den Verantwortlichen von einer weiteren Datenbeschaffung.[746]

Etwas anderes gilt, wenn in einem arbeitsteiligen Forschungsprojekt im Forschungsinteresse Prozesse zur **Reidentifizierung von pseudonymisierten Einzeldatensätzen** ausdrücklich vorgesehen sind. Dies ist z.B. dann der Fall, wenn Forschungsergebnisse wieder in die individuelle Behandlung eingeführt werden sollen. Dies ist auch der Fall, wenn über den Dritten (Treuhänder) eine spätere Kontaktierung vorgesehen ist oder wenn der Dritte die ausdrückliche Funktion hat, Betroffenenauskünfte zu erteilen. Angesichts des der DSGVO innewohnenden Risikoansatzes besteht in solchen Fällen ein Prozess zur Reidentifizierung, der auch jenseits der Auskunft ein spezifisches Risiko einer Zuordnung zum Betroffenen begründet. Die organisatorische Aufgabenteilung zwischen verschiedenen Stellen darf sich nicht zu Lasten der Betroffenen auswirken.[747] I.d.R. dürfte in solchen Fällen ohnehin eine gemeinsame Verantwortlichkeit gegeben sein, woraus sich die Auskunftspflicht gegenüber jedem der Verantwortlichen ableitet (s.o. Kap. 5.3).

Erfolgt dagegen eine eindeutige, aber **nicht rückgängig zu machende Pseudonymisierung** der Identitätsdaten, etwa durch Verwendung eines festgelegten Einweg-Hash-Verfahrens, so ist ein Verantwortlicher regelmäßig nicht in der Lage, den Betroffenen zu identifizieren, solange ihm nicht die für das Hash-Verfahren genutzten

744 Weichert in DWWS, § 27 BDSG Rn. 23.
745 Weichert in Kühling/Buchner, Art. 11 Rn. 7, 9.
746 Weichert in Kühling/Buchner, Art. 11 Rn. 15.
747 EuGH 05.06.2018 – C-210/16 (Facebook Fanpage), Rn. 42; EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 70.

Identitätsdaten des Betroffenen erneut mitgeteilt werden. Wendet sich ein Betroffener mit seinen glaubhaft gemacht Identitätsdaten an einen Verantwortlichen mit einem Auskunftsersuchen, dann stellt er die zusätzlichen Informationen bereit, mit denen eine Identifizierung möglich ist (Art. 11 Abs. 2 S. 2 DSGVO). Dem Verantwortlichen oder, im Fall einer Zwischenschaltung eines Treuhänders, diesem, ist es möglich, die Identitätsdaten erneut zu pseudonymisieren bzw. zu hashen. So entsteht regelmäßig das Pseudonym, mit dem der Datensatz dem Betroffenen zuzuordnen ist. Ist durch das eingesetzte Hash-Verfahren nicht ausgeschlossen, dass unterschiedliche Identitätsdaten zu einem gleichen Pseudonym führen, muss vor der Auskunftserteilung mithilfe weiterer (z.B. Merkmals-)Daten eine Plausibilitätskontrolle erfolgen. Voraussetzung für die Auskunftserteilung aus einwegpseudonymisierten Daten ist, dass der Betroffene genau die Identitätsdaten bereitstellt, die als Grundlage für das Erstellen des Pseudonyms genutzt werden.

Die Frage einer ernsthaften Forschungsbeeinträchtigung durch die Auskunft kann u.a. davon abhängen, wieviel Betroffene typischerweise aus realistischer Sicht eine Auskunft beantragen. Handelt es sich bei Auskunftsersuchen um Ausnahmefälle, so ist ein größerer Aufwand zumutbar als bei Projekten, bei denen Auskunftsersuchen regelmäßig erfolgen. Dies kann z.B. bei Bevölkerungsstudien mit starker Pseudonymisierung angenommen werden. Eine ernsthafte Beeinträchtigung liegt vor, wenn die Auskunftserteilung das **Projekt insgesamt infrage** stellt.

Gegen einen Auskunftsanspruch nach Art. 15 DSGVO kann nicht ein **Betriebs- und Geschäftsgeheimnis** des Verantwortlichen vorgebracht werden. Der Forschende mag den Wunsch haben, Dritten seine Art der Forschungsauswertung als „Forschungsgeheimnis" vorzuenthalten. Dieses Interesse hat aber in Bezug auf den einzelnen Betroffenen seine Grenze, wenn zu diesem (noch) ein Personenbezug besteht.[748]

Ergänzend zum mehrere Betroffenenrechte einschränkenden § 27 Abs. 2 S. 1 BDSG (s.o. Kap. 12.2) regelt **§ 27 Abs. 2 S. 2 BDSG**[749] für das Auskunftsrecht folgende weitere Einschränkungsmöglichkeit:

> *„Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde."*

Diese Regelung ist nicht von der Öffnungsklausel des Art. 89 Abs. 2 DSGVO gedeckt. Der gesetzliche Verweis auf einen **unverhältnismäßigen Aufwand**[750] beruft sich auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i DSGVO. Der wesentliche Anwendungsfall liegt darin, dass ein Forschungsvorhaben mit besonders großen Datenmengen arbeitet.[751] Ein unverhältnismäßiger Aufwand kann gegeben sein, wenn eine große Zahl von Betroffenen erfasst wird und diese ihre Rechte (voraussichtlich) wahrnehmen. Ein solcher Aufwand kann sich auch daraus ergeben, dass für die Zuordnung der

748 Bischoff/Wienecke ZD 2019, 12; Dix in SHS, Art. 23 Rn. 35; Albrecht ZD 2017, 51; Weichert in DWWS, § 29 Rn. 6; zur Auskunftsverweigerung über das Zustandekommen von Scores ausführlich Weichert DANA 3/2018, 133f.

749 In Fortführung der zuvor geltenden § 33 Abs. 2 S. 1 Nr. 5 i.V.m. § 34 Abs. 7 sowie § 19a Abs. 2 Nr. 2 BDSGaF.

750 Die Formulierung wird auch verwendet bei 34 Abs. 1 Nr. 2, 35 Abs. 1 BDSG; BT-Drs. 18/11325, 99; kritisch zur Berufung auf die Öffnungsklausel des Art. 23 Greve in Auernhammer, § 27 Rn. 22.

751 BR-Drs. 110/17, 99.

Betroffenen ein hoher Aufwand betrieben werden muss, weil die Daten nur noch pseudonym vorliegen oder vorhandene Adressen wegen Zeitablaufs mit großer Wahrscheinlichkeit nicht mehr aktuell sind.[752] Für eine Auskunftsverweigerung kann der Aufwand für die Erreichbarkeit des Betroffenen nur in seltenen Fällen eine Rechtfertigung sein, da der Betroffene mit seinem Auskunftsersuchen regelmäßig hinreichende Informationen zu seiner Erreichbarkeit gibt. Wohl aber kann der Aufwand dadurch unverhältnismäßig werden, dass die Überprüfung der Identität der Anspruchsteller und der Glaubhaftmachung große Ressourcen beansprucht bzw. beanspruchen würde. Ausschlaggebend kann auch die Kommunikationsform sein: So ist ein postalische und eine analoge Bearbeitung aufwändiger als eine teilweise automatisierte Bearbeitung mit digitaler Kommunikation. So ermöglicht der neue Personalausweis eine sichere digitale Identifizierung. Mithilfe von Dashboards oder durch einen digitalen Datentransfer können auch umfangreiche Datensätze an einen Betroffenen übermittelt werden. Ob ein Forschungsprojekt solche Instrumente nutzen und anbieten muss, hängt davon ab, ob dies im Einzelfall zumutbar ist.

Die Beschränkung der Auskunft kann schließlich im **Interesse des Betroffenen** liegen, etwa wenn die Analyseergebnisse den Betroffenen belasten oder seinem Selbstbild widersprechen können. Eine Auskunft über Forschungsergebnisse kann zu Selbstzweifeln und seelischen Schäden führen. In § 630g Abs. 1 BGB ist die Einschränkung der Einsicht in die Patientenakte aus therapeutischen Gründen vorgesehen. Eine Übertragung dieses Rechtsgedankens auf medizinische Forschungsdaten ist nicht angebracht, da mit Forschung vorrangig keine individuellen therapeutischen Zwecke verfolgt werden. Es können aber Maßnahmen im Rahmen der Auskunftserteilung ergriffen werden, die eine schädigende Wirkung einer Auskunft minimieren oder ausschließen, etwa indem die Auskunftserteilung im Rahmen eines Beratungsgesprächs erfolgt oder indem weitere erläuternde medizinische Informationen zur Verfügung gestellt werden. Auf der Grundlage von Art. 23 Abs. 1 lit. i DSGVO kann zum Schutz des Betroffenen in Fällen erheblicher Gefährdungen die Auskunft eingeschränkt werden. Hierfür bedarf es aber einer – bisher nicht bestehenden – eigenständigen Rechtsvorschrift.[753]

Wegen der Schicksalhaftigkeit insbesondere von genetischen Anlagen, etwa hinsichtlich der Disposition für nicht behandelbare Krankheiten, besteht bzgl. dieser Informationen ein verfassungsrechtlich abgeleitetes **Recht auf Nichtwissen**. Die Menschenwürde des Art. 1 Abs. 1 GG bzw. Art. 1 GRCh sowie das allgemeine Persönlichkeitsrecht schützen die auf sich selbst bezogene Selbsterkenntnis oder das *„Recht auf das je eigene Menschenbild"*.[754] Die Kenntnis über erblich angelegte Dispositionen kann das persönliche Wohlbefinden massiv beeinträchtigen. Sie kann die Wahrung der informationellen Selbstbestimmung des Betroffenen wie auch von dessen biologischen Verwandten beeinträchtigen.[755]

752 Werkmeister/Schwaab CR 2019, 88, Rn. 24; Weichert in DWWS, § 27 BDSG Rn. 16; Graf von Kielmansegg in TMF, 100.

753 Dix in SHS, Art. 23 Rn. 33; Weichert in DWWS, § 27 BDSG Rn. 22; Bäcker in Kühling/Buchner, Art. 23 Rn. 30; Roßnagel/Geminn in Dierks/Roßnagel, 131, 215ff., 224f.

754 Höfling in Sachs, Grundgesetzkommentar, 2003, Art. 1 GG Rn. 30; Schmidt-Bleibtreu/Hofmann/Hopf, GG, 12. Aufl. 2001, Art. 1 Rn. 51ff.; Stockter, Verbot genetischer Diskriminierung, Berlin 2008, 488ff.

755 Weichert DuD 2002, 141f.; Graf von Kielmansegg in TMF, 113f.

Informationelle Selbstbestimmung findet auch darin ihren Ausdruck, dass sich ein Betroffener dafür entscheiden können muss, nur einen Teil von Untersuchungsergebnissen zur Kenntnis zu nehmen (**Recht auf Teilwissen**).[756]

Um über die Frage entscheiden zu können, in welchem Umfang ein Betroffener von seinem Recht auf Nichtwissen Gebrauch machen möchte, ist es erforderlich, dass er eine hinreichende Vorstellung davon hat, was Wissen bzw. Nichtwissen für ihn und sein Umfeld zur Folge haben kann. Um insofern eine Absicherung vorzunehmen, sehen § 8 Abs. 1, 9 Abs. 1 S. 2, Abs. 3 GenDG für genetische Untersuchungen gesteigerte formelle Anforderungen an die Einwilligung des Betroffenen hierzu vor: ausdrückliche Erklärung gegenüber einem Arzt, Differenzierung bzgl. des Umfangs, Bestimmungsrecht über den Umfang des gewünschten Nichtwissens, angemessene Bedenkzeit, umfassende Dokumentation der Aufklärung. § 9 GenDG fordert eine **umfassende Aufklärung**, u.a. über *„die Bedeutung der zu untersuchenden genetischen Eigenschaften für eine Erkrankung oder gesundheitliche Störung sowie die Möglichkeiten, sie zu vermeiden, ihr vorzubeugen oder sie zu behandeln [Abs. 2 Nr. 1], sowie das Recht der betroffenen Person auf Nichtwissen, einschließlich des Rechts, das Untersuchungsergebnis oder Teile davon nicht zur Kenntnis zu nehmen, sondern vernichten zu lassen [Abs. 2 Nr. 5].“*

Diese Regelungen des GenDG sind gemäß § 7 Abs. 1 GenDG nur für **diagnostische genetische Untersuchungen** anzuwenden, also für solche Untersuchungen im medizinischen Bereich.[757] Für andere Zwecke (Abstammungsklärung, Versicherungsbereich, Arbeitsleben) werden geringere Anforderungen gestellt. Ausdrücklich nicht anwendbar ist das Gesetz gemäß § 2 Abs. 2 Nr. 1 GenDG „zu Forschungszwecken“. Begründet wurde dies vom Gesetzgeber damit, dass es bei der genetischen Forschung um die allgemeine Erforschung von Ursachenfaktoren menschlicher Manifestationen geht, die nicht in konkrete Maßnahmen gegenüber einzelnen Personen mündet. Insofern sollten die allgemeinen Regelungen, etwa des Datenschutzrechts, gelten.[758] Sofern im Rahmen von Forschungsvorhaben gewonnene Informationen des Probanden zu seiner Genetik für dessen medizinische Behandlung verwendet werden, sind die o.g. Regelungen der §§ 7ff. GenDG jedoch entsprechend anzuwenden, wenn sich die Informationen auf medizinische Feststellungen beziehen.[759]

Wegen der Relevanz genetischer Daten für die **biologische Verwandtschaft** kann es zu Verwandtenkonflikten kommen zwischen dem Recht auf Wissen und auf Nichtwissen, z.B. wenn jemand Auskunft zu seinen Daten erlangt und hierdurch ein Familienmitglied ungewollt von genetischen Anlagen Kenntnis erlangt, die wahrscheinlich auch bei ihm vorliegen.[760]

Da zu beauskunftende Daten auch **Angaben über Dritte** enthalten können (z.B. bei Gendaten), kann eine Auskunft eine Gefährdung von deren Recht auf Nichtwissen darstellen. Die Regelung des Art. 15 Abs. 4 DSGVO, wonach das Recht auf Kopie durch die Rechte Dritter begrenzt wird, betrifft nur den Fall, dass neben Angaben zum Betroffenen solche von Dritten aufgeführt sind, und erstreckt sich gemäß dem Wortlaut

756 Stockter in Prütting, § 1 GenDG Rn. 7.
757 Stockter in Prütting, Vor §§ 7 GenDG Rn. 1.
758 BR-Drs. 633/08, 35.
759 Stockter in Prütting, § 2 GenDG Rn. 32.
760 Weichert DuD 2019, 150f.

nicht auf eine Auskunftserteilung durch reine Inhaltswiedergabe.[761] Bei Betroffenendaten mit Drittbezug kann aber auf Art. 23 Abs. 1 lit. i DSGVO zurückgegriffen werden, wonach eine Auskunftsverweigerung zum Schutz „anderer Personen" zulässig ist. § 29 Abs. 1 S. 2 BDSG sieht eine Ausnahme vom Auskunftsanspruch vor, *„soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden Interessen eines Dritten, geheim gehalten werden müssen"*. Die Anwendbarkeit dieser Norm auf eine datenschutzrechtliche Drittbetroffenheit ist aber fraglich. Teilweise wird die Ansicht vertreten, dass diese Regelung gegen Unionsrecht verstößt.[762]

Umfasst eine Auskunft zwangsläufig auch **Informationen über Dritte** mit persönlichkeitsrechtlicher Relevanz, so ist bei Auskunftserteilung der Betroffene hierauf hinzuweisen sowie darauf, dass diesen Dritten ein Recht auf Nichtwissen oder Teilwissen zustehen kann und dass sie dies bei der Kommunikation über ihr Auskunftsergebnis berücksichtigen müssen. Für die „Weiterverarbeitung" von Auskunftsergebnissen ist der Betroffene selbst verantwortlich.[763]

12.4 Recht auf Berichtigung

Art. 16 DSGVO regelt das „Recht auf Berichtigung": „Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen." Dieses Recht wird ausdrücklich in Art. 8 Abs. 2 S. 2 GRCh gewährleistet (s.o. Kap. 2.1). Es dient der Durchsetzung des in Art. 5 Abs. 1 lit. d DSGVO postulierten **Grundsatzes der „Richtigkeit"**. Dabei geht es darum, die Realität in Bezug auf den Betroffenen korrekt darzustellen.[764]

Die Antwort auf die Frage, welche Daten richtig sind, ist jeweils vom **Kontext** abhängig, in dem die Daten verarbeitet werden. Geht es um eine operative Nutzung von Daten, kommt es regelmäßig auf deren Aktualität an. Richtig sind aber auch Daten, wenn diese unter Zeitangabe korrekte Angaben über vergangene Sachverhalte darstellen. Bei medizinischen Forschungsvorhaben sind Ablaufdaten, also die Entwicklung eines Gesundheitsmerkmals über einen bestimmten Zeitablauf, von Bedeutung.

In vielen Fällen werden Dokumentationszwecke verfolgt, bei denen es nicht (nur) auf die inhaltliche Richtigkeit ankommt, sondern vorrangig darauf, wie ein Vorgang dokumentiert wurde und dass die **Dokumentation nicht verfälscht** ist. Dies gilt z.B. für die ärztliche Dokumentationspflicht gemäß § 10 MBOÄ. Um wahrheitsgemäß dargestellte, aber inhaltlich nicht der Wahrheit entsprechende Dokumentationen

761 Däubler in DWWS, Art. 15 Rn. 31; ausführlich zum Anspruch auf eine Kopie gem. Art. 15 Abs. 3 DSGVO Korch/Chatard CR 2020, 438ff.

762 Dix in SHS, Art. 23 Rn. 23; für eine Anwendbarkeit und eine Abwägung bei Drittbetroffenheit Herbst in Kühling/Buchner, § 29 Rn. 10; Weichert in DWWS, § 29 Rn. 9; zu weit gehend, weil auf eine Abwägung verzichtend, Lapp in Gola/Heckmann, § 29 Rn. 15; Gräber/Nolden in Paal/Pauly, § 29 Rn. 10.

763 Weichert DuD 2019, 150f.

764 Weichert in DWWS, Art. 5 Rn. 51; zur Notwendigkeit, insofern Standards zu entwickeln, Health Ethics Policy Lab, 76.

richtigzustellen, kann es geboten sein, korrigierende Ergänzungen in eine Dokumentation aufzunehmen.[765] Die Richtigkeit eines (möglicherweise inhaltlich falschen) Dokuments kann z.B. im Rahmen der Erforschung von medizinischen Dokumentations- oder Behandlungsfehlern von Bedeutung sein.

Der Grundsatz der Richtigkeit der Daten spielt in **Forschungskontexten** eine zentrale Rolle, da es Aufgabe der Forschung ist, neue Erkenntnisse zu erlangen, also die Wahrheit über bestimmte Fakten, Zusammenhänge oder Entwicklungen zu erkennen. Eine unrichtige Datengrundlage führt zwangsläufig zu unrichtigen oder zumindest zu verfälschten Erkenntnissen.

Angesichts des Anspruchs auf Wahrhaftigkeit von Forschung ist es verblüffend, dass Art. 89 Abs. 2 DSGVO und in der Folge § 27 Abs. 2 BDSG bei der forschenden Zweckverfolgung Ausnahmen zulassen, *„wenn der Berichtigungsanspruch die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind."*

Hinsichtlich der **in die Forschung einfließenden Daten** sind wenige Anwendungsfälle vorstellbar, wonach unrichtige Daten aus Gründen der Zweckverfolgung verarbeitet werden müssen.

Da Forschung irren kann und zu unrichtigen **Forschungsergebnissen** führen kann, ist die Ausnahmeregelung aber gerechtfertigt: Forschung steht in der Pflicht zur Wahrheit, die im wissenschaftlichen Diskurs gesucht wird (s.o. Kap. 3.2). Diesem Diskurs soll sich der Forschende nicht dadurch entziehen können, dass er sich auf seine Berichtigungspflicht nach Art. 16 DSGVO beruft. Unrichtige Forschungsergebnisse können darauf beruhen, dass falsche Daten als Forschungsgrundlage verwendet wurden. Auch um diese Fehler nachvollziehen zu können, kann eine Weiterspeicherung und -verarbeitung der unrichtigen Daten nötig sein.

Erweisen sich personenbezogene Forschungsergebnisse als falsch, so besteht – analog zur ärztlichen Dokumentationspflicht – die Möglichkeit zur Aufnahme einer **Gegendarstellung oder ergänzenden Richtigstellung**. Hierzu kann eine Pflicht bestehen, wenn durch diese „Bedingung" oder „Garantie" die Ausnahme vom Grundsatz der Richtigkeit kompensiert wird (Art. 89 Abs. 2 DSGVO).[766]

12.5 Einschränkung der Verarbeitung

Art. 18 Abs. 1 DSGVO gibt dem Betroffenen ein „Recht auf Einschränkung der Verarbeitung", wenn die Daten vom Betroffenen bestritten werden (lit. a), trotz einer unzulässigen Verarbeitung im Betroffeneninteresse eine Löschung nicht in Frage kommt (lit. b), trotz Wegfalls der ursprünglichen Erforderlichkeit die Nutzung für die Umsetzung von Rechtsansprüchen nötig sein kann (lit. c) oder im Fall eines Betroffenenwiderspruchs dessen Berechtigung unklar ist (lit. d). Das Rechtinstitut des Art. 18 DSGVO entspricht dem der **Sperrung** nach altem deutschen Datenschutzrecht

765 Weichert in DWWS, Art. 5 Rn. 53.

766 Dix in SHS, Art. 16 Rn. 18; zum Recht auf Gegendarstellung BVerfG 08.02.1983 – 1 BvL 20/81, BVerfGE 63, 131 (142f.); BVerfG 09.04.2018 – 1 BvR 840/15, Rn. 11, NJW 2018, 2250.

(z.B. §§ 20 Abs. 3, 35 Abs. 3 BDSGaF). Die Zulässigkeit der Verarbeitung wird auf bestimmte enge Zwecke „beschränkt".

Die **Beschränkung des Rechts** aus Art. 18 DSGVO nach Art. 89 Abs. 2 DSGVO und § 27 Abs. 2 BDSG soll verhindern, dass im Laufe eines Forschungsvorhabens durch die Wahrnehmung des Betroffenenrechts dessen Ablauf beeinträchtigt wird oder die Repräsentativität verloren geht. Es genügt nicht, entsprechende Beeinträchtigungen zu vermuten, vielmehr bedarf es einer dokumentierten nachvollziehbaren und plausiblen Begründung.[767]

12.6 Recht auf Datenübertragbarkeit

Art. 20 DSGVO begründet erstmals ein „Recht auf Datenübertragbarkeit":

> *„(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.*
>
> *(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.*
>
> *(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. […]"*

Eine Umsetzung dieser völlig neuen Regelung, die das Vorliegen der technischen Möglichkeiten für einen Austausch voraussetzt[768], also die Vereinbarung von Standards für den Datenaustausch, ist bisher noch nicht erfolgt. Daher gibt es zu deren Auslegung noch **keine praktischen Erfahrungen**.

Das Recht auf Übertragbarkeit beschränkt sich auf Daten, die der Betroffene einem Verantwortlichen **bereitgestellt** hat. Voraussetzung hierfür ist ein Willensakt, etwa im Rahmen einer Einwilligung oder eines Vertrags, was regelmäßig eine Erhebung beim Betroffenen (Art. 13 DSGVO) und nicht bei einem anderen Verantwortlichen (Art. 14 DSGVO) voraussetzt.[769] Es war offensichtlich die Intention des Gesetzgebers, auch von den Betroffenen generierte Internet-, Kfz- oder Smartmeter-Nutzungsdaten

767 EDPS 2020, 21; Weichert in DWWS, § 27 Rn. 25.
768 Däubler in DWWS, § 20 Rn. 3.
769 Kamann/Braun in Ehmann/Selmayr, Art. 20 Rn. 13; Schürmann in Auernhammer, Art. 20 Rn. 24; Härting, Rn. 729.

mit einzubeziehen.[770] Es soll also nicht darauf ankommen, dass die Erstellung der Daten durch den Betroffenen selbst bewusst erfolgt ist, sondern darauf, dass Daten auf Grundlage einer willentlichen Aktion entstanden sind, wobei die Hoheit über die Verarbeitung ausschließlich beim Verantwortlichen liegen kann.[771] Insofern sind auch medizinische Messdaten, etwa MRT-Bilder, EEG-Aufnahmen oder Röntgenbilder, bereitgestellt. Von Art. 20 DSGVO erfasst sein sollen auch Wearable-Daten, also vom Betroffenen am Körper durch Mobilsysteme erhobene gesundheitsrelevante Daten.[772]

Ebenso erfasst sein müssten damit auch beim Betroffenen erhobene oder von diesem abgegebene **Biomaterialproben** (z.B. Haare, Speichel, Urin oder Blut). Dabei handelt es sich begrifflich aber nicht um Daten, sondern um Datenträger (s.o. Kap. 10.1). Eine zentrale Erwägung des Art. 20 DSGVO besteht darin, dass automatisiert verarbeitete Daten ohne nennenswerten Aufwand repliziert werden können und dadurch die Funktionalität der Verarbeitung durch den ursprünglichen Verantwortlichen nicht beeinträchtigt wird.[773] Diese Voraussetzung ist bei Biomaterialien (derzeit noch) nicht gegeben. Die Aufbewahrung von Biomaterialien erfolgt analog, nicht automatisiert, so wie dies Art. 20 Abs. 1 Nr. 2 DSGVO verlangt.

Unstreitig nicht mehr erfasst sind von dem Anspruch des Art. 20 DSGVO **Auswertungsergebnisse**, die der Verantwortliche mithilfe der bereitgestellten Daten gewonnen hat.[774] Laboruntersuchungsergebnisse, Arztbriefe oder Patientenakten, in welche die medizinische Dokumentation der Behandlung einfließt, sind also von der Datenportabilität des Art. 20 DSGVO nicht mehr erfasst. Dies gilt auch für die Analyseergebnisse aus Biomaterialproben, also z.B. für derart erlangte Gendaten. Werden dagegen Gendaten vom Betroffenen selbst auf eine Plattform eingestellt, so sind diese bereitgestellt.

Aufgrund einer **Einwilligung oder eines Vertrags** bereitgestellte Daten sind nur solche, bei denen sich die Einwilligung oder die Vertragsabsprache auf eine Speicherung des Verantwortlichen bezieht, d.h. der Betroffene den Verantwortlichen kennt.[775] Nicht mehr bereitgestellt sind insofern ursprünglich vom Betroffenen bereitgestellte Daten, die von Dritten an den Verantwortlichen weitergegeben wurden.

Die Regelung enthält keine thematische Beschränkung; vielmehr stellt sie darauf ab, dass der Betroffene die Daten auf Grundlage einer Einwilligung oder eines Vertrags einem Verantwortlichen bereitgestellt hat. Die Regelung ist auf den **medizinischen wie für den Forschungsbereich** grundsätzlich anzuwenden.[776]

770 Dix in SHS, Art. 20 Rn. 8; Rudolph in SJTK, Art. 20 Rn. 51f.

771 Art.-29-Arbeitsgruppe, WP 2422, Rev. 01, 11; Schantz in Schantz/Wolff, Rn. 1239; einschränkend Strubel ZD 2017, 357, der das Merkmal des Bereitstellens „servicespezifisch" auslegt; vgl. Kamann/Braun in Ehmann/Selmayr, Art. 20 Rn. 13; sowie Kamlah in Plath, DSGVO BDSG, 3. Aufl. 2018, Art. 20 Rn. 7, der als zusätzliche Voraussetzung für die Anwendung des Art. 20 eine „Schutzbedürftigkeit" des Betroffenen nennt; dagegen Rudolph in SJTK, Art. 20 Rn. 44; Westphal/Wichtermann ZD 2019, 192.

772 Weichert 2018, Kap. 4.5.

773 Sydow in Sydow, Art. 20 Rn. 11.

774 Dix in SHS, Art. 20 Rn. 8; Kamann/Braun in Ehmann/Selmayr, Art. 20 Rn. 13; Art.-29-Arbeitsgruppe, WP 2422, Rev. 01, 12; Rudolph in SJTK, Art. 20 Rn. 53.

775 Dix in SHS, Art. 20 Rn. 9.

776 Piltz in Gola, Art. 20 Rn. 6.

Ausgenommen ist der Anspruch auf Datenübertragung bei einer Verarbeitung, die in Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung einer dem Verantwortlichen übertragenen **öffentlicher Gewalt** erforderlich ist (Art. 20 Abs. 3 S. 2 DSGVO). Öffentliche Gewalt ist die Erhebung von Medizindaten durch die Gesundheitsbehörden etwa im Rahmen der Gesundheitsberichterstattung.[777] Öffentliche oder hoheitliche Gewalt wird nicht durch öffentlich-rechtliche Gesundheitsanbieter im Behandlungskontext ausgeübt, etwa durch kommunale, landes- oder bundeseigene Krankenhäuser oder von der öffentlichen Hand getragene Arztpraxen.[778] Auch soweit diese Forschung betreiben, erfolgt keine Ausübung hoheitlicher Gewalt, selbst wenn die Datenverarbeitung nicht auf der Grundlage eines Vertrages oder einer Einwilligung, sondern auf gesetzlicher Basis erfolgt.

Die Anwendung des Art. 20 DSGVO ist auch ausgeschlossen, wenn eine Verarbeitung in Wahrnehmung einer Aufgabe im **öffentlichen Interesse** liegt. Die Formulierung knüpft, ebenso wie der Verweis auf die „öffentliche Gewalt", an Art. 6 Abs. 1 lit. e DSGVO an. Gemäß der hier vertretenen Ansicht bedarf es für die Privilegierung von Forschungsvorhaben nach der DSGVO in jedem Fall eines öffentlichen Interesses (s.o. Kap. 3.3, Kap. 3.4, Kap. 8.1). Vom Wortlaut erfasst sind aber nur Stellen, die eine entsprechende Aufgabe wahrnehmen. Davon erfasst sind Aufgaben der Daseinsvorsorge, wozu auch die Gesundheitsvorsorge (Sicherstellung und Überwachung der Gesundheit, Gesundheitsüberwachung, Gewährleistung der öffentlichen Gesundheit, Verwaltung von Leistungen der Gesundheitsversorgung, Sicherstellung von Qualität und Wirtschaftlichkeit) gehört. Ausdrücklich nennt der Erwägungsgrund dann auch die Verarbeitung zu wissenschaftlichen Forschungszwecken (ErwGr 52, S. 1, 2). Dies spricht dafür, dass die Datenportabilität für die privilegierte Forschung selbst nicht gelten soll.[779]

Erfolgt eine Datenverarbeitung für Forschungszwecke auf der Grundlage von **Einwilligungen**, so liegen die Voraussetzungen des Art. 20 Abs. 1 DSGVO für die Datenübertragbarkeit insofern vor, unabhängig davon, ob die Verarbeitung durch öffentliche oder private Verantwortliche erfolgt. Gemäß Art. 20 Abs. 3 S. 2 DSGVO soll der Anspruch auf Übertragbarkeit nicht bestehen, wenn die Verarbeitung *„für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt."* Hieraus ist zu schließen, dass der Anspruch auf Übertragbarkeit ausgeschlossen ist, auch wenn die Datenpreisgabe freiwillig oder aufgrund eines Vertrags erfolgt.[780] Dies gilt für den gesamten privilegierten Forschungsbereich (s.o.).[781] Demgegenüber wird die Ansicht vertreten, dass der Ausschluss nur den hoheitlichen Bereich betrifft, wozu wohl die Forschung nicht zu zählen ist.[782] Art. 89 Abs. 3 DSGVO ermöglicht für Datenübertragungen nationale Regelungen, aber nur in Bezug auf öffentliche Archivzwecke, wovon in § 28 Abs. 4 BDSG Gebrauch gemacht wurde. Daher erfolgt in der entsprechenden Regelung für die Forschung in § 27 Abs. 2 BDSG kein Verweis auf Art. 20 DSGVO. Steht eine öffentliche Stelle im Wettbewerb, so ist auf

777 Weichert 2018, Kap. 3.10.

778 So wohl auch Roßnagel in SHS, Art. 6 Rn. 80.

779 Ähnlich Roßnagel ZD 2019, 163, wonach Art. 20 DSGVO für öffentliche Stellen wie staatliche Hochschulen ausgeschlossen ist.

780 Dix in SHS, Art. 20 Rn. 17; kritisch zu dem Ausschlussgrund Sydow in Sydow, Art. 20 Rn. 16f.

781 Schürmann in Auernhammer, Art. 20 Rn. 53.

782 BMH, Art. 20 Rn. 43.

diese der Grundsatz der Datenübertragbarkeit anwendbar.[783] Es ist derzeit davon auszugehen, dass Art. 20 DSGVO auf den Verbraucherwettbewerb zielt[784], nicht auf den Wettbewerb unter Forschungseinrichtungen.

Nicht als Ausnahme erwähnt werden die **medizinischen Leistungserbringer**, egal ob die Leistungen in öffentlich-rechtlicher oder in privater Form erbracht werden. Insofern kommt eine Anwendung des Art. 20 DSGVO in Frage. Bei der Auslegung des Art. 20 DSGVO sind die Hintergründe und Motivationen des Gesetzgebers mit zu berücksichtigen. Dem ging es um eine Begrenzung der Marktmacht privater Unternehmen zugunsten der Betroffenen. Mit der Wechselmöglichkeit zu einem anderen Marktanbieter soll die Abhängigkeit der Kunden reduziert werden.[785] Diese Erwägung lässt sich nicht auf den Forschungsbereich übertragen und nur begrenzt auf medizinische Leistungserbringer, in etwas stärkerem Maße aber wohl auf informationstechnische Dienstleister im Medizinbereich.[786]

Voraussetzung des Anspruchs des Art. 20 DSGVO ist, dass die Daten *„in einem **strukturierten, gängigen und maschinenlesbaren Format**“ weiterzugeben sind. Diese „Interoperabilität“ wird definiert „als die Fähigkeit verschiedener und unterschiedlicher Organisationen zur Interaktion zum beiderseitigen Nutzen und im Interesse gemeinsamer Ziele; dies schließt den Austausch von Informationen und Waren zwischen beteiligten Organisationen durch von ihnen unterstützte Geschäftsprozesse mittels Datenaustausch zwischen ihren jeweiligen IKT-Systemen ein.“*[787]

In ErwGr 68 S. 3 heißt es:

> *„Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen.“*

Die europäischen Datenschutzbehörden haben zur Zusammenarbeit der Hersteller und Wirtschaftsverbände bei der Entwicklung interoperabler Standards und Formate aufgefordert.[788] Solange derartige Standards nicht verpflichtend sind, droht die Regelung des Art. 20 DSGVO nicht umgesetzt zu werden.[789] Die Datenethikkommission empfiehlt demgemäß die Erarbeitung von spezifischen Verhaltensregeln und Standards und eine regelmäßige Evaluierung zur Datenportabilität.[790]

Art. 89 Abs. 2 DSGVO erlaubt, anders als für Archivzwecke (Art. 89 Abs. 3 DSGVO), keine **Einschränkung des Anspruchs** auf Portabilität durch eine nationale Regelung, wenn dies zur Erfüllung von Forschungszwecken notwendig ist. Dies dürfte darauf

783 Piltz in Gola, Art. 20 Rn. 4.
784 Albrecht CR 2016, 93; Kamann/Braun in Ehmann/Selmayr, Art. 20 Rn. 3; Schürmann in Auernhammer, Art. 20 Rn. 2; BMH, Art. 20 Rn. 2.
785 Dix in SHS, Art. 20 Rn. 1.; Herbst in Kühling/Buchner, Art. 20 Rn. 1; Piltz in Gola, Art. 20 Rn. 3; Kamann/Braun in Ehmann/Selmayr, Art. 20 Rn. 3; Schürmann in Auernhammer, Art. 20 Rn. 5, 7; Rudolph in SJTK, Art. 20 Rn. 26; Paal in Paal/Pauly, Art. 20 Rn. 6.
786 Zu Konzentrationsbestrebungen in diesem Bereich s. Weichert 2018, Kap. 3.1–3.4
787 Art. 2 Beschluss Nr. 922/2009/EG v. 16.09.2009 über Interoperabilitätslösungen für öffentliche Verwaltungen (ISA), ABl. I. 260 v. 03.10.2009, 20; Schürmann in Auernhammer, Art. 20 Rn. 35.
788 Dix in SHS, Art. 20 Rn. 11; Art.-29-Arbeitsgruppe, WP 242 rev. 01, 21; generell zur digitalen Standardisierung Datenethikkommission, 76.
789 Rudolph in SJTK, Art. 20 Rn. 77; skeptisch auch Herbst in Kühling/Buchner, Art. 20 Rn. 21.
790 Datenethikkommission, 21 (These 22).

zurückzuführen sein, dass derzeit nicht absehbar ist, wie durch die Portabilitätsregelung Forschungszwecke beeinträchtigt werden könnten.[791]

Die Grunderwägungen des Art. 20 DSGVO können auch für die medizinische Forschung relevant sein, da dieselben Daten für verschiedene Projekte Bedeutung haben können. In der aktuellen Diskussion über die Verbesserung der Datengrundlage für die medizinische Forschung spielt die sog. **Datenspende**[792] von betroffenen Probanden bzw. Patienten eine gewisse Rolle.[793] Entsprechend den Vorgaben des Art. 20 DSGVO könnten diese ihre Daten unter Ausübung ihrer informationellen Selbstbestimmung den Forschungsprojekten ihrer Wahl zur Verfügung stellen.

Insbesondere eine **gemeinwohlorientierte Bereitstellung** auch von personenbeziehbaren Daten wird – über die in Art. 20 DSGVO enthaltene Regelung hinausgehend – erörtert.[794] Dabei könnte der Bereitstellung von Daten für Forschungszwecke eine wichtige Funktion zukommen.

12.7 Widerspruchsrecht

Art. 21 DSGVO begründet für die Betroffenen ein Widerspruchsrecht:

> *„(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. […]*
>
> *(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.“*

Mit dem Widerspruchsrecht soll es dem Betroffenen ermöglicht werden, die Verarbeitung seiner Daten einer **Prüfung auf ihre Notwendigkeit und Rechtmäßigkeit** zu unterziehen.[795] Auf diese Weise kann er negative Wirkungen der Datenverarbeitung für sich zu vermeiden suchen. Im Forschungsbereich soll die Widerspruchsmöglichkeit einen gewissen Ausgleich dafür schaffen, dass dem Betroffenen in diesem Bereich verschiedene Duldungspflichten auferlegt sind.[796]

791 Dix in SHS, Art. 20 Rn. 19.
792 Deutscher Ethikrat, 176 (A4.2), 188f. (Fischer); Dierks 2019, 55ff.; Zenker/Krawczak/Semler in TMF, 45ff.; zur ethischen Bewertung ausführlich Strech in TMF, 49ff.
793 Zu Recht kritisch Datenethikkommission, 124; Dierks 2019, 57.
794 Datenethikkommission, 137, ausführlich zum Datenzugang, 141ff.
795 Herbst in Kühling/Buchner, Art. 21 Rn. 1.
796 Herbst in Kühling/Buchner, Art. 21 Rn. 46.

Der Widerspruch des Betroffenen muss die **Einstellung der Verarbeitung** von dessen personenbezogenen Daten zur Folge haben, wenn sich im Rahmen der Prüfung erweist, dass die Datenverarbeitung unzulässig ist. Je nach Widerspruch kann die Einstellung der Verarbeitung darin bestehen, dass die Daten gelöscht werden (Art. 17 DSGVO). Möglicherweise liegt aber das Interesse des Betroffenen in einer Einschränkung der Verarbeitung (Art. 18 DSGVO).[797] Erweist sich eine Datenverarbeitung im Rahmen der Prüfung als grundsätzlich zulässig, ist aber der Anwendungsbereich des Art. 21 Abs. 6 DSGVO eröffnet, so ist die Verarbeitung auch einzustellen (s.u.).

Auf die **Rechtsgrundlage** der ursprünglichen Datenverarbeitung kommt es für die Begründetheit des Widerspruchs bei einer unzulässigen Datenverarbeitung nicht an. Wird gegen eine Datenverarbeitung Widerspruch eingelegt, die auf einer Einwilligung (Art. 4 Nr. 11 DSGVO) beruht, so ist hierin ein Widerruf der Einwilligung zu sehen (Art. 7 Abs. 3 DSGVO). Erfolgt die Datenverarbeitung von sensitiven Daten auf der Grundlage einer Aufgabenerfüllung *„im öffentlichen Interesse"* (vgl. Art. 6 Abs. 1 lit. e DSGVO) oder nach einer positiven Güterabwägung (vgl. Art. 6 Abs. 1 lit. f DSGVO), so hängt das Ergebnis des Widerspruchs von einer Güterabwägung ab: Wird ein Widerspruch erklärt, so soll dieser die **Gründe für die besondere Situation** des Schutzbedarfs des Betroffenen möglichst nachvollziehbar enthalten, sodass von dem Verantwortlichen eine Prüfung und eine Interessenabwägung vorgenommen werden kann.[798]

Forschungsdatenverarbeitung ist nicht auf einen operativen Einsatz in Bezug auf den Betroffenen aus, sondern auf das Erlangen von generalisierbaren Erkenntnissen. Damit geht ein **verringertes Betroffeneninteresse** einher, das im Rahmen einer Erforderlichkeitsprüfung verdrängt werden kann. Eine Erforderlichkeit kann z.B. dadurch begründet sein, dass durch den Widerspruch die Repräsentativität einer Untersuchung beeinträchtigt ist.[799] Lässt sich das öffentliche Interesse jedoch durch Datenminimierung oder durch technisch-organisatorische Maßnahmen wahren, so müssen diese Maßnahmen ergriffen werden. Eine solche Maßnahme kann z.B. in der Pseudonymisierung liegen.[800] Keine Erforderlichkeit ist gegeben, wenn die Daten anonymisiert verarbeitet werden können.[801]

Art. 21 Abs. 6 DSGVO mit seiner Sonderregelung für die Verarbeitung für Forschungszwecke gewährt generell ein Recht auf Widerspruch, wenn nicht die Verarbeitung zur Erfüllung einer Aufgabe **im „öffentlichen Interesse"** erforderlich ist. Private, möglicherweise überwiegende Interessen des Verantwortlichen können bei einer Forschungsverarbeitung eine Behandlung des Widerspruchs nicht ausschließen.[802] Erweist sich ein Widerspruch als unbegründet oder ist die weitere Verarbeitung der Daten im öffentlichen Forschungsinteresse erforderlich, so ist der Verantwortliche an der Weiterverarbeitung nicht gehindert.[803] Ein öffentliches Interesse besteht nicht nur bei der Forschung an staatlichen Hochschulen und in Forschungseinrichtun-

797 Atzert in SJTK, Art. 21 Rn. 57
798 Helfrich in Sydow, Art. 21 Rn. 91f.; Martini in Paal/Pauly Art. 21 Rn. 26; Herbst in Kühling/Buchner, Art. 21 Rn. 54.
799 Atzert in SJTK, Art. 21 Rn. 111.
800 Caspar in SHS, Art. 21 Rn. 40.
801 Herbst in Kühling/Buchner, Art. 21 Rn. 54; Martini in Paal/Pauly, Art. 21 Rn. 60; Atzert in SJTK, Art. 21 Rn. 108.
802 Kamann/Braun in Ehmann/Selmayr, Art. 21 Rn. 65.
803 Herbst in Kühling/Buchner, Art. 21 Rn. 54f.

gen.[804] Selbst wenn man den Anwendungsbereich des Art. 21 Abs. 6 DSGVO auf öffentliche Stellen begrenzt sieht, kann auf der Grundlage Art. 89 Abs. 2 DSGVO ein Widerspruchsrecht bestehen (s.u.).[805] Weder Art. 21 Abs. 6 DSGVO noch die Sonderregelung des auf Art. 89 Abs. 2 DSGVO zurückzuführenden § 27 Abs. 2 BDSG differenzieren zwischen sensitiven und sonstigen Daten; sie sind also auf die Verarbeitung von Gesundheitsdaten anwendbar.

Art. 21 Abs. 6 DSGVO verpflichtet den Verantwortlichen zur **Glaubhaftmachung des öffentlichen Interesses** an der konkreten Verarbeitung.[806] Dieses unterscheidet sich von dem öffentlichen Interesse, das an dem Forschungsprojekt insgesamt bestehen muss.[807]

Art. 21 DSGVO wird zudem im Katalog des Art. 89 Abs. 2 DSGVO aufgeführt, der **nationale und europarechtliche Ausnahmen** erlaubt. § 27 Abs. 2 BDSG sieht eine solche Ausnahme vor. Dabei handelt es sich letztlich um eine Konkretisierung des Art. 6 Abs. 1 lit. f DSGVO, der eine Interessenabwägung vorsieht. Dies führt dazu, dass das Widerspruchsrecht grundsätzlich eröffnet ist.[808] § 27 Abs. 2 S. 1 BDSG erlaubt die Beschränkung des Widerspruchsrechts, soweit dies für privilegierte Forschungszwecke erforderlich ist, weil der Ausschluss der Daten die Verwirklichung der Forschungszwecke *„unmöglich machen oder ernsthaft beeinträchtigen"* würde.

Der Ausschluss des Widerspruchsrechts hindert im Ergebnis nicht am Widerspruch; wohl aber dispensiert er den Verantwortlichen von der Notwendigkeit der **Darlegung der zwingenden Gründe** für die konkrete Weiternutzung der Daten.[809] Zudem ist der Verantwortliche von seinen Hinweispflichten gegenüber dem Betroffenen in Bezug auf dessen Widerspruchsrecht (Art. 21 Abs. 4 DSGVO) befreit.[810]

Der Ausschluss des **Widerspruchsrechts** folgt einer gewissen Logik, da schon die vorgenannten Betroffenenrechte eingeschränkt werden können. Ohne Auskunftsanspruch ist regelmäßig eine Kenntnis der Daten ausgeschlossen, gegen deren Verarbeitung widersprochen werden könnte. Ist die Wahrnehmung eines sonstigen Betroffenenrechts aus Forschungsgründen unzulässig, so ist auch ein Widerspruch gegen die Datenverarbeitung wirkungslos. Die Betroffenen sollen sich nicht ermuntert sehen, gegen eine Verarbeitung Widerspruch einzulegen, gegen die sie aus berechtigten Gründen ohnehin nicht vorgehen können.[811]

Das Widerspruchsrecht ist nur ausgeschlossen, soweit dies für Forschungszwecke erforderlich ist. Ein Grund hierfür kann die Verarbeitung von großen Datenmengen sein (s.o. z.B. Kap. 12.3).[812] **Nicht erforderlich**, ja für die Forschung möglicherweise förderlich ist die Ausübung des Widerspruchsrechts, wenn der Betroffene dabei berechtigterweise die Unrichtigkeit seiner Daten geltend macht. Ein solcher „Widerspruch" ist dann als Berichtigungsanspruch zu behandeln (Art. 16 DSGVO). Eine

804 So Roßnagel, Rewiew des vorliegenden Gutachtens, 02.02.2020, 11.
805 Caspar in SHS Art. 21 Rn. 36; Kamann/Braun in Ehmann/Selmayr, Art. 21 Rn. 62.
806 Martini in Paal/Pauly, Art. 21 Rn. 60; Helfrich in Sydow, Art. 21 Rn. 98.
807 Caspar in SHS, Art. 21 Rn. 39
808 A.A. wohl Werkmeister/Schwaab CR 2019, 89f. Rn. 36f.
809 Caspar in SHS, Art. 21 Rn. 37–40, der auf die Relativität selbst dieser Privilegierung hinweist.
810 Dazu Helfrich in Sydow, Art. 21 Rn. 107f.
811 Weichert in DWWS, § 27 Rn. 27.
812 Martini in Paal/Pauly, Art. 21 Rn. 54.

Überprüfung der Daten kann so möglicherweise eine relevante Verbesserung der Datengrundlage bewirken. Daher sollte mit der Beschränkung bzw. dem völligen Ausschluss des Widerspruchsrechts bei Forschungsprojekten zurückhaltend umgegangen werden.

12.8 Recht auf Löschung

Art. 17 DSGVO regelt das „Recht auf Löschung" sowie spezifische Ausnahmeregelungen:

> *„(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:*
>
> *a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.*
>
> *b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.*
>
> *c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.*
>
> *d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.*
>
> *e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.*
>
> *f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben. […]*
>
> *(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist*
>
> *a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;*
>
> *b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;*
>
> *c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;*
>
> *d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt […]."*

Das in Art. 17 normierte Recht auf Löschung wird auch als **„Recht auf Vergessenwerden"** bezeichnet. Es dient der Umsetzung des Grundsatzes der „Datenminimierung" nach Art. 5 Abs. 1 lit. c DSGVO und des Grundsatzes der „Speicherbegrenzung" nach Art. 5 Abs. 1 lit. e DSGVO.[813]

Für den **Grundsatz der Speicherbegrenzung** gilt als Ausnahme, dass Daten länger gespeichert werden dürfen, soweit sie, *„vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden."*

Im alten Recht war die Verarbeitung **öffentlich zugänglicher Daten** grundsätzlich privilegiert (§ 28 Abs. 1 Nr. 3 BDSGaF). In der DSGVO besteht mit Art. 9 Abs. 2 lit. e lediglich eine Regelung für (sensitive) Daten, die *„die betroffene Person offensichtlich öffentlich gemacht hat"*.[814] Ist diese Regelung nicht anwendbar, so ist die Zulässigkeit einer Weiterverarbeitung vom Vorliegen einer Einwilligung oder einer gesetzlichen Regelung, z.B. einer Forschungsklausel, abhängig. Bei einer in Forschungsklauseln vorgesehenen Abwägung kann der Umstand, dass Daten veröffentlicht worden sind, eine Rolle spielen, wenn in dieser Veröffentlichung ein öffentliches Interesse an der Information zum Ausdruck kommt. Das öffentliche Interesse kann auch darin liegen, dass im Rahmen eines Forschungsprojektes der Umstand der Veröffentlichung zum Gegenstand der wissenschaftlichen Untersuchung gemacht wird.[815]

Art. 9 Abs. 2 lit. e DSGVO erlaubt die Verarbeitung sensitiver Daten, wenn der Betroffene diese **„offensichtlich öffentlich gemacht hat"**. Öffentlich gemacht sind Daten, die einem unbestimmten Personenkreis zugänglich gemacht werden.[816] Dies ist der Fall, wenn ein Betroffener auf seiner eigenen Homepage ohne weitere Zugangsbeschränkung über seine Gesundheitsgeschichte berichtet. Dies ist nicht der Fall, wenn ein Betroffener Daten über sich in einer geschlossenen Selbsthilfegruppe austauscht. Dies ist auch nicht der Fall, wenn der Betroffene die Daten einem Forschenden bereitgestellt hat und der Forschende diese Daten dann veröffentlicht hat.[817] Nicht offensichtlich öffentlich gemachte Daten sind auch Ableitungen eines Forschers aus öffentlich gemachten Daten, also wenn z.B. aus einem Facebook-Profil Rückschlüsse auf den Gesundheitszustand einer Person gezogen werden. Voraussetzung ist, dass sich der Betroffene vollständig dessen bewusst ist, dass seine Daten mit allgemein verfügbaren Mitteln jedermann, und damit möglicherweise auch forschenden Dritten, zugänglich sind.[818] Die Datenschutzbehörden fordern insofern eine enge Auslegung.[819]

Der EuGH hat aus den Art. 7 u. Art. 8 GRCh zum „Anspruch auf Vergessenwerden" bzw. zu einem „Anspruch auf Vergessen" bei im Internet veröffentlichten Daten nähere Ausführungen gemacht.[820] Danach muss nicht in jedem Fall eine vollständige

813 Däubler in DWWS, Art. 17 Rn. 1.
814 BKL-R, 230f.
815 Weitergehend Golla/von Schönfeld K&R 2019, 19: i.d.R. Vorrang öffentlich-rechtlich organisierter Forschung.
816 Petri in SHS, Art. 9 Rn. 58.
817 Weichert in Kühling/Buchner Art. 99 Rn. 77–82.
818 Petri in SHS, Art. 9 Rn. 57.
819 EDPS 2020, 19.
820 Erstmals EuGH 13.05.2014 – C-131/12 (Google Spain), NJW 2014, 2257 = NVwZ 2014, 857 = MMR 2014, 559.

und endgültige Löschung erfolgen. Soweit Daten auf einer gesetzlichen Grundlage für einen spezifischen Zweck gespeichert sind und die Verarbeitung für diesen Zweck weiterhin zulässig ist und besteht, kann auch eine weitere Speicherung erfolgen; dennoch kann ein Anspruch auf **Einschränkung der Erreichbarkeit** der Daten gegeben sein.

Widerspricht ein Betroffener einer Veröffentlichung seiner Daten über eine Internet-Suchmaschine und besteht an dieser **Form der Erreichbarkeit** kein überwiegendes berechtigtes Interesse, so ist eine Suchmaschine verpflichtet, die Links auf die ursprüngliche Datenspeicherung zu löschen.[821] Bei der Frage nach der Reichweite dieses Löschanspruchs ist ein Ausgleich zwischen den Grundrechten des Betroffenen und den Interessen des Verantwortlichen bzw. der Öffentlichkeit an der Datenverarbeitung vorzunehmen. Hierbei kommt es auf die Art der betreffenden Informationen, die Sensibilität für den Betroffenen und das Interesse der Öffentlichkeit am Zugang an.[822] Bei einer zutreffenden Information, die berechtigterweise gespeichert wurde, kann ein Betroffener wegen eines längeren Zeitablaufs einen Anspruch auf Vergessenwerden geltend machen. Dies gilt selbst dann, wenn durch die Erreichbarkeit der Daten kein Schaden für den Betroffenen entsteht. Dieser Anspruch ist aber nicht begründet, wenn die Erreichbarkeit durch ein überwiegendes öffentliches Interesse legitimiert wird.[823] Es muss eine Abwägung zwischen dem Interesse des Betroffenen am Schutz seines Persönlichkeitsrechts und dem Interesse der Öffentlichkeit an der Zugänglichkeit der Information vorgenommen werden.[824] Ein Anspruch auf erschwerte Zugänglichkeit von Daten kann dabei sogar gegenüber einem Verantwortlichen weltweit geltend gemacht werden.[825]

Die vom EuGH entschiedenen Urteile sowie die vom BVerfG zum „Recht auf Vergessen" ergangenen weiter konkretisierenden Beschlüsse bezogen sich auf Veröffentlichungen im Internet. Aus ihnen kann nicht geschlossen werden, dass personenbezogene Daten generell einer Verfallsfrist unterliegen. Die Frage der Löschung von Daten muss jeweils im Rahmen einer Abwägung beantwortet werden. Dabei ist auf Betroffenenseite das Interesse einzustellen, dass sich Dritte nicht individueller Daten bemächtigen und sie in nicht nachvollziehbarer Weise als Instrument nutzen, um die Betroffenen auf Eigenschaften, Typen oder Profile festzulegen, auf die sie keinen Einfluss haben und die für die freie Entfaltung der Persönlichkeit und eine Teilhabe in der Gesellschaft von Bedeutung ist.[826] Dem kann ein öffentliches Verarbeitungsinteresse entgegenstehen. Dies kann darin bestehen, als Quelle vollständig und wahrhaftig für journalistische und zeithistorische Recherchen zur Verfügung zu stehen.[827] Entsprechendes muss für ein öffentliches Interesse an Forschung und speziell an medizinischer Forschung gelten. Die Abwägung kann zu einer Erschwerung

821 EuGH 13.05.2014 – C-131/12 (Google Spain), Rn. 74–76.
822 EuGH 13.05.2014 – C-131/12 (Google Spain), Rn. 81.
823 EuGH 13.05.2014 – C-131/12 (Google Spain), Rn. 89–99.
824 BVerfG 06.11.2019 – 1 BvR 16/13 (Recht auf Vergessen I), Rn. 101–113, DuD 2020, 203f. = WRP2020, 52f.; BVerfG 06.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II), Rn. 120, DuD 2020, 209 = WRP 2020, 71.
825 EuGH 24.09.2019 – C-507/17 (Recht auf Vergessenwerden), Rn. 64, NJW 2019, 3501 = ZD 2020, 33; vgl. EuGH 24.09.2019 – C-136/17 (Auslistung Google), ZD 2020,36; EuGH 03.10.2019 – C-18/18 (Glawischnik-Piesecek), NJW 2019, 3287; Spindler NJW 2019, 3274.
826 BVerfG 06.11.2019 – 1 BvR 16/13 (Recht auf Vergessen I), Rn. 90.
827 BVerfG 06.11.2019 – 1 BvR 16/13 (Recht auf Vergessen I), Rn. 113.

der Erreichbarkeit von Daten führen, ohne dass damit eine Löschverpflichtung in weniger leicht erreichbaren Archiven verbunden sein muss.[828] Eine zweckgebundene **Speicherung im öffentlichen Forschungsinteresse** rechtfertigt grundsätzlich eine weitere Verarbeitung.

Die Erreichbarkeit einer **wissenschaftlichen Veröffentlichung im Internet** kann eingeschränkt sein, etwa über eine (populäre) Suchmaschine, wenn daran kein öffentliches Interesse (mehr) besteht.[829]

Die **Ausnahmen zum Löschungsanspruch** bei einer Forschungsdatenverarbeitung ergeben sich direkt aus Art. 17 Abs. 3 DSGVO. § 27 BDSG enthält insofern keine Aussage.

Der Löschanspruch besteht – ebenso wie das Recht auf Berichtigung – unabhängig davon, ob ein **Betroffener seinen Anspruch geltend macht**.[830] Liegen die rechtlichen Voraussetzungen vor, so hat eine Löschung zu erfolgen, auch wenn der Betroffene von der Verarbeitung keine Kenntnis hat und keine Löschung gefordert hat.

Löschen oder die „Vernichtung" von Daten wird in Art. 4 Nr. 2 DSGVO als eine Form der Datenverarbeitung beschrieben. Dies setzt voraus, dass die Daten unkenntlich gemacht werden. Das **Unkenntlichmachen** kann in Form der Zerstörung des Datenträgers erfolgen oder durch ein Überschreiben bzw. Beseitigen auf dem Datenträger. Der zuvor gespeicherte Text oder sonstige Inhalt darf nicht mehr lesbar sein. Allein das Kenntlichmachen, dass die Daten nicht mehr gelten sollen, genügt nicht. Wird nur die Erschließung eines Datums durch Löschen der Referenz erschwert, erfolgt keine Löschung. Löschen ist der tatsächliche Vorgang des Unkenntlichmachens; dessen Anordnung oder Freigabe genügt nicht.[831] Angesichts der technischen Möglichkeiten der Rekonstruktion nach Löschungsversuchen[832] ist die Auslegung des Begriffs vom aktuellen Stand der Technik abhängig. Dieser wird durch Standards festgelegt, etwa durch die seit 2012 gültige DIN 66399 „Büro- und Datentechnik, Vernichtung von Datenträgern".[833]

Eine **wirksame Anonymisierung** (s.o. Kap. 10.2) kommt einer Löschung weitgehend gleich.[834] Soweit personenbezogene Daten der Löschpflicht unterfallen, können diese auch anonymisiert werden.[835] Gegen eine völlige Gleichsetzung von Löschung und Anonymisierung kann vorgebracht werden, dass bei der Anonymisierung im Vergleich zur Löschung ein Restrisiko der Reidentifizierung verbleibt.[836] Doch auch bei einer Löschung muss es nicht zwangsläufig zu einer endgültigen Vernichtung der Daten kommen.[837]

828 Vgl. BVerfG 06.11.2019 – 1 BvR 16/13 (Recht auf Vergessen I), Rn. 128ff.
829 BVerfG 06.11.2019 – 1 BvR 16/13 (Recht auf Vergessen I), Rn. 128–130.
830 Heberlein in Ehmann/Selmayr, Art. 5 Rn. 27.
831 Gräff/Günsel, DuD 1990, 77; Jürgens, DuD 1998, 449; zu Entscheidungen des VG Wiesbaden zur Löschung bei SAP vgl. Schild, DANA 1/2013, 13.
832 Fox, DuD 2009, 110.
833 Technische Hochschule Mittelhessen (THM), Datenschutz-Tipp 4; dazu Köppen, DANA 1/2013, 12.
834 Dierks in Dierks/Roßnagel, 91f. m.w.N.; Roßnagel/Geminn in Dierks/Roßnagel, 192.
835 BfDI, Anonymisierung unter der DSGVO, Konsultationsverfahren 09.03.2020, 8f.
836 Roßnagel, Review des vorliegenden Gutachtens, 02.02.2020, 29.
837 BfDI, Anonymisierung unter der DSGVO, Konsultationsverfahren 09.03.2020, 9.

Art. 17 Abs. 2 DSGVO sieht vor, dass ein zur Löschung verpflichteter Verantwortlicher vertretbare Schritte unternehmen muss, um weitere Verantwortliche darüber zu informieren, dass ein Betroffener von ihnen die Löschung *„aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat"*. Dabei soll der Verantwortliche unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel angemessene Maßnahmen – auch technischer Art – treffen, um die Daten **weiterverarbeitenden Verantwortlichen** über den Antrag des Betroffenen zu informieren (ErwGr. 66 S. 2). Diese Regelung bezieht sich explizit ausschließlich auf die vom Betroffenen beantragte Löschung, nicht eine Anonymisierung.[838] Die von Art. 17 Abs. 2 DSGVO verfolgte Zielrichtung lässt sich aber auf eine Anonymisierung als „ein Weniger" zur Löschung übertragen.

Im Fall einer **Pseudonymisierung** von Datensätzen kommt es für die Wahrnehmung der Betroffenenrechte und damit auch des Rechts auf Löschung darauf an, ob der Datensatz, auf den sich ein Antrag bezieht, für den Verantwortlichen identifizierbar ist. Auf die obigen Ausführungen zur Auskunft und die Anwendung des Art. 11 DSGVO kann umfassend verwiesen werden (s.o. Kap. 12.3).

Bei Vorliegen einer wegen der **Nutzung für Forschungszwecke** privilegierten Ausnahme kann es überflüssig sein zu klären, ob ein rechtlicher Grund für eine Löschung nach Art. 17 Abs. 1 lit. a–f DSGVO besteht. Die Ausnahme vom Grundsatz der Speicherbegrenzung hat zur Folge, dass für den (Sekundär-)Zweck Forschung die Daten länger gespeichert werden dürfen, als dies für die Erreichung eines primären Zwecks erforderlich ist. Sie dürfen so lange gespeichert werden, wie dies für den Forschungszweck erforderlich ist. Die Gründe für die Privilegierung bei der Speicherbegrenzung sind dieselben wie für die Lockerung der Zweckbindung (s.o. Kap. 8.1).[839] Dies bedeutet jedoch nicht, dass eine Prüfung, ob und wie lange die Speicherung nötig ist, entfallen kann.[840] Personenbezogene Forschungsdaten sind zu löschen oder zu anonymisieren, sobald diese für die Forschungszwecke nicht mehr benötigt werden.[841]

Die Ausnahme von der Löschpflicht aus Gründen der **Meinungs- und Informationsfreiheit** (Art. 17 Abs. 3 lit. a DSGVO) gilt direkt und unabhängig von den Regelungsaufträgen in Art. 85 DSGVO.[842] Soweit mit der Wahrnehmung der Meinungs- und Informationsfreiheit zugleich der Schutzzweck der Forschungsfreiheit tangiert ist, können lit. a und lit. d sich gegenseitig ergänzen (vgl. Art. 85 Abs. 1 Abs. 1 DSGVO, s.o. Kap. 4.4). Bei Vorliegen von lit. a ist nicht in jedem Fall eine fortgesetzte Datenverarbeitung erlaubt; vielmehr bedarf es einer Abwägung mit dem Recht auf Datenschutz und dem daraus abgeleiteten Löschanspruch sowie mit anderen Grundrechten.[843]

Ob eine Ausnahme von der Löschpflicht aus Gründen der Wahrnehmung einer **Aufgabe, die im öffentlichen Interesse vorliegt** (Art. 17 Abs. 3 lit. b DSGVO), oder hierfür ein Zweck der Forschung oder des Gesundheitsschutzes (lit. c, d) angenommen wird, ist im Ergebnis nicht von Bedeutung. Gesetzlich geregelte, im öffentlichen

838 Roßnagel, Review des vorliegenden Gutachtens, 29.
839 Herbst in Kühling/Buchner, Art. 5 Rn. 71.
840 Roßnagel in SHS, Art. 5 Rn. 162; a.A. Herbst in Kühling/Buchner, Art. 5 Rn. 69.
841 Johannes in Roßnagel 2018, § 7 Rn. 249; Roßnagel in SHS, Art. 5 Rn. 162.
842 Dix in SHS, Art. 17 Rn. 31.
843 Dix in SHS, Art. 17 Rn. 31.

Interesse liegende Aufbewahrungszeiträume sind z.B. für klinische Prüfungen nach dem AMG vorgesehen (s.o. Kap. 7.4).[844]

Die Ausnahme von der Löschpflicht aus Gründen des öffentlichen Interesses im **Bereich der öffentlichen Gesundheit** (Art. 17 Abs. 3 lit. c DSGVO) nimmt Bezug auf Art. 9 Abs. 2 lit. h und lit. i. Darin wird auf spezifisches Recht der Union oder der Mitgliedstaaten verwiesen. Ein Fall des Art. 9 Abs. 2 lit. h DSGVO ist die ärztliche Dokumentationspflicht, wonach Patientenakten für eine bestimmte Zeit aufzubewahren sind (vgl. § 630f BGB, § 10 MBOÄ).[845] Bei Arzneimittelstudien nach dem AMG liegen die Voraussetzungen von Art. 9 Abs. 2 lit. h und lit. i vor.[846] Art. 17 Abs. 3 lit. c DSGVO (öffentliches Interesse im Bereich der Gesundheit) und lit. d DSGVO (Forschung) schließen sich aus, wenn, was die Regel ist, mit der Verfolgung von Forschungszwecken nicht zugleich operative Zwecke verfolgt werden (s.o. Kap. 8.1).[847] Zwar liegt bei wissenschaftlicher Forschung oft auch ein öffentliches Interesse im Bereich der öffentlichen Gesundheit vor. Primäre Zielrichtung von Forschung ist aber die Erkenntnisgewinnung. Daher wird die Forschung in Art. 17 Abs. 3 DSGVO ausdrücklich erwähnt. Zielt ein Forschungsprojekt direkt auf eine Verbesserung der Gesundheitsversorgung, so können beide Alternativen anwendbar sein.

Die Ausnahme von der Löschpflicht aus **Forschungsgründen** (Art. 17 Abs. 3 lit. d DSGVO) legitimiert die Speicherung im Rahmen der Erforderlichkeit für diese Zwecke. Dabei kommt es auf den jeweiligen konkreten Zweck bzw. die konkreten Zwecke an. Art. 17 Abs. 3 lit. d DSGVO ist nicht die Rechtsgrundlage für die weitergehende Datenverarbeitung; diese findet sich vielmehr in den Art. 6 und Art. 9 DSGVO sowie in den diese spezifizierenden Rechtsgrundlagen. Mit der Regelung wird vielmehr die Speicher- und Nutzungsdauer erweitert. Die bisher geltende Rechtsgrundlage bleibt jeweils bestehen.[848]

Auch für Forschungszwecke soll nach dem Ansatz der DSGVO grundsätzlich – nach einer gegenüber der ursprünglichen Speicherfrist möglicherweise **verlängerten Speicherdauer** – eine Datenlöschung erfolgen.[849] Unmittelbar nach Erreichung des Forschungsziels sind die Daten zu löschen.[850] Hätte eine Löschung einzelner Datenpunkte eine signifikante Verringerung der statistischen Validität zur Folge, so ist die Ausnahme anwendbar, bei einer geringfügigen und nicht relevanten Beeinträchtigung dagegen nicht.[851]

Eine Aufbewahrung wird nach Art. 17 Abs. 3 lit. d DSGVO auch für im öffentlichen Interesse liegende **Archivzwecke** erlaubt. Im öffentlichen Interesse wird ein Archiv geführt, wenn das Recht der Union oder der Mitgliedstaaten einer Stelle die Aufgabe übertragen hat, Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen. Dies be-

844 Bischoff/Wiencke ZD 2019, 12.
845 Dix in SHS, Art. 17 Rn. 33
846 Bischoff/Wiencke ZD 2019, 10.
847 A.A. wohl Bischoff/Wiencke ZD 2019, 10.
848 Dix in SHS, Art. 17 Rn. 34; vgl. Herbst in Kühling/Buchner, Art. 17 Rn. 82; Peuker in Sydow, Art. 17 Rn. 66.
849 EPDS, 23f.
850 Bischoff/Wiencke ZD 2019, 12.
851 Werkmeister/Schwaab CR 2019, 88, Rn. 20; Metschke/Wellbrock, 46.

trifft nicht nur das Bundesarchive und die Landesarchive, sondern auch andere Stellen, die mit Archivtätigkeit hoheitlich betraut sind. Archivzwecke sind nicht nur Zwecke für die historische Forschung.[852]

Auch die medizinische Forschung soll von dieser Privilegierung der DSGVO profitieren können. Eine zentrale Zielrichtung von Archiven liegt in der Förderung des wissenschaftlichen Lebens, ohne dass die Aufgaben sich herauf beschränken müssen.[853] Bei medizinischen **Forschungsregistern**[854] ist zu prüfen, ob und inwieweit mit ihnen öffentliche Archivzwecke verfolgt werden. So dienen Krebsregister, das Implantateregister[855] oder das Forschungsdatenzentrum im Bereich der gesetzlichen Krankenversicherung[856] Forschungszwecken. Für diese Register sind teilweise keine Löschungsregelungen vorgesehen.[857] Soweit diese fehlen, können, soweit archivarische Zwecke verfolgt werden, langjährige Aufbewahrungsfristen gerechtfertigt sein.

Eine zentrale Rechtfertigung für eine langfristige Speicherung von Forschungsdaten kann es sein, dass auch nach Abschluss eines Forschungsvorhabens im wissenschaftlichen Diskurs die Ergebnisse auf Basis der Ausgangsdaten nachvollzogen werden können müssen. Zumeist bedarf es hierfür aber keiner identifizierenden Datensätze, weshalb dann die Speicherung pseudonymisiert erfolgen muss. Entsprechendes gilt für die Notwendigkeit der Überprüfung von klinischen Prüfungen nach dem Arzneimittelgesetz (vgl. § 42 Abs. 3 Nr. 6 AMG). Besteht eine spezielle Regelung für eine Aufbewahrung zwecks **Überprüfung von Forschungsergebnissen**, so dürfen die Daten nur noch für diesen Zweck verwendet werden.

Eine Ausnahme von der Löschpflicht wegen privilegierter Forschung setzt in jedem Fall voraus, dass hinreichende geeignete **technisch-organisatorische Schutzmaßnahmen** ergriffen werden (Art. 89 Abs. 1 DSGVO, s.o. Kap. 9, Kap. 10). Diese müssen einen im Wesentlichen gleichwertigen Schutz wie die Löschung bzw. Anonymisierung bieten und insbesondere die Datenverwendung für Maßnahmen oder Entscheidungen zulasten des Betroffenen ausschließen.[858] Auf die Pseudonymisierung ist als Standardschutzmaßnahme nur in seltenen Fällen zu verzichten, da der Forschungszweck zumeist auch mit pseudonymen Daten erreicht werden kann (vgl. z.B. § 40 Abs. 2a Nr. 1 lit. b–d AMG).[859] Entsprechendes gilt für die verschlüsselte Datenspeicherung. Je länger die Daten aufbewahrt werden, je breiter die Forschungszwecke definiert sind und je mehr Stellen Zugriff auf die Daten nehmen können, also je höher das Verarbeitungsrisiko ist, desto höhere Anforderungen sind an die langfristige

852 Johannes in Roßnagel 2018, § 7 Rn. 197; Johannes/Richter DuD 2017, 300.
853 Partsch, in Partsch, Bundesarchivgesetz, 2019, Einleitung Rn. 1.
854 Metschke/Wellbrock, 52f.
855 §§ 1 Abs. 2 Nr. 6, 4 Abs. 1 Nr. 5, 29 Abs. 1 Nr. 2 Implantateregister-Errichtungsgesetz v. 12.12.2019 (EIRD), BGBl. I S. 2494; dazu BfDI, TB 2020, Kap. 7.3 (S. 68).
856 §§ 303d Abs. 1 Nr. 10, 303e SGB V gemäß Digitale-Versorgung-Gesetz v. 09.12.2019, BGBl. I S. 2562; Weichert DANA 202, 20; ders. MedR 2020, 539ff.; Schulz SGb 2020, 536ff.; Bretthauer/Spiecker JZ 2020, 990ff.; Schrahe/Städter DuD 2020, 713ff.; Dierks 2020, 11ff.
857 § 32 EIRD sieht vor, dass die Registerstelle die pseudonymisierten Daten zu anonymisieren hat, wenn den Zwecken des Registers so entsprochen werden kann.
858 Johannes in Roßnagel 2018, § 7 Rn. 249; Roßnagel in SHS, Art. 5 Rn. 163; so schon Dammann/Simitis, Art. 6 Rn. 18.; Bizer, 234f.
859 Dix in SHS, Art. 17 Rn. 35.

Sicherung der Daten vor unberechtigter Verarbeitung zu stellen (Art. 25, 32, 35 DSGVO, vgl. ErwGr 74–78, 83, 91).[860]

Zulässig bleibt die **Nutzung für reine Forschungszwecke**, etwa für die statistische Analyse, um Forschungsergebnisse zu verifizieren. Auch eine Anfrage bei Betroffenen, ob sie für eine weitere Datenerhebung zu Forschungszwecken zur Verfügung stehen, wird davon mit umfasst.[861]

12.9 Sozialdatenschutzrecht

Das Sozialdatenschutzrecht enthält **eigenständige Regelungen** zur Einschränkung der Informationspflicht (§§ 82, 82a SGB X), des Auskunftsrechts (§ 83 SGB X), des Rechts auf Widerspruch, auf Einschränkung der Verarbeitung und auf Berichtigung (§ 84 SGB X) sowie zum Recht auf Vergessenwerden (s.u.).[862]

Hinsichtlich der Weiterverarbeitung von übermittelten Sozialdaten für Forschungszwecke enthält § 75 Abs. 4 S. 5 Nr. 4 SGB X die Festlegung, dass die **Löschung von Forschungsdaten** zu einem genau zu benennenden Termin zu erfolgen hat. Weiter heißt es in S. 6:

„Nach Ablauf der Frist nach Satz 5 Nummer 4 können die verarbeiteten Daten bis zu zehn Jahre lang gespeichert werden, um die Nachprüfung der Forschungsergebnisse auf der Grundlage der ursprünglichen Datenbasis sowie eine Verarbeitung für weitere Forschungsvorhaben nach Absatz 2 zu ermöglichen."[863]

Die Betroffenenrechte werden in Bezug auf die Verarbeitung von Sozialdaten zudem in § 84 SGB X konkretisiert:

> *„(1) Ist eine Löschung von Sozialdaten im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung von Sozialdaten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die Sozialdaten unrechtmäßig verarbeitet wurden.*
>
> *(2) Wird die Richtigkeit von Sozialdaten von der betroffenen Person bestritten und lässt sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen, gilt ergänzend zu Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679, dass dies keine Einschränkung der Verarbeitung bewirkt, soweit es um die Erfüllung sozialer Aufgaben geht; die ungeklärte Sachlage ist in geeigneter Weise festzuhalten. Die bestrittenen Daten dürfen nur mit einem Hinweis hierauf verarbeitet werden.*

860 Zur Risikobewertung und zu den zu ergreifenden Maßnahmen vgl. das Schwerpunktheft DuD 3/2020.
861 Dammann/Simitis, Art. 6 Rn. 18.
862 Bieresborn NZS 2018, 10ff.; Schäfer in Kipker/Voskamp, 314ff.
863 Dierks in Dierks/Roßnagel, 89.

(3) Ergänzend zu Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 gilt Absatz 1 Satz 1 und 2 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(4) Sind Sozialdaten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig, gilt ergänzend zu Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 Absatz 1 entsprechend, wenn einer Löschung satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

(5) Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung von Sozialdaten verpflichtet.

(6) § 71 Absatz 1 Satz 3 bleibt unberührt."

13 Auslandskooperationen

Angesichts von **globalen Herausforderungen**, auch im Gesundheitsbereich, ist eine weltweite Kooperation von Forschenden zur Erlangung neuer Erkenntnisse oft unabdingbar. Tatsächlich findet medizinische Forschung immer mehr grenzüberschreitend, gesamteuropäisch und international statt.[864] Dies setzt in vielen Fällen einen Austausch personenbeziehbarer Daten voraus. Das Regelungsregime für die Forschung unterscheidet sich in den Rechtsordnungen teilweise stark, insbesondere wenn es um die Anerkennung und den Schutz des Grundrechts auf Datenschutz geht. Es ist aus verfassungsrechtlicher Sicht nicht möglich, aber auch aus praktischer Sicht nicht angebracht, einen in anderen Staaten gepflegten Umgang mit Gesundheitsdaten für Forschungszwecke, der nicht europäischen Standards entspricht, zum Vorbild zu nehmen.[865] Datenschutz darf und soll zugleich aber auch sinnvolle grenzüberschreitende Forschungsprojekte nicht verhindern.

Unterschiedliche Konzepte beim Datenschutz in verschiedenen Staaten müssen respektiert werden.[866] Dies darf jedoch nicht dazu führen, dass die grundlegenden Verfassungsrechte der Betroffenen und der Schutz von deren informationeller Selbstbestimmung aufgegeben werden. Insofern bestehen schon für den Gesundheitsbereich einige wenige grundlegende Regelwerke.[867] Die DSGVO enthält darüber hinausgehend wirksame Lösungsansätze.

---

864 Deutscher Ethikrat, 61; Weichert 2018, Kap. 3.12.

865 So aber Thüsing/Rombey NZS 2019, 203.

866 RfII, 11.

867 Z.B. World Medical Association (WMA), WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, überarbeitet Oktober 2016; Überblick bei Dochow, 279ff.

13.1 Übermittlungen in der EU und im EWR

Die Einbindung ausländischer Beteiligter als Projektpartner oder Dienstleister bei der Verarbeitung personenbezogener Daten richtet sich nach der DSGVO. Soweit hierbei Daten an **Projektpartner mit Sitz in der Europäischen Union** (EU) übermittelt werden sollen, gelten die gleichen Voraussetzungen wie für Übermittlungen innerhalb Deutschlands (Art. 1 Abs. 3 DSGVO).

Entsprechendes gilt für Empfänger in den Mitgliedstaaten des **Europäischen Wirtschaftsraums** (EWR) Norwegen, Liechtenstein und Island.[868] Gemäß Art. 7 lit. a Hauptabkommen über den EWR (EWR-Abkommen) sind alle EWR-Staaten verpflichtet, die DSGVO innerstaatlich zu übernehmen. Um Anwendung zu finden, müssen Rechtsvorschriften vom EWR-Ausschuss überprüft werden und, so sie zur Anwendung kommen sollen, in die Protokolle und Anhänge zum EWR-Abkommen übernommen werden. Dies ist am 06.07.2018 geschehen, sodass die DSGVO seit dem 20.07.2018 dort gilt und unmittelbar anwendbar ist.

Das Verhältnis zwischen der EU und Großbritannien ist noch nicht endgültig geklärt. Gemäß dem Brexit-Abkommen wurde der Übergangszeitraum der Zulassung von Datentransfers zunächst bis zum 31.07.2021 verlängert. Danach ist das Land als Drittland zu behandeln (s.u. Kap. 13.2). Die EU-Kommission hat am 28.06.2021 einen Angemessenheitsbeschluss gemäß Art. 45 DSGVO angenommen. Datenübermittlungen in das Vereinigte Königreich benötigen also keiner besonderen Genehmigung. Diese Entscheidung steht aber unter einem Prüfungsvorbehalt, da die britische Regierung angekündigt hat, ihr Datenschutzrecht zu entbürokratisieren. Zu den Punkten, die weitere Klarstellungen beziehungsweise eine spezielle Kontrolle erforderten, zählt zudem die im Vereinigten Königreich praktizierte Massenüberwachung. Ob das Datenschutzniveau in Großbritannien von der EU-Kommission langfristig als angemessen anerkannt werden wird, hängt davon ab, ob und inwieweit das Land die bisherigen Datenschutzregeln ändert.[869]

13.2 Übermittlungen an Drittstaaten

Ansonsten, also bei Datenübermittlungen an Empfänger aus Drittländern außerhalb der EU und des EWR, gelten die Art. 44ff. DSGVO, wonach beim Empfänger nicht ein gleichwertiges, wohl aber ein angemessenes Datenschutzniveau gewährleistet sein muss. Generell ist Art. 44 DSGVO anzuwenden:

> *„Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestim-*

868 Art. 217, 288 Abs. 2 AEUV, vgl. zu Großbritannien Selmayr/Ehmann in Ehmann/Selmayr, Einführung Rn. 106.
869 Mühlauer, Großbritannien: Goodbye, verhasste Cookie-Banner, www.sueddeutsche.de 26.08.2021.

mungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird."

Hat die Kommission der EU beschlossen, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet, dann bedarf es für die jeweiligen Datenübermittlungen keiner besonderen Genehmigung (Art. 45 Abs. 1 DSGVO). Solche umfassenden **Genehmigungen für Übermittlungen** gibt es noch nach den Regelungen des Art. 25 Abs. 6 UAbs. 1 EG-DSRl, die auch unter der DSGVO weiterhin gültig sind, für folgende Staaten: Andorra, Argentinien, Guernsey, Faröer-Inseln, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz[870], Uruguay.[871] Die für die EG-DSRl geltenden Angemessenheitsbeschlüsse wurden durch den Durchführungsbeschluss (EU) 2016/2295 an die Anforderungen angepasst, die der EuGH durch sein Safe-Harbor-Urteil vom 06.10.2015 (Schrems I) aufgestellt hatte.[872] Die Anforderungen wurden vom EuGH in seinem Urteil zum Privacy Shield vom 16.07.2020 (Schrems II) bekräftigt und präzisiert.[873]

Am 23.01.2019 wurde von der EU-Kommission ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO in Bezug auf **Japan** gefällt.[874]

Das in den **USA** geltende Datenschutzniveau wird vom EuGH als nicht angemessen bewertet.[875] Das oberste europäische Gericht hat deshalb die Angemessenheitsbeschlüsse der EU-Kommission aus dem Jahr 2000 und aus dem Jahr 2016 aufgehoben. Diese Angemessenheitsbeschlüsse beruhten jeweils auf einem umfangreichen Rechtsrahmen, der beim EU-US-Privacy-Shield in seinen wesentlichen Grundstrukturen von Safe-Harbor übernommen worden war.

Die fehlende Angemessenheit des Datenschutzniveaus hat seinen Grund in gesetzlichen Regelungen in den USA, die es Behörden mit den Argumenten der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates erlaubt, in massenhaftem Umfang auf personenbezogene Daten zuzugreifen. Hiergegen bestehen **keine wirksamen Rechtsschutzmöglichkeiten** für die Betroffenen. Außerdem fehlt es an einer unabhängigen Datenschutzkontrolle.

Zwecks Kompensation dieser Defizite bedarf es bei einem Datenexport in die USA „geeigneter Garantien". Diese können sich aus von der Kommission erarbeiteten Standarddatenschutzklauseln ergeben (s.u.). Die bisher geltenden Klauseln sind aber nicht ausreichend. Vielmehr sind **ergänzende Vertragsregelungen** nötig. Diese können darin bestehen, dass dem Datenimporteur in den USA Informationspflichten gegenüber dem europäischen Exporteur auferlegt werden, wenn die importierten Daten einer zweckwidrigen Nutzung zugeführt werden sowie wenn von den Betrof-

870 Mausbach ZD 2019, 450.

871 Schantz in SHS, Art. 45 Rn. 28.

872 EuGH 06.10.2015 – C-362/14 (Safe Harbor), NJW 2015, 3151 = JZ 2016, 360 = DuD 2015, 823 = NVwZ 2016, 43 = WM 2015, 2383 = MMR 2015, 753 = K&R 2015, 710 = DÖV 2015, 1070.

873 EuGH 16.07.2020 – C-311/18 (Privacy Shield), NJW 2020, 2613 = DuD 2020, 685 = WM 2020, 1495 = EuZW 2020, 941 = MMR 2020, 597; dazu Botta CR 2020, 505ff.; Golland NJW 2020, 2593ff.; Schröder DB 2020, 1945ff.; Voigt CR 2020, 513ff.; Frenz DVBl 2020, 1270ff.

874 Siehe https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en m.w.N. zu den Angemessenheitsbeschlüssen.

875 EuGH 06.10.2015 – C-362/14 (Safe Harbor, Schrems I), EuGH 16.07.2020 – C-311/18 (Privacy Shield Schrems II).

fenen, von europäischen Gerichten oder von europäischen Aufsichtsbehörden begründete Informationsersuchen vorliegen. Ein angemessener Rechtsschutz kann den Betroffenen gegenüber dem europäischen Datenexporteur zugesichert werden.[876]

Bei Nichtbestehen eines Angemessenheitsbeschlusses zu einem Empfängerland und Vorliegen geeigneter Garantien bedarf es der Genehmigung des Datentransfers. Dies ist insbesondere möglich über zuvor von der EU-Kommission genehmigte Standarddatenschutzklauseln (Art. 46 Abs. 2 DSGVO) oder über verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, Art. 47 DSGVO). Letztgenannte müssen von den **Aufsichtsbehörden genehmigt** werden. Möglich und auch zu empfehlen ist der separate Abschluss eines – auch zu genehmigenden – Export-Import-Vertrags, in dem Vertragspartner die Geltung und die Durchsetzbarkeit eines angemessenen Datenschutzniveaus verabreden.[877]

Als Legitimation von Datenübermittlungen ins Drittausland im Forschungsbereich bieten sich **Standarddatenschutzklauseln** (früher Standardvertragsklauseln) gemäß Art. 46 Abs. 2 lit. c, d DSGVO an, an denen sich alle Beteiligten eines möglicherweise umfangreichen Forschungsprojektes beteiligen. Bisher gibt es keine von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der EU-Kommission gemäß Art. 93 Abs. 2 DSGVO genehmigt wurden (Art. 46 Abs. 2 lit. d DSGVO). Notwendig ist aber eine Ergänzung bei den genehmigten Klauseln, wenn im konkreten Fall die Garantien nicht ausreichen.[878] Gemäß Art. 46 Abs. 5 DSGVO bleiben aber auf der Grundlage der Richtlinie 95/46/EG (EG-DSRl) genehmigte Standardvertragsklauseln gültig, bis sie geändert, ersetzt oder aufgehoben wurden. Die EU-Kommission hat bisher folgende Klauseln genehmigt: Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer vom 15.06.2001 (Set 1)[879], alternative Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer vom 27.12.2004 (Set 2)[880] und Standardvertragsklauseln über die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer vom 05.02.2010.[881]

Als Grundlage für eine Datenübermittlung ins Drittausland kommen weiterhin genehmigte **Verhaltensregeln** nach Art. 40 Abs. 3 DSGVO in Betracht (Art. 46 Abs. 2 lit. e DSGVO). Derartige Verhaltensregeln (Codes of Conduct – CoC) werden von Verbänden oder Vereinigungen aufgestellt und dienen der Spezifizierung der Vorgaben der DSGVO in bestimmten Branchen (vgl. Art. 40 Abs. 2 DSGVO). Sie müssen geeignete Garantien für Übermittlungen in Drittländer vorsehen und von einer Aufsichtsbehörde genehmigt worden sein. Derartige Verhaltensregeln können für den Forschungsbereich oder spezifische für den medizinischen Forschungsbereich von den einschlägigen Forschungsverbänden in Deutschland erarbeitet und von den jeweils zuständigen Aufsichtsbehörden genehmigt werden.[882]

876 EuGH 16.07.2020 – C-311/18 Rn. 105; LfDI Baden-Württemberg, Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer? 07.09.2020; so schon Weichert/Schuler, DuD 2016, 386ff.

877 Weichert/Schuler DuD 2016, 386ff.

878 EuGH 16.07.2020 – C-311/18, Rn. 132f; Kociok/Hofmann K&R 2020, 594f.

879 2001/497/EG, ABl. L 181 v. 04.07.2001, 19–31, Aktenzeichen K(2001) 1539, konsolidierte Fassung v. 17.12.2016.

880 2004/915/EG, ABl. L 385/74 v. 19.12.2004, Aktenzeichen K(2004) 5271.

881 2010/87/EU, ABl. L 39/5 v. 12.02.2010, Aktenzeichen K(2010) 593, alle Klauseln sind abgedruckt in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2015, Anlagen 4–6.

882 Ausführlich dazu die Kommentierung von Weichert in DWWS, Art. 40, 41.

13.3 Einwilligung und weitere bestimmte Ausnahmen

Fehlt es an einem Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO, an verbindlichen internen Datenschutzvorschriften nach Art. 47 sowie an sonstigen geeigneten Garantien für eine Datenübermittlung ins Drittausland oder an eine internationale Organisation, so erlaubt Art. 49 Abs. 1 UAbs. 1 DSGVO Datenübermittlungen unter folgenden **Bedingungen**:

> *„a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde, […]*
>
> *d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig, […]*
>
> *g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind."*

Art. 49 DSGVO ist als **Ausnahmevorschrift** konzipiert. Sie eignet sich nicht für Verarbeitungen, die massenhaft, wiederholt und routinemäßig erfolgen.[883] Bevor eine Übermittlung nach Art. 49 DSGVO erlaubt wird, ist zu prüfen, ob dies nicht durch Art. 48 DSGVO ausgeschlossen wird, der eine internationale Übereinkunft oder ein Rechtshilfeabkommen voraussetzt.[884]

Gemäß Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO kann eine **Einwilligung** Übermittlungen ins unsichere Drittausland legitimieren. Hierfür müssen zunächst sämtliche Voraussetzungen für eine wirksame Einwilligung nach der DSGVO vorliegen (Art. 4 Nr. 11, 6 Abs. 1 UAbs. 1 lit. a, 7, 9 Abs. 2 lit. a), wozu insbesondere die Freiwilligkeit, die Bestimmtheit und der Hinweis auf die Widerruflichkeit gehören. Die Einwilligung muss „ausdrücklich" sein. Entsprechend Art. 9 Abs. 2 lit. a DSGVO, wonach sich die ausdrückliche Erklärung auf die Verarbeitung sensitiver Daten beziehen muss, muss hier ausdrücklich auf die Verarbeitung im unsicheren Drittausland Bezug genommen werden. Zudem muss auf die bestehenden Risiken hingewiesen worden sein. Diese Unterrichtung kann allgemeiner Art sein, sollte aber so konkret wie möglich auf die beim Empfänger bestehenden Risiken eingehen. Der Betroffene ist darüber zu informieren, welche Daten an welchen Empfänger und welchen Zielort übermittelt werden und welche Verarbeitungen dort geplant sind. Als Risiko ist zu benennen, dass möglicherweise Betroffenenrechte nicht adäquat durchgesetzt werden können. Liegen konkrete Erkenntnisse über die Verarbeitungspraxis vor, so ist darauf hinzuweisen.[885] Ändern

883 Zerdick in Ehmann/Selmayr, Art. 49 Rn. 4.

884 EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 v. 25.05.2018, 5; Schantz in SHS, Art. 49 Rn. 36; Schröder in Kühling/Buchner, Art. 49 Rn. 24.

885 EDPB, Guidelines 2/2018 v. 25.05.2018, 7f.; Ambrock/Karg ZD 2017, 157; Däubler in DWWS, Art. 49 Rn. 5; Zerdick in Ehmann/Selmayr, Art. 49 Rn. 6; vgl. das Beispiel der Gendatenübermittlung nach Hongkong, Netzwerk Datenschutzexpertise, 20.03.2020, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_eluthia_previatest_final.pdf.

sich Bedingungen bei der Datenverarbeitung und dem Risiko, so ist zumindest eine Information an den Betroffenen, bei wesentlichen Änderungen eine erneute Einwilligung nötig.[886]

Wegen der verschärften Anforderungen gegenüber dem alten Recht kann nicht davon ausgegangen werden, dass (wirksame) **alte Einwilligungen** in den Drittlandstransfer[887] ab Mai 2018 weiterhin wirksam sind. Es bedarf vielmehr einer Feststellung im konkreten Fall, dass die Voraussetzungen des Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO vorliegen.[888]

Die Ausnahmevorschrift des Art. 49 Abs. 1 UAbs. 1 lit. d DSGVO, die Übermittlungen ins unsichere Drittausland aus Gründen des **öffentlichen Interesses** erlaubt, zielt auf öffentliche Stellen ab. Private als Empfänger sind aber nicht völlig ausgeschlossen.[889] Solche Gründe können in den Bereichen der Steuerverwaltung, der sozialen Sicherung oder der öffentlichen Gesundheit liegen. Ausdrücklich als Beispiele genannt werden die *„Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport"* (ErwGr 112 S. 1). Ein öffentliches Interesse des Empfängerstaates soll nicht genügen; es bedarf eines solchen Interesses der Union oder eines Mitgliedstaats. Für die Übermittlung muss im konkreten Fall ein wichtiger Grund vorliegen. Der wichtige Grund muss nach Art. 49 Abs. 4 DSGVO im Unionsrecht oder im Recht eines Mitgliedsstaats anerkannt sein.[890] Weiterhin ist zu prüfen, ob geeignete Garantien gemäß Art. 46 Abs. 2 lit. a DSGVO oder in Form völkerrechtlicher Zusicherungen bestehen.[891] Für Forschungszwecke kommt eine Übermittlung z.B. zur Erkundung der Ursachen und der Bekämpfung einer aktuellen Pandemie in Frage.

Eine **Registerübermittlung** nach Art. 49 Abs. 1 UAbs. 1 lit. g DSGVO betrifft öffentliche Register, die nicht notwendigerweise von einer Behörde geführt sein müssen. Private Datensammlungen werden aber nicht erfasst. Als Beispiele werden das Grundbuch, das Handelsregister, das Vereinsregister, das Bundeszentralregister sowie sonstige „Transparenzregister" genannt. Die Register müssen für jedermann frei zugänglich sein. Eine Übermittlung ist nur zulässig an Personen oder Stellen, die ein berechtigtes Interesse haben und selbst in das Register Einblick nehmen dürften.[892] Besondere Relevanz erlangt die Regelung für internetgestützte Register.[893] Es ist nicht erkennbar, dass der Unionsgesetzgeber von der Vorschrift auch Forschungsregister erfasst sehen wollte. Sind aber die rechtlichen Voraussetzungen gegeben, so können über diese Ausnahmeregelungen Übermittlungen gerechtfertigt sein.

886 Klein/Pieper in SJTK, Art. 49 Rn. 6.
887 Hierzu Artikel 29-Datenschutzgruppe, WP 114 v. 25.11.205, 12–14.
888 EDPD, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 v. 25.05.2018, 4f.; Ambrock/Karg ZD 2017, 157f.; vgl. ErgGr 111.
889 EDPB, Guidelines 2/2018 v. 25.05.2018, 11.
890 EDPB, Guidelines 2/2018 v. 25.05.2018, 10f.; Zerdick in Ehmann/Selmayr, Art. 49 Rn. 14; Hladjik in Auernhammer, Art. 49 Rn. 6.
891 Schantz in SHS, Art. 49 Rn. 38 mit Verweis auf die Rechtsprechung von EuGH und BVerfG.
892 EDPB, Guidelines 2/2018 v. 25.05.2018, 13f.; Zerdick in Ehmann/Selmayr, Art. 49 Rn. 17; Däubler in DWWS, Art. 49 Rn. 16; Schantz in SHS, Art. 49 Rn. 49.
893 Zerdick in Ehmann/Selmayr, Art. 49 Rn. 17.

13.4 Übermittlungen von Sozialdaten

Wegen der Öffnungsklauseln in der DSGVO und des abschließenden Charakters der Verarbeitungsregeln in den SGB richtet sich die grenzüberschreitende Übermittlung von Sozialdaten, **auch für Forschungszwecke**, nicht direkt nach den Regeln der DSGVO, sondern ist im SGB selbst geregelt. § 77 Abs. 1 SGB X dient als Rechtsgrundlage für die Übermittlung in andere Staaten der EU bzw. des EWR. § 77 Abs. 2 SGB X ist Rechtsgrundlage für Übermittlungen in Länder außerhalb der EU mit Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO). Liegt kein Angemessenheitsbeschluss vor, so ist in Anwendung von § 77 Abs. 3 SGB X eine Datenübermittlung erlaubt auf der Grundlage *„zwischenstaatlicher Übereinkommen auf dem Gebiet der sozialen Sicherheit"* (Nr. 1) oder soweit die Voraussetzungen von § 69 Abs. 1 Nr. 1 u 2 oder § 70 SGB X vorliegen und dem keine schutzwürdigen Interessen der Betroffenen entgegenstehen.[894] Da die §§ 69, 70 SGB X auf die Erfüllung sozialer Aufgaben sowie des Arbeitsschutzes abzielen, können Sozialdaten für Forschungszwecke in das aus Datenschutzsicht unsichere Drittausland nur auf der Grundlage zwischenstaatlicher Übereinkommen übermittelt werden.

13.5 Übermittlung von Berufsgeheimnissen

Keine Rechtsklarheit besteht, inwieweit **Berufsgeheimnisse** ins Ausland transferiert werden dürfen. Eine Vermutung hierfür besteht, wenn datenschutzrechtlich die Angemessenheit des Schutzniveaus im Ausland festgestellt wurde. Art. 9 Abs. 3 DSGVO erlaubt ergänzend, dass sensitive Daten für die in Art. 9 Abs. 2 lit. h DSGVO genannten Zwecke verarbeitet werden, *„wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedsstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt."*

Hintergrund dieser Regelung ist, dass die EU-Mitgliedstaaten ihre Regelungen zu Berufsgeheimnissen mit der DSGVO nicht aufgeben wollten.[895] Die Regelung ist dahingehend zu verstehen, dass national oder europarechtlich zusätzliche Verarbeitungsvoraussetzungen geregelt werden können, aber nicht müssen. Art. 9 Abs. 3 DSGVO erlaubt dem deutschen Gesetzgeber die Aufrechterhaltung des für Berufsgeheimnisse geltenden Zwei-Schranken-Prinzips (s.o. Kap. 6.3).

Irritierend ist aber, dass die Öffnungsklausel des Art. 9 Abs. 3 DSGVO auf Verarbeitungszwecke nach Abs. 2 lit. h beschränkt ist. Die dort genannten *„Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich"*

schließen **medizinische Forschung** nicht generell mit ein. Diese findet als „wissenschaftliche Forschung" in Art. 9 Abs. 2 lit. j DSGVO ausdrücklich Erwähnung.

Bei der Verwendung von **Gesundheitsdaten** für Forschungszwecke kann auf die lit. h oder i zurückgegriffen werden, wenn diese „im öffentlichen Interesse" „gesundheits-

894 Bieresborn NZS 2017, 931f.
895 Albrecht/Jotzo, Teil 3 Rn. 58.

bezogenen Zwecken" dient (ErwGr 53 S. 159). Damit kommt keine skeptische Haltung des Verordnungsgebers gegenüber medizinischer Forschung und Entwicklung zum Ausdruck.[896] Es wird lediglich klargestellt, dass rein kommerziell ausgerichtete Forschung etwa von Pharmaunternehmen oder Unternehmen im Bereich der Biotechnik die Privilegierungen von Art. 9 Abs. 2 DSGVO nicht in Anspruch nehmen können.[897] Die Alternativen in Art. 9 Abs. 2 DSGVO können sich teilweise überschneiden. Die nicht anwendungsorientierte medizinische Forschung ist aber ausschließlich in lit. j und nicht in lit. h geregelt. Aus Art. 9 Abs. 3 DSGVO kann also nicht geschlossen werden, dass und inwieweit mit der Geltung der DSGVO Berufsgeheimnisse ein Hindernis für einen grenzüberschreitenden Datentransfer sind.

Auch aus den sonstigen Regelungen ergeben sich keine klaren Hinweise darauf, ob grenzüberschreitende Übermittlungen von Berufsgeheimnissen für Forschungszwecke erlaubt oder untersagt sein sollen. Klar ist, dass insofern Öffnungsklauseln zur Anwendung kommen, die insbesondere in Art. 9 Abs. 2 lit. j und Art. 89 Abs. 2 DSGVO geregelt sind. Die deutschen Gesetzgeber sahen es offenbar bisher nicht für notwendig an, die internationale Forschungskommunikation mit Berufsgeheimnissen zu regeln. Es ist deshalb naheliegend, insofern eine **grundrechtsbasierte Abwägung** vorzunehmen. Dabei kann die Erwägung eine Rolle spielen, inwieweit angesichts der spezifischen Situation der Auslandsverarbeitung und angesichts der bestehenden konkreten Risiken ein gleichartiger Schutz im Interesse der Schutzziele des Berufsgeheimnisses nötig ist.[898] Angesichts der restriktiven Regeln in Art. 49 Abs. 1 S. 1 lit. a DSGVO kann eine Einwilligung als Offenbarungsbefugnis zu Berufsgeheimnissen gegenüber Empfängern im unsicheren Drittausland im Ausnahmefall wirksam sein. Auch bei sonstigen Offenbarungen in ein Drittland muss eine wirksame Schweigepflichtentbindung als Mindestvoraussetzung vorliegen.

Bei einer **Verarbeitung für Forschungszwecke** kommt es – den Grunderwägungen der Privilegierung dieser Zwecke in der DSGVO folgend – weniger auf den Schutz des individuellen Vertrauensverhältnisses an als auf eine strenge Zweckbindung und Abschottung der Forschung gegen operative Zwecke (s.o. Kap. 8). Von materiell-rechtlicher Relevanz ist der Umstand, dass Dienstleister, die durch § 203 Abs. 3, 4 StGB gebunden sind und dadurch zu Berufsgeheimnisträgern werden, vor deutschen Gerichten gemäß § 5 Nr. 7 StGB zur Verantwortung gezogen werden können, selbst wenn der Geheimnisverrat nach ausländischem Recht nicht strafbar ist.[899] Umgekehrt kann von Bedeutung sein, wenn, anders als nach deutschem Recht, wo mitwirkende Personen durch ein Zeugnisverweigerungsrecht geschützt sind (§ 53a StPO)[900], ein entsprechender Schutz im Ausland nicht besteht.[901] Kein Berufungsfall kann es dagegen sein, dass mit bestimmten Auslandsübermittlungen ein bestehendes Vollzugsdefizit nur vertieft wird.[902]

896 So aber Härting, Rn. 549.
897 Weichert in Kühling/Buchner, Art. 9 Rn. 150.
898 Grosskopf/Momsen CCZ 2018, 103.
899 Pohle/Ghaffari CR 2017, 493.
900 Zu dieser Notwendigkeit Momsen/Savić, KriPoZ 2017, 303f.
901 Grosskopf/Momsen CCZ 2018, 105.
902 Ebenso Grosskopf/Momsen CCZ 2018, 103f.

Für einige Berufsgeheimnisträger ist die Mitwirkung von ausländischen Dienstleistern ausdrücklich geregelt, etwa für Rechtsanwälte (§ 43e Abs. 4 BRAO), Steuerberater oder Wirtschaftsprüfer:

„Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet."[903]

Eine entsprechende **explizite Regelung** für medizinische Berufsgeheimnisträger gibt es nicht. In der Gesetzesbegründung zu den genannten Regelungen wird ausgeführt, dass für die anderen Mitgliedstaaten der EU *„in der Regel von einem solchen Schutz ausgegangen werden"* kann. Bei anderen Staaten sei im Einzelfall zu prüfen, ob der erforderliche Schutz gewährleistet ist.[904] Aus den bereichsspezifischen Regelungen wird teilweise geschlossen, dass in Bezug auf die nicht spezifisch geregelten Berufsgruppen, zu denen auch die Heilberufe gehören, keine weiteren Einschränkungen bestehen.[905] Ein mit dem Inland vergleichbares Schutzniveau wird aber generell im Datenschutzrecht gefordert (Art. 44ff. DSGVO). Es ist nicht erkennbar, dass mit den Übermittlungsregelungen der DSGVO der berufsspezifische Geheimschutz umgangen werden sollte, soweit keine spezifischen Regelungen zur Auslandsübermittlung bestehen.

13.6 Anonymität bei Datenbeschaffung aus einem Drittland

Auf eine Datenübermittlung aus dem Drittland folgt eine Datenerhebung in der EU. Die Übermittlung für Forschungszwecke von Daten aus dem Ausland ist nach dem jeweiligen Recht des Staates zu bewerten, aus dem die Daten übermittelt werden. Werden nach dem **Recht des übermittelnden Staates** Daten als anonym eingestuft, sodass sie nicht unter das dortige Datenschutzrecht fallen und deshalb übermittelt werden dürfen, so hat dies jedoch keine Indizwirkung für die Bewertung der Erhebung dieser Daten und deren weitere Verarbeitung nach europäischem Recht.

Eine **Erhebung in der EU** stellt gemäß Art. 4 Nr. 1 DSGVO eine Form der Datenverarbeitung dar, soweit nach der DSGVO die Daten als personenbezogen zu bewerten sind. Alleiniger Beurteilungsrahmen sind hierbei die Vorgaben zum Personenbezug nach Art. 4 Nr. 1 DSGVO. Gemäß dem hierbei anzulegenden objektiven Maßstab kommt es darauf an, ob die übermittelten Proben oder Datensätze *„nach allgemeinem Ermessen genutzt werden [können], um die natürliche Person direkt oder indirekt zu identifizieren […]"* (ErwGr 26, S. 3). Bei dieser Feststellung sollen *„alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."* (ErwGr 26, S. 4).

903 So § 43e Abs. 4 BRAO, ebenso § 62a Abs. 4 Steuerberatungsgesetz, § 50a Abs. 4 Wirtschaftsprüferordnung.

904 BT-Drs. 18/11936, 35; dazu ausführlich mit Ausführungen zum Beschlagnahmeschutz in verschiedenen Ländern der EU Dierlamm/Ihwas BB 2017, 1097ff.

905 Eisele JR 2018, 85.

Maßgeblich ist also auch, wie wahrscheinlich es ist, dass im Drittausland vorliegende Information innerhalb der EU zur Reidentifizierung von Datensätzen verfügbar gemacht werden können.

Es kommt also darauf an, ob das zur Identifizierung erforderliche Zusatzwissen für die Verantwortlichen, also hier für Forschende in der EU, verfügbar gemacht werden kann. Ein hierfür relevanter Aspekt ist gemäß der Rechtsprechung des EuGHs, ob das **Zusatzwissen rechtmäßig beschafft** werden kann.[906] Dabei geht der EuGH davon aus, dass die unzulässige Beschaffung von Zusatzwissen unwahrscheinlich sei. Hiervon kann aber selbst im EU-Binnenmarkt nicht ausgegangen werden. Besteht bzgl. der Verhinderung der Beschaffung des Zusatzwissens ein Vollzugsdefizit, so muss ein Personenbezug angenommen werden, wenn eine illegale Datenbeschaffung vorstellbar ist.[907] Ist das Zusatzwissen nur in einem Drittstaat verfügbar und besteht auch dort ein Vollzugsdefizit im Bereich des Datenschutzes, so ist die Unzulässigkeit der Beschaffung ebenso wenig ein Hinderungsgrund für die Beschaffung und das Nutzen des Zusatzwissens. Dies gilt erst recht, wenn, wie etwa in den USA, kein wirksamer Rechtsschutz gegen Datenschutzverstöße gewährt wird.[908] So zeigte sich z.B., dass in den USA die Fa. Clearview – rechtlich bisher unbeanstandet – eine Datenbank zur automatisierten biometrischen Gesichtserkennung weltweit bereitgestellt hat, die mithilfe von Scraper-Software im Internet mehr als 3 Mrd. Fotos abgesaugt hat, mit denen global Gesichter Identitäten zugeordnet werden können.[909] Ist dagegen das Zusatzwissen im Drittstaat für den Verantwortlichen in der EU faktisch nicht zugänglich, so kann sich hieraus ergeben, dass ein konkreter Datensatz als anonym anzusehen ist.

906 EuGH 19.10.2016, C-582/14 (Breyer), Rn. 46, NJW 2016, 3579 = NVwZ 2017, 213 = EuZW 2016, 909 = BB 2016, 2830 = K&R 2016, 811.

907 Karg in SHS, Art. 4 Nr. 1 Rn. 64; Weichert in DWWS, Art. 4 Rn. 25; Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 28f.

908 In Bezug auf Gesundheitsdaten Solove/Schwartz, Privacy Law Fundamentals, 2011, 71ff.; generell EuGH 06.110.2015 – C-362/14 Rn. 84–98; EDPS, Stellungnahme 4/2016 zu EU-US-Datenschutzschild v. 30.05.2016, 11f.; Article 29 Data Protection Working Party, WP 255, EU-U.S. Privacy Shield – First annual Joint Review, v. 28.11.2017, 18; dies., WP 238, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, v. 13.04.2016, 25ff., 51f.; Schantz in SHS, Art. 45 Rn. 42f.; 69; Weichert, ZD 2016, 213f.; Weichert RDV 2012, 113ff.

909 Beuth/Horchert, Anonym? War gestern! Der Spiegel Nr. 5 v. 25.01.2020, 43; Hurtz, Eine Technologie und ihre Gefahren; Schmieder, Modus Tarnkappe, SZ 23.01.2020, 18; Brühl/Hurtz, Ich kann dich sehen, SZ 21.01.2020, 18.

14 Kritik und Verbesserungsmöglichkeiten

Die obige Darstellung der Rechtslage zeigt, dass die Vorgaben der DSGVO einen sinnvollen Ausgleich zwischen der Forschungsfreiheit und dem Datenschutz ermöglichen. Zugleich ist aber erkennbar, dass die wegen der Öffnungsklauseln zulässigen nationalen Regelungen die europäischen Vorgaben nur unzureichend umsetzen. Im Folgenden sollen die sich daraus ergebenden **Probleme bei der Umsetzung** von Datenschutz in der medizinischen Forschung dargelegt werden. Daraus werden dann Vorschläge abgeleitet, mit denen insbesondere gesetzgeberisch bestehende Defizite behoben werden können.

14.1 Defizite

Von vielen Seiten wird immer wieder beklagt, dass Datenschutzregelungen die **medizinische Forschung behindern** würden. Dabei werden die bestehenden Regelungen zumeist mit dem grundrechtlichen Anliegen des Datenschutzes in einen Topf geworfen.[910]

Der Datenschutz im Gesundheitsbereich generell wie auch der Datenschutz im Bereich der Medizinforschung leiden darunter, dass sie einerseits über-, andererseits unterreguliert sind: Die **Überregulierung** ergibt sich daraus, dass Regelungen auf vielen Ebenen und aus verschiedenen Regelwerken anzuwenden sind: auf EU-Ebene – DSGVO, auf nationaler Ebene – BDSG, das BGB (§§ 630a ff.), § 203 StGB, die

910 Nachweise, auch für die Undifferenziertheit der Kritik, bei Thüsing/Rombey NZS 2019, 201f.

Sozialgesetzbücher, viele bereichsspezifische Regelungen, auf Landesebene – die LDSG, Landeskrankenhausgesetze und viele weitere spezialgesetzliche Regelungen sowie die Berufsordnungen der Landesärztekammern, die sich weitgehend an der MBOÄ orientieren.[911] Die Regelungen sind nur begrenzt aufeinander abgestimmt, auch soweit deren Anpassung an die DSGVO erfolgte. Es wurde vorrangig eine formelle und keine inhaltliche Anpassung vorgenommen. Die Regelungen führen zu einem normativen Flickenteppich. Sie sind unübersichtlich, in sich teilweise widersprüchlich und für Anwender in der Praxis oft nicht oder nur unter großem Aufwand umzusetzen.[912]

Die **Unterregulierung** insbesondere im Forschungsbereich ergibt sich daraus, dass eine Vielzahl von Fragen ungeklärt bleibt, so etwa der Bereich der Genforschung, der Umgang mit Biobanken, aber auch die Konkretisierung der teilweise sehr allgemeinen strafrechtlichen und datenschutzrechtlichen Vorgaben, etwa die Feststellung eines privilegierten Forschungsvorhabens. Soweit Gesetze eine Abwägung zwischen den Betroffeneninteressen und den Forschungsinteressen vorsehen, werden keine handhabbaren Abwägungskriterien vorgegeben.[913] Hinzu kommen große Vollzugsdefizite insbesondere im Bereich der Datenschutzaufsicht.[914]

Den geltenden Regelungen zur (medizinischen) Forschung ist gemein, dass eine Datennutzung ohne Einwilligung der Betroffenen nur im Ausnahmefall auf der Grundlage einer Güterabwägung erlaubt ist. Die **Einwilligung hat absoluten Vorrang** als rechtliche Legitimation. Dieser Grundsatz folgt dem Wunsch, dass der Betroffene idealerweise selbst bestimmen soll, wer worüber mit seinen Daten forschen darf. Dieses Kernprinzip der informationellen Selbstbestimmung ist unbestritten. Allerdings kann es nicht in allen Lebensbereichen uneingeschränkt realisiert werden, weil in Zivilgesellschaften stets eine Balance zwischen individuellen und gemeinschaftlichen Belangen herzustellen ist. Im überwiegenden Allgemeininteresse müssen Abweichungen zulässig sein, wobei es allerdings (gesetzlicher) Regeln bedarf, die die Wahrung der Verhältnismäßigkeit garantieren.[915] Von diesem Ansatz ist die DSGVO geprägt. Insofern sind im Zuge einer Neuregulierung der Nutzung medizinischer Daten für Forschungszwecke organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die einer Verletzung von Persönlichkeitsrechten effektiv vorbeugen.

Eine wirksame Einwilligung bzw. Schweigepflichtentbindung setzt voraus, dass sie informiert erfolgt, d.h. auf **hinreichend präzisen Informationen** darüber basiert, welche Stelle für welche Zwecke mit welchen Daten forschen können soll. Aus den unter Kap. 7.2 genannten Gründen fehlt eine klare Information aber oftmals.

911 Kritisch hierzu schon Kilian NJW 1998, 788.

912 Datenethikkommission, 20 (These 17); Sachverständigenrat, S. XXVIII (These 23), 200, 205; Weichert 2018, Kap. 10.8; Weichert MedR 2019, 624; Weichert/Krawczak MIBE 2019, Vol. 15(1), 3f./8; Kühling, 33; BKL-R, 218; ähnlich BT-Drs. 19/18111, 27; siehe auch den systematischen Überblick bei Weichert in Dockweiler/Fischer, ePublicHealth, 2019, 31, 42; Weichert in Bär/Grädler/Mayr, Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht, Bd. 1, 2018, 558f.; Dierks 2019, 11; ders. 2020, 4f.; Graf von Kielmansegg in TMF, 90; Hense in Sydow, Bundesdatenschutzgesetz, 2020, § 27 Rn. 5.

913 Graf von Kielmansegg in TMF, 106ff.

914 Datenethikkommission, 20 (These 18); Weichert MedR 2019, 624; zu den Defiziten bei der Strafverfolgung Weichert in AG Medizinrecht in DAV/IMR, Aktuelle Entwicklungen im Medizinstrafrecht, 2018, 119f.

915 Datenethikkommission, 96; Thüsing/Rombey NZS 2019, 203; Krawczak/Semler/Zenke/Strech/Graf von Kielmansegg in TMF, 129f.

Häufig lässt sich das wissenschaftliche Potenzial von Gesundheitsdaten nur durch eine **einrichtungsübergreifende** (**möglicherweise weltweite**) **Zusammenführung** der Daten angemessen ausschöpfen, etwa bei der Erforschung seltener Erkrankungen. Unter Umständen bedarf es darüber hinausgehend sogar einer interdisziplinären stellenübergreifenden wissenschaftlichen Zusammenarbeit.[916] Die Zusammenführung von Daten ist über Forschungsnetzwerke, Krankheitsregister oder andere Großprojekte realisierbar.[917] Allerdings gibt es hierfür, abgesehen von den Spezialfällen der Krebsregistergesetze, dem Implantateregister (§ 1 Abs. 2 Nr. 6 IRegG) und dem Transplantationsregister (§ 15a TPG), keine expliziten gesetzlichen Grundlagen. Die Rechtmäßigkeit der Datennutzung gründet vielmehr allein auf der Einwilligung der Betroffenen mit dem Vorbehalt, dass Art und Umfang der Datenzusammenführung zum Zeitpunkt der Einwilligung meist völlig unbekannt sind.

Für die betreffenden Datenquellen gibt es in der Regel bereichsspezifische Vorgaben, die die Datennutzung bzw. -weitergabe an eine Genehmigung oder zumindest Kenntnisnahme durch Ministerien oder Datenschutzbehörden knüpfen.[918] Die daraus resultierenden **administrativen Anforderungen** bedeuten einen hohen Aufwand für die Forscher und führen wegen rechtlicher Unwägbarkeiten leicht zu Verunsicherungen.[919] Bisweilen können sich einschlägige Regelungen oder deren Auslegung durch Aufsichtsbehörden auf unterschiedlichen Ebenen widersprechen (z.B. bei Forschungsprojekten, für die zugleich Bundes- und Landesgesetze anwendbar sind),[920] was Forscher dazu bringt, unabsichtlich und oft unwissentlich gegen rechtliche Vorgaben zu verstoßen.[921]

Über die Erfüllung der datenschutzrechtlichen Vorgaben hinaus müssen bei vielen medizinischen Forschungsvorhaben entsprechend § 15 MBOÄ auch **Ethikkommissionen** einbezogen werden. Dauer und Ergebnis der damit verbundenen Beratungs- und Genehmigungsprozesse sind oftmals schwer einschätzbar. Außerdem kommt es in vielen Belangen zur Doppelung von Aufgaben und Infrastrukturen, da ethische und datenschutzrechtliche Erwägungen teilweise identische Schutzziele verfolgen (Würdeschutz, Persönlichkeitsschutz, sonstiger Grundrechtsschutz). Beide Verfahren fordern letztlich eine Abwägung von Forschungsinteressen und Betroffeneninteressen; sie unterscheiden sich insbesondere in der Zusammensetzung des „Spruchkörpers" und der dort präsenten Expertise.[922]

Das neue BDSG und die neuen Landesdatenschutzgesetze schaffen **weder Rechtssicherheit noch Rechtsklarheit**, da der Flickenteppich von Regelungen zur Forschungsdatenverarbeitung mitsamt dem bereichsspezifischen Recht fortbesteht.[923] Die Zweigleisigkeit des Datenschutzes zwischen SGB und sonstigem Recht verstärkt die Verunsicherung und legt zugleich eine Anpassung nahe.[924] Gemäß Art. 9 Abs. 3

916 Datenethikkommission, 75; Deutscher Ethikrat, 11ff. (Thesen 15–17, 19, 74), 60ff.; GMDS, 5.
917 GMDS, 10.
918 Z.B. § 75 Abs. 4 SGB X, § 27a Abs. 2 ThürKHG.
919 Dierks 2019, 62ff.
920 So die Begründung zu § 287a SGB V des „Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" v. 24.03.2020, BT-Drs. 19/18111, 27; Graf von Kielmansegg in TMF, 116.
921 Dierks 2019, 86f.
922 Graf von Kielmansegg in TMF, 117f.
923 Datenethikkommission, 125; Graf von Kielmansegg in TMF, 104.
924 Zum Novellierungsdarf im SGB Thüsing/Rombey NZS 2019, 205.

DSGVO bleibt das nationale Recht zu Berufsgeheimnissen erhalten, was getreu dem in Deutschland bestehenden Zwei-Schranken-Prinzip bedeutet, dass die Weiterverarbeitung von Berufsgeheimnissen (wie etwa des Patientengeheimnisses) durch Dritte neben der datenschutzrechtlichen Erlaubnis eine zusätzliche Offenbarungsbefugnis verlangt. Die völlig offen formulierten Regelungen, etwa in § 27 BDSG, können diesbezüglich nicht zufriedenstellen.

Die fehlende Rechtssicherheit betrifft auch die Frage, welche Forschungsprojekte überhaupt in den Genuss der in der DSGVO und in nationalstaatlichen Regelungen vorgesehenen Privilegierungen kommen können. Es fehlt an einer klaren materiellen **Definition privilegierter Forschung**. Zudem fehlt es an einem Verfahren, durch das die Voraussetzungen für die Privilegierung verbindlich festgestellt werden können. Selbst der jüngste Vorstoß der Bundespolitik, die medizinische Forschung durch neue Regelungen zum Transparenzregister (§§ 303a SGB V) zu stärken, hat dieses Problem nicht aufgegriffen.[925]

Die bestehende Rechtsunsicherheit könnte auf der **Grundlage der DSGVO** beseitigt werden. Kritisch zu bewerten sind dagegen Vorschläge des Deutschen Ethikrates, die unter dem Stichwort der „Datensouveränität" eine Abkehr von den Grundsätzen der Zweckbindung und der Datenminimierung propagieren.[926] Mit der DSGVO wurde ein supranationaler Rechtsrahmen geschaffen, in dem Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) weiterhin einen hohen Schutz genießen (Art. 9 DSGVO). Die DSGVO anerkennt aber auch das hohe öffentliche Interesse an der Weiterverarbeitung zu Forschungszwecken und erklärt deshalb diese nicht länger als unvereinbar mit dem ursprünglichen Erhebungszweck (Art. 5 Abs. 1 lit. b DSGVO). Eine wissenschaftliche Verarbeitung personenbezogener Gesundheitsdaten ist zulässig, wenn *„angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person"* bestehen (Art. 9 Abs. 2 lit. j, 89 DSGVO). Leider wurde die Hoffnung auf eine Vereinheitlichung und Modernisierung der Datenschutzregelungen in Deutschland zur medizinischen Forschung dadurch getrübt, dass die Gesetzgeber die bisher gültigen Regelungen nur unwesentlich geändert haben.[927]

14.2 Nationaler Regelungsvorschlag

Diese Defizite veranlassten den Autor und den Medizininformatiker Michael Krawzcak, zunächst in einem engen Kreis von Kollegen aus den Bereichen Medizinforschung und Datenschutz eine Diskussion über den rechtlichen Reformbedarf zu führen. Die Ergebnisse wurden in ein **Handlungskonzept** überführt und bundesweit an 50 einschlägige Adressaten aus einer ausgewählten Fachöffentlichkeit von Medizinforschern (u.a. Rat für Informationsinfrastruktur, Wissenschaftsrat, Deutsches Netzwerk Versorgungsforschung), Medizinfachverbänden (u.a. Bundesärztekammer), Datenschützern (u.a. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Gesellschaft für Datenschutz und Datensicherheit), Verbraucherschützern (u.a. Verbraucherzentrale Bundesverband), Verwaltung (zuständige Bundesministe-

925 Digitale-Versorgung-Gesetz v. 09.12.2019, BGBl. S. 2562; Riechert DANA 2019, 211f.; Weichert DANA 2020, 25; ders. MedR 2020, 539ff.; Schulz SGb 2020, 536ff.; Bretthauer/Spiecker, JZ 2020, 990ff.

926 Deutscher Ethikrat, u.a. 22f.; kritisch und richtig dazu Kühling DuD 2020, 182ff.

927 Weichert/Krawczak MIBE 2019, Vol. 15(1), 3/8.

rien) und Politikern (Bundestagsfraktionen) zur Stellungnahme übermittelt. Auf Grundlage der Rückmeldungen wurde das Konzept modifiziert und anschließend zur allgemeinen politischen Diskussion gestellt.[928] Das überarbeitete Konzept war u.a. Gegenstand einer Diskussion beim „Round Table Nutzung von Gesundheitsdaten zu Forschungszwecken unter der EU-Datenschutz-Grundverordnung (DSGVO)", der am 03.07.2018 vom Bundesministerium für Wirtschaft und Energie mit über hundert Teilnehmenden – unter anderem aus den zuständigen Bundesministerien, vielen Landesministerien, der Wirtschaft (Pharma, Medizinprodukte- und Medizininformationsdienstleister), der medizinischen Versorgung und Forschung (u.a. TMF), Datenschutzbehörden und weiteren Institutionen aus der Fachöffentlichkeit – durchgeführt wurde.[929]

Die im Folgenden vorgestellten Regelungsvorschläge beruhen auf der Grundlage der bisher geführten Diskussion. Sie verfolgen das Ziel, den Vertraulichkeits- und Persönlichkeitsschutz von Patienten und Probanden in der medizinischen Forschung zu gewährleisten und gleichzeitig sicherzustellen, dass das wissenschaftliche Potenzial existierender Datenbestände so weit wie möglich ausgeschöpft wird. Dabei sind folgende **grundsätzliche Erwägungen** anzustellen:

Moderne Forschung ist immer mehr darauf angewiesen, räumlich und zeitlich auseinanderliegende Datenquellen mit unterschiedlicher Zweckbindung für eine gemeinsame Analyse zusammenzuführen.[930]

- Zur Sicherung der guten wissenschaftlichen Praxis müssen Forschungsergebnisse unabhängig nachvollziehbar sein, was wiederum die Aufbewahrung der diesen Ergebnissen zugrunde liegenden Daten in möglichst unverändertem Zustand voraussetzt.
- Angesichts der dynamischen Entwicklung von Erzeugung, Erfassung und Auswertung medizinischer Forschungsdaten sind die faktischen Möglichkeiten einer Anonymisierung zunehmend begrenzt.

Es bestehen heute technische Möglichkeiten (asymmetrische Kryptografie, homomorphe Verschlüsselung), die Verarbeitung von Forschungsdaten auf bestimmte Stellen und Zwecke zu begrenzen und so deren Vertraulichkeit zu wahren.[931]

Die Rechtszersplitterung in Deutschland sollte zugunsten eines möglichst **einheitlichen Regelungsregimes** beendet werden.[932] Bei dieser länderübergreifenden Harmonisierung kann eine gestaffelte Melde- und Genehmigungspflicht für die Verarbeitung personenbezogener Forschungsdaten vorgesehen werden. Dadurch sollen gesetzliche Rahmenbedingungen geschaffen werden, mit denen die Einwilligung der Betroffenen als erforderliche Rechtsgrundlage ersetzt wird.[933]

Allerdings folgt die Gesetzgebungsbefugnis im Bereich der Forschung den jeweils zu regelnden Rechtsbereichen und den Zuständigkeiten für die tätigen Einrichtungen. Sie liegt daher sowohl beim Bund als auch bei den Ländern (s.o. Kap. 2.4). Wegen der

928 Krawczak/Weichert DANA 2017, 194f.
929 Weichert/Krawczak MIBE 2019, Vol. 15(1), 2/8.
930 RfII, 4.
931 Weichert/Krawczak MIBE 2019, Vol. 15(1), 5/8; Krawczak/Weichert DANA 2017, 198.
932 RfII, 10; GMDS, 3.
933 Datenethikkommission, 139 (These 17).

im Grundgesetz festgeschriebenen geteilten Gesetzgebungskompetenzen kann eine einheitliche Regulierung durch einen **Bund-Länder-Staatsvertrag** erfolgen.[934]

Eine bundesweit einheitlich geltende Regelung für den Bereich der medizinischen Forschung ließe sich in der Praxis leichter durch eine **Grundgesetzänderung** erreichen. Darin sollte dann festgelegt werden, dass der Bereich des Datenschutzes in der medizinischen Forschung oder gar der Forschung generell in die (konkurrierende) Gesetzgebungskompetenz des Bundes übertragen wird.[935] Zwar kann man die Ansicht vertreten, dass eine solche Gesetzgebungskompetenz schon durch die bestehenden Regelungen abgedeckt sei. Insbesondere Art. 74 Abs. 1 Nr. 13 GG, der die „Förderung der wissenschaftlichen Forschung" dem Bundesgesetzgeber zuspricht, ließe sich nutzbar machen.[936] Angesichts des Umstandes, dass es derzeit aber eine Vielzahl von Landesgesetzen gibt, die medizinische Forschung regeln, ist es zweifelhaft, dass die Bundesländer eine solche Zentralisierung der Normsetzungszuständigkeit ohne eine explizite Änderung des GG akzeptieren werden.

Erstrebenswert wäre darüber hinausgehend ein bundesweit geltendes **Gesundheitsdatenschutzgesetz**.[937] Angesichts der Komplexität einer solchen Materie ist – zunächst – die Verwirklichung eines Medizinforschungsgesetzes realistischer. Angesichts der hohen Hürden für die Realisierung eines Bund-Länder-Staatsvertrags wird auch vorgeschlagen, ein Medizinisches Forschungsdatengesetz oder ein Gesundheitsdatennutzungsgesetz auf Bundesebene zu erlassen, dem sich die Bundesländer über Verweisungen anschließen können.[938]

Ein möglicher Ansatz für eine Harmonisierung besteht darin, dass auf Bundesebene keine umfassenden Regelungen erlassen werden, sondern lediglich **regulatorische Festlegungen**, etwa zur Federführung bei der Datenschutzaufsicht.[939] Hierdurch werden jedoch nur einige Symptome der Rechtszersplitterung angegangen und keine praktische Vereinheitlichung erreicht.

Einen Weg zu einer untergesetzlichen Harmonisierung des Datenschutzes bei der medizinischen Forschung eröffnen die Art. 40, 41 DSGVO. Danach können Verbände oder andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, **Verhaltensregeln** ausarbeiten, mit denen eine Präzisierung der Regeln zur Verarbeitung personenbezogener Daten sowie des Umgangs damit festgelegt wird (Art. 40 Abs. 2 DSGVO).[940] Der Vorteil solcher Regeln liegt darin, dass es für ihre Ausarbeitung keines aufwändigen Gesetzgebungsverfahrens bedarf. Deren Inhalt wird zwischen den beteiligten Stellen und den Datenschutzbehörden – auf der Grundlage der bestehenden Gesetze – ausgehandelt. Über solche Regeln können auch Stellen in Drittländern ohne angemessenes Datenschutzniveau einbezogen werden

934 Weichert/Krawczak MIBE 2019, Vol. 15(1), 6/8; Krawczak/Weichert DANA 2017, 199; ebenso Weichert in Steckler, Einzelaspekte rechtswissenschaftlicher Begleitforschung für Projekte der Mensch-Technik-Interaktion, 2019, 218ff.; kritisch bzgl. der praktischen Realisierbarkeit Dierks 2019, 89; Schneider, 344, schlägt eine Mustergesetzgebung vor, dazu Dierks 2019, 89f.

935 Kingreen/Kühling in Kingreen/Kühling, 468ff.; Dierks 2019, 103f.; vgl. Graf von Kielmansegg in TMF, 122f.

936 Dierks 2019, 90–100.

937 Dierks 2019, 112; Kingreen/Kühling in Kingreen/Kühling, 468ff.

938 Netzwerk Datenschutzexpertise; Sachverständigenrat, S. XXVIII; ähnlich Graf von Kielmansegg in TMF, 121.

939 Dierks 2019, 100–103; dem folgend, aber unsystematisch im SGB eingeordnet jetzt § 287a SGB V; dazu Sachverständigenrat 203; Schäfer in Kipker/Voskamp, 350ff.

940 Dierks 2019, 104ff.

(Art. 40 Abs. 3 DSGVO, s.o. Kap. 13.2). Die Reichweite solcher Verhaltensregeln ist skalierbar.[941] Gesetzliche Vorgaben können mit Verhaltensregeln nicht abbedungen werden. Wohl aber können darüber Verfahren für den Umgang mit Normenkollisionen festgelegt werden. Vorlageberechtigt sind Vereinigungen von Daten verarbeitenden Stellen.[942] Insofern kommt auch die TMF als „Normgeber" in Betracht. Verhaltensregeln können für die erfassten Stellen verbindliche Vorgaben machen, die gemäß Art. 41 DSGVO überwacht werden. Sie bedürfen für ihre Verbindlichkeit der Genehmigung durch die zuständige Aufsichtsbehörde (Art. 40 Abs. 5 DSGVO). Verhaltensregeln könnten letztlich als Vorlage für spätere verbindliche gesetzliche Festlegungen dienen.

Bei der Schaffung einer einheitlichen materiellen Regulierung der Datennutzung für die medizinische Forschung kann auf die **Grundsätze bestehender Forschungsklauseln** zurückgegriffen werden, die sich in der Vergangenheit weitgehend bewährt haben.

- Soweit möglich, sind Daten für Forschungszwecke zu anonymisieren; ansonsten ist eine Pseudonymisierung vorzunehmen. Besteht später Bedarf an einer identifizierenden Zuordnung pseudonymer Datensätze, so kann über eine File-Trennung und eine unabhängige Vertrauensstelle gewährleistet werden, dass keine ungewollten Identifizierungen pseudonymisierter Datensätze erfolgen.
- Eine Verarbeitung personenbeziehbarer Forschungsdaten ist nur zulässig, wenn alle einschlägigen Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nichtverkettbarkeit) in angemessener Weise durch technisch-organisatorische Maßnahmen gewährleistet werden.
- Eine Verarbeitung ist zulässig, wenn sie auf einer ausdrücklichen, informierten, freiwilligen und widerrufbaren Einwilligung basiert. Die in der DSGVO enthaltenen Vorgaben ermöglichen Präzisierungen für die medizinische Forschung.
- Eine Verarbeitung kann auch ohne Einwilligung der Betroffenen zulässig sein, wenn ein öffentliches Interesse am jeweiligen Forschungsvorhaben besteht und der Schutz der Betroffenen gewährleistet werden kann.
- Personenbezogene Daten dürfen nicht veröffentlicht werden, es sei denn, die betroffene Person hat eingewilligt oder dies ist für die Darstellung der Forschungsergebnisse unerlässlich.

Die datenschutzrechtlichen Betroffenenrechte müssen stets so weit wie möglich gewährleistet werden.[943]

Forschung mit Berufsgeheimnissen, also insbesondere mit Patientengeheimnissen, erfordert wegen des **Zwei-Schranken-Prinzips** in Deutschland neben der Beachtung allgemeiner Datenschutzregelungen auch die Einhaltung der rechtlichen Anforderungen an die Verarbeitung von Berufsgeheimnissen. Diese Rechtslage sollte dahingehend geändert werden, dass an der Forschung Beteiligte unter bestimmten Bedingungen in einen an § 203 StGB orientierten Geheimnisschutz einbezogen werden. Ein gesetzliches Forschungsgeheimnis sollte ein Zeugnisverweigerungsrecht und

941 Weichert in DWWS, Art. 40 Rn. 17.
942 Dierks 2019, 109.
943 Weichert/Krawczak MIBE 2019, Vol. 15(1), 5/8.

Beschlagnahmeverbot mit einschließen.[944] Bei der Festlegung der Bedingungen sind Genehmigungen oder Zertifikate denkbar.[945]

Neben technisch-organisatorischen und rechtlichen Regelungen gibt es in den bestehenden Forschungsklauseln prozedurale Vorkehrungen wie z.B. **Genehmigungsvorbehalte und Meldepflichten**. Diese haben sich in der Praxis oft nicht bewährt. Der Prüfaufwand der beteiligten Stellen (Ministerien, Datenschutzaufsichtsbehörden, Ethikkommissionen) kann mit den vorhandenen Ressourcen nicht oder nur eingeschränkt erbracht werden.

Im Interesse der Entbürokratisierung und Vereinfachung wird demgegenüber ein Verfahren angeregt, in das technisch-organisatorische, datenschutzrechtliche, ethische und fachliche Erwägungen einfließen können, indem die erforderliche Expertise in unabhängigen, lokal agierenden Gremien (englisch: **Use and Access Committees**, UAC) im Sinne eines „One-Stop-Shopping" gebündelt wird. Damit wird dem Bedürfnis Rechnung getragen, dass die Überprüfung der rechtlichen Zulässigkeit auf eine institutionelle Instanz übertragen wird, die sowohl die Sichtweise der Wissenschaft wie auch die der Beforschten bzw. des Datenschutzes berücksichtigt.[946] Diesen UACs werden in Abhängigkeit von der Sensitivität des jeweiligen Forschungsvorhabens Genehmigungs- bzw. Vetorechte für die Nutzung personenbezogener Gesundheitsdaten per Gesetz übertragen, sie erhalten also eine hoheitliche Funktion. In den UACs muss fachlicher, ethischer und datenschutzrechtlicher Sachverstand vertreten sein.

Das Verhältnis der UACs zu den Ethikkommissionen und Datenschutzaufsichtsbehörden sollte unter Einräumung eines gegenseitigen Konsultationsrechts so geregelt werden, dass eine Kollision ihrer datenschutz- und berufsrechtlichen Compliance-, Kontroll- und Beratungspflichten weitestgehend vermieden und eine Entlastung der Beteiligten erreicht wird. Die **Zuständigkeit eines UAC** für ein bestimmtes Forschungsprojekt könnte sich aus der geographischen oder organisatorischen Zugehörigkeit des jeweils Projektverantwortlichen ergeben. Vorbild hierfür könnte die in der DSGVO verankerte Regelung zur Zuständigkeit der Aufsichtsbehörden sein, die sich an der Hauptniederlassung eines Verantwortlichen orientiert (Art. 56 Abs. 1 DSGVO).[947]

Während die organisatorischen und administrativen Verfahren der UACs gesetzlich zu regeln sind, sollten die Kriterien für die Bewertung von Forschungsvorhaben im Rahmen einer „**regulierten Selbstregulierung**" durch Einrichtungen wie z.B. die TMF entwickelt werden. Die resultierenden Standards könnten im Konsens der betroffenen Fach-Communities auch als verbindlicher und rechtssicherer Rahmen für die Konzipierung und Zulassung von Forschungsvorhaben dienen.[948] Bei diesen Standards können Treuhänderlösungen einen wesentlichen Beitrag leisten (s.o. Kap. 10.4).

944 GMDS, 7; Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 7. Aufl. 2020, Rn. 523-525.
945 Krawczak/Weichert DANA 2017, 198.
946 Sachverständigenrat, 234, 327 (Rn. 761); RfII, 13; Graf von Kielmansegg in TMF, 121f.; tendenziell ebenso Deutscher Ethikrat, 183 (D2.1); Platzer NSZ 2020, 94; Dierks 2020, 11ff.; zur ethischen Bewertung Strech in TMF, 72ff.
947 Krawczak/Weichert, DANA 2017, 199.
948 RfII, 14; generell dazu Datenethikkommission, 29 (These 58), 201ff.; Weichert 2018, Kap. 8.22; Health Ethics Policy Lab, 72ff.

Ein wichtiger Baustein kann auch in der Zertifizierung von Einzellösungen, in standardisierten Prozessen und in der Erarbeitung von Verhaltensregeln (Codes of Conduct) liegen (vgl. Art. 42, 43 DSGVO).[949]

Derzeit gibt es im Kontext der Verarbeitung von personenbezogenen Daten für medizinische Forschungszwecke keine demokratische Kontrolle; den entsprechenden Verfahren fehlt **systematische Transparenz** (s.o. Kap. 3.4). Bei einer (teilweisen) Bündelung der bisherigen Aufgaben von Ministerien, Aufsichtsbehörden und Ethikkommissionen in eigens dafür eingerichteten und untereinander vernetzten UACs ließe sich dieser Missstand durch den Betrieb eines öffentlich einsehbaren Forschungsregisters beheben, an das die UAC wesentliche Informationen zu den von ihnen freigegebenen Forschungsprojekten weitergeben. Dieses Register wäre im Interesse eines wissenschaftlichen Dialogs eine Informationsgrundlage für andere Forschende. Es könnte zudem den von den Forschungsprojekten Betroffenen einen Überblick über die Forschung mit ihren Daten, die dafür jeweils Verantwortlichen, ihre Ziele und Fragestellungen sowie die in der Forschung ergriffenen grundrechtsschützenden Maßnahmen erlauben. Nicht zuletzt könnte damit auch der immer wieder erhobenen Forderung nach stärkerer Teilhabe der Patienten und Probanden und der Möglichkeit für diese, Widerspruch einzulegen, Rechnung getragen werden.[950]

Die den Forschenden abzuverlangende Transparenz sollte gesetzlich **möglichst präzise so festgelegt** werden, dass einerseits die wissenschaftliche Nutzung der personenbezogenen Daten hinreichend nachvollziehbar und überprüfbar ist, dass andererseits den Forschenden der größtmögliche wissenschaftliche Freiraum bewahrt wird. Bezüglich des Forschungszweckes erscheint eine Offenlegung der Fragestellung, der eingesetzten Methoden und Verfahren und der damit verbundenen Datenverarbeitung (Forschungs- bzw. Datenschutzkonzept) gegenüber einem gesetzlich legitimierten Gremium, etwa dem UAC, ausreichend, das die Befugnis zur Bewertung und zur Genehmigung des Projektes hat.

Wird ein Forschungsprojekt nicht auf Einwilligungsbasis durchgeführt, so sollte mit der Antragstellung im Interesse der Transparenz gegenüber Betroffenen in allgemeiner Form eine Veröffentlichung, z.B. über ein **Internetportal**, zur Pflicht gemacht werden.[951] Wurde ein entsprechendes Vorhaben zugelassen und begonnen, so ist dies öffentlich zu vermerken. Dabei sollte auch erkennbar gemacht werden, für wann der Abschluss des Projektes geplant ist; bei langfristigen Forschungsprojekten können auch Angaben zu beabsichtigten Zwischenzielen sinnvoll sein. Nach Abschluss eines Projektes sollte nach einer bestimmten Frist eine allgemeine Veröffentlichung der Ergebnisse zur Pflicht gemacht werden. Insofern erscheint eine Frist von einem Jahr nach Projektabschluss angemessen.

Durch eine **bundesweit einheitliche Regelung** könnten die bisherigen, teilweise verstreuten und widersprüchlichen Bundes- und Länderregelungen zur medizinischen Forschung ersatzlos wegfallen. Darin müssten die materiell-rechtlichen und prozeduralen Voraussetzungen für die Zulässigkeit medizinischer Forschungsvorhaben normiert werden – einschließlich eventueller Einwilligungserfordernisse, der

949 EDPS 2020, 25f.; RfII, 15, 19, 23.
950 Datenethikkommission, 126; Krawczak/Semler/Zenke/Strech/Graf von Kielmansegg in TMF, 132.
951 Ähnlich für Forschungsprojekte auf der Basis des Forschungsdatenzentrums § 303d Abs. 1 Nr. 6 SGB V.

Verfahren der UACs, der Einbindung von Ethikkommissionen und Datenschutzaufsicht sowie der Transparenzverpflichtungen gegenüber der Öffentlichkeit.

Die Anregung zur Einrichtung unabhängiger UACs für medizinische Forschungsdaten basiert neben inhaltlichen Erwägungen auch auf der Notwendigkeit, Doppelentwicklungen und Parallelstrukturen in diesem wichtigen und sensiblen Bereich zu vermeiden. Seit Juli 2017 fördert das Bundesministerium für Bildung und Forschung (BMBF) umfänglich die **Medizininformatik-Initiative**, in der deutsche Universitätskliniken gemeinsam mit externen Partnern sogenannte „Datenintegrationszentren" (DIZ) zum standortübergreifenden Managen und Teilen medizinischer Daten aufbauen. Die geförderten Konsortien sehen in ihren Konzepten in der einen oder anderen Weise Mechanismen vor, um den Zugang zu den zu teilenden Daten formal auszugestalten.[952] Die Etablierung solcher Verfahren wird voraussichtlich zentral für die Funktionsfähigkeit der DIZ sein. Aus der Medizininformatik-Initiative können umfassendere Verfahren entwickelt und etabliert werden.[953]

Welche Forschungsprojekte unabhängig vom Datenzugang **melde- bzw. genehmigungspflichtig** sein sollen bzw. können, bedarf der weiteren fachlichen Erörterung. Maßgebliches Kriterium soll dabei das mit dem jeweiligen Projekt verbundene Datenschutzrisiko sein.

- Auf eine Meldung und Registrierung kann verzichtet werden, wenn klassische Eigenforschung erfolgt oder die Forschungsdatenverarbeitung auf einer informierten Einwilligung der Betroffenen basiert.
- Melde- und registrierungspflichtig sollten Projekte sein, bei denen eine Interessenabwägung die informierte Betroffeneneinwilligung ganz oder teilweise ersetzen soll, was impliziert, dass die UACs bei solchen Projekten neben Aufklärungs- auch Untersagungsrechte haben müssen.
- Zusätzlich zur bestehenden Meldepflicht sollten Projekte genehmigungspflichtig sein, wenn in ihnen hochsensitive Daten verarbeitet werden, wie dies z.B. bei umfangreichen Gensequenzierungen der Fall ist, oder wenn weiterreichende Zweckänderungen beabsichtigt sind. Auch zeitlich unbegrenzte Studien bzw. Forschungsdatenbanken sollten unter Genehmigungsvorbehalt gestellt werden.

Für ethisch oder technisch **besonders anspruchsvolle Projekte** wie z.B. internationale Studien, Forschungsnetzwerke, Krankheitsregister oder Biomaterialdatenbanken könnten vom zuständigen UAC bei Bedarf zusätzliche Anforderungen festgelegt und zur Genehmigungsgrundlage gemacht werden.[954]

Das vorgeschlagene Regelungsverfahren trägt zu einer Optimierung des Datenschutzes bei medizinischen Forschungsprojekten bei und erleichtert und verbessert zugleich die Forschungspraxis. Die Umsetzung des Konzepts ist nicht vom Schreibtisch aus möglich. Vielmehr ist hierfür eine umfassende Fortführung des begonnenen **Diskussions- und Abstimmungsprozesses** unter Einbindung aller Betroffenen erforderlich. Die genaue Ausgestaltung der UACs muss auf den in der Vergangenheit

952 Der Bayerische Landesbeauftragte für den Datenschutz, 28. TB, 2017/2018, 108ff.; Zenker/Krawczak/Sempler in TMF, 43ff.

953 Netzwerk Datenschutzexpertise, 7f.; generell zur Initiative Sachverständigenrat, 37f., 211.

954 Weichert/Krawczak MIBE 2019, Vol. 15(1), 7 u. 8; Weichert ZD 2020, 23f.

gemachten Erfahrungen basieren und einem strukturierten Prozess folgen, an dessen Ende eine gesetzliche Festlegung stehen sollte. Wie vom Rat für InformationsInfrastrukturen (RfII) und jüngst vom Sachverständigenrat gefordert, sollte dieser Entwicklungsprozess Hand in Hand mit dem Aufbau einer netzwerkförmigen Nationalen Forschungsdateninfrastruktur (NFDI) erfolgen.[955]

14.3 Europäische Reformmöglichkeiten

Angesichts der zunehmenden Europäisierung der Forschung generell wie der medizinischen Forschung speziell und dem damit verbundenen Austausch personenbeziehbarer Informationen innerhalb der EU und mit Projekten außerhalb der EU wäre nicht nur eine einheitliche nationale Regulierung der Forschungsdatenverarbeitung wünschenswert, sondern darüber hinausgehend eine verbindliche **europäische Regelung**.[956]

Zwar besitzt die EU keine **Regelungskompetenz** im Hinblick auf Forschungsfragen generell. Hinsichtlich der Normierung der personenbezogenen Datenverarbeitung für Forschungsprojekte sowie der Verarbeitung in solchen Projekten hat die Union über Art. 16 Abs. 2 AEUV aber eine umfassende Zuständigkeit (s.o. Kap. 2.3). Gegen eine unionsweite Regulierung kann der Subsidiaritätsgrundsatz (Art. 5 EUV) schwerlich in Stellung gebracht werden. Eine nationale bzw. regionale Differenzierungsmöglichkeit besteht im Hinblick auf die Anforderungen an einen europäischen „Forschungsbinnenmarkt" nicht.

Dies gilt insbesondere für die **medizinische Forschung**, zumal die zu beantwortenden Forschungsfragen von nationalen Grenzen weitestgehend unabhängig sind. Möglich wäre eine umfassende europäische Regulierung des Datenschutzes im Rahmen der wissenschaftlichen Forschung. Möglich wäre aber auch eine Beschränkung auf die medizinische Forschung: Zwar bestehen zwischen der medizinischen Forschung und anderen Forschungsbereichen, etwa im Bereich der Umwelt- und der Sozialwissenschaft, Wechselbeziehungen und disziplinübergreifende Ansätze. Doch ist die personenbezogene Datenverarbeitung in der medizinischen Forschung, einschließlich der wissenschaftlichen Behandlung der Biotechnik, ein Sektor, der weitgehend separat reguliert werden kann und derzeit im Hinblick auf spezifische Anwendungen auch auf nationaler Ebene quellenbezogen separat geregelt ist.

Als Grundlage für eine europäische Harmonisierung der Regelungen zur (medizinischen) Forschung mit personenbezogenen Daten genügt die **DSGVO mit ihrer Privilegierung** von Forschungszwecken und dem Erfordernis kompensierender Garantien für die Betroffenen. Die einschlägigen Öffnungsklauseln, etwa in Art. 6 Abs. 3 u. 4, 9 Abs. 2 lit. j, 23, 89 Abs. 2 u. 3 DSGVO, eröffnen nicht nur den Mitgliedstaaten, sondern auch der Union selbst die Befugnis zur Konkretisierung der allgemeinen Vorgaben in der DSGVO. Eine Harmonisierung auf Unionsebene hätte zudem den Effekt, dass verbindliche Regelungen für Deutschland auf Bundes- wie auf Landesebene

955 RfII, 15ff.; Deutscher Ethikrat, 174 (A1); Sachverständigenrat, 231ff.; generell zum Aufbau von Dateninfrastrukturen Datenethikkommission, 143.

956 Datenethikkommission, 32, 125, 139 (These 17), 226ff.; Platzer NZS 2020, 295; Weichert ZD 2020, 18; Martini/Hohmann NJW 2020, 3578; ausführlich Dierks 2020, 5ff.

geschaffen würden, da das EU-Recht dem Recht auf beiden Ebenen vorgeht. Dies hätte den Vorteil, dass das derzeit auf nationaler Ebene bestehende Problem unterschiedlicher Gesetzgebungskompetenzen (s.o. Kap. 2.4, Kap. 14.1) keine Rolle spielen würde. Die ungenügende Umsetzung der Vorgaben der DSGVO (s.o. Kap. 14.1) im Bereich der Forschung würde überregelt. Die unübersichtliche Annexregulierung der Forschung in vielen unterschiedlichen Normtexten ließe sich überwinden (s.o. Kap. 2.4). Die Zweigleisigkeit der nationalen Regelung mit dem Datenschutzrecht und dem Berufsgeheimnisrecht (s.o. Kap. 6, Kap. 14.1) könnte zusammengeführt werden.

Als Regelungsinstrument bietet sich eine **Verordnung** an. Eine Richtlinie, die wieder in nationales Recht umzusetzen wäre, hätte nicht die wünschenswerte Harmonisierungswirkung. Als Übergangsregelung wäre ein Code of Conduct (Verhaltensregeln) gemäß Art. 40 DSGVO denkbar.[957] Das Problem solcher Verhaltensregeln bestünde darin, dass sie sich zwangsläufig in Widerspruch setzen müssten zu bestehenden nationalen gesetzlichen Regelungen, die in der Normhierarchie über Verhaltensregeln anzusiedeln sind.[958] Rechtfertigen ließe sich ein solches Vorgehen allenfalls damit, dass diese Verhaltensregeln Vorgaben zu einer DSGVO-konformen Umsetzung des bestehenden Rechts machen. Für nationale Sonderwege sind keine Notwendigkeiten erkennbar. Sollten sich diese in der weiteren Diskussion ergeben, kann man, dem Vorbild der DSGVO folgend, über Öffnungsklauseln eng beschränkte Regelungsspielräume schaffen.

Bezüglich des **Regelungsinhaltes** kann weitgehend auf die Ausführungen unter Kapitel 14.2 verwiesen werden. Die gemeinsamen Grundannahmen bestehen für die gesamte Union mit der Grundrechte-Charta; diese Grundrechte entsprechen denen des deutschen Verfassungsrechts. Zudem bestehen internationale Standards, an die angeknüpft werden kann (s.o. Kap. 7.2). Soweit erkennbar, bestehen hinsichtlich der Grundannahmen zwischen den Rechtsordnungen innerhalb der EU keine wesentlichen Unterschiede. Inwieweit nationale Besonderheiten bestehen, muss eventuell durch Studien im Detail abgeklärt werden. Der Umstand, dass sich über die Forschungsförderung der EU in der Gemeinschaft der Forschenden schon gemeinsame Standards entwickelt haben, ist für die Konkretisierung der Forschungsdatenverarbeitung förderlich.

Politische Initiativen zur Harmonisierung des Datenschutzrechts bei der Forschung sind bisher nicht erkennbar. Es ist aber auch nicht ersichtlich, dass nationale oder interessenspezifische Interessen einer solchen Harmonisierung im Wege stehen. Die Chancen für die Entwicklung eines einheitlichen Forschungsraumes in der EU für Wissenschaft, Politik und Wirtschaft dürften allen Beteiligten einleuchten.

957 s. hierzu den umfassenden Vorschlag von Dierks 2020, 31ff., mit dem Titel „Europäischer Schutzraum für Forschungsdaten".

958 Dierks 2020, 35.

14.4 Fazit: Novellierungsbedarf

Der Wissenschaftsstandort Deutschland leidet im internationalen Wettbewerb seit Jahren unter dem Fehlen einheitlicher gesetzlicher Rahmenbedingungen, die ein **zukunftsgerichtetes Forschen mit Gesundheitsdaten** unter gleichzeitiger Wahrung der Grundrechte der betroffenen Menschen ermöglichen. Dadurch ergeben sich Nachteile für die wirtschaftliche Entwicklung, den gesellschaftlichen Fortschritt und den Grundrechtsschutz der Menschen. Durch die Vorschläge zur Regulierung und durch den parallelen Aufbau einer entsprechenden Infrastruktur könnte diese Blockade aufgelöst werden. Im föderalen Deutschland gesammelte Erfahrungen können in dem größeren Rechtsraum der EU sowie darüber hinausgehend international nutzbar gemacht werden.

Ohne eine Vermittlung dieser Anliegen gegenüber der Öffentlichkeit wird es nicht möglich sein, die nötige Einsicht in die Notwendigkeit einer Weiterentwicklung des rechtlichen Rahmens für die medizinische Forschung bei den politisch Verantwortlichen zu schaffen und die nötige Akzeptanz dafür zu gewinnen, dass die sensitiven Daten der Bevölkerung im Interesse des Gemeinwohls beforscht werden.[959] Datenschutz und Forschung sind beides Gemeinwohlanliegen. Grundlage für das Einwirken auf die öffentliche Meinung sollte es sein, dass sich die Gemeinschaft der Forschenden und die der Datenschützer auf gemeinsame Positionen verständigen. Hierzu muss der **Austausch zwischen diesen Beteiligten** intensiviert werden.[960]

959 EDPS 2020, 26.
960 EDPS 2020, 24f.

15 Fragenkatalog des TMF-Rechtsgutachtens aus dem Pflichtenheft

Die ausführliche Begründung der Antworten zu den Fragen im Fragenkatalog finden sich in den mit einem „»»“ angezeigten Kapiteln des obigen Gutachtens.

Rechtsgrundlagen

1. Verhältnis der Rechtsgrundlagen aus Art. 6 und Art. 9 EU-Datenschutzgrundverordnung (im Folgenden: DSGVO):

1.1 Inwiefern stellen die Rechtsgrundlagen in Art. 9 DSGVO eigenständige Rechtsgrundlagen dar oder sind sie immer nur als zusätzliche, einschränkende Anforderungen in Bezug auf eine notwendige (aber eben im Falle der von Art. 9 DSGVO erfassten Daten nicht hinreichende) Rechtsgrundlage nach Art. 6 DSGVO anzusehen?

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten muss ergänzend zu den Erlaubnistatbeständen des Art. 9 Abs. 2 DSGVO ein Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 DSGVO vorliegen. Im Anwendungsbereich der Öffnungsklauseln in Art. 9 Abs. 2 lit. b, g, h, i, j DSGVO erlauben aufgrund dieser Vorschriften erlassene Spezialvorschriften der Union oder der Mitgliedstaaten die Datenverarbeitung. (»» Kap. 4.2–4.5)

1.2 Welche Auswirkungen ergeben sich insbesondere im Hinblick auf das Widerspruchsrecht aus Art. 21 DSGVO für die Forschung, wenn besondere Kategorien personenbezogen Daten (z.B. Gesundheitsdaten) verarbeitet werden, wenn eine Verarbeitung auf Grundlage von Art. 6 Abs. 1e) oder f) erfolgt?

Es macht im Ergebnis keinen Unterschied im Hinblick auf die Behandlung des Widerspruchsrechts, auf welcher rechtlichen Grundlage die Verarbeitung der Daten erfolgt. (»» Kap. 12.7)

2. Kann sich die Rechtsgrundlage im Laufe der Verarbeitung verändern? Kann z.B. bei Widerruf einer Einwilligung ggf. noch eine andere Rechtsgrundlage anzuwenden sein, die eine weitere Verarbeitung erlaubt?

Es kann mehrere Rechtsgrundlagen geben, auf denen eine Datenverarbeitung beruht. Eine Veränderung der Rechtsgrundlagen kann sich dadurch ergeben, dass mit einer Datenverarbeitung zusätzliche andere Zwecke verfolgt werden. Die Berufung auf eine Rechtsgrundlage durch den Verantwortlichen hat für den Betroffenen die Funktion, die Rechtmäßigkeit einer Verarbeitung beurteilen und prüfen zu können. Der Wechsel der Berufung von einer Einwilligung zu einer gesetzlichen Rechtsgrundlage ist nur im Ausnahmefall unter Beachtung des Grundsatzes von Treu und Glauben möglich. Ein Wechsel ist unzulässig, wenn damit die Vertrauenserwartungen des Betroffenen verletzt werden. (»» Kap. 7.3).

2.1 Welche Auswirkungen hat dies auf die Transparenzverpflichtungen (s. Art. 12ff. DSGVO) und hier die notwendige Nennung der Rechtsgrundlage? Muss z.B. in einer Einwilligung explizit auf mögliche ergänzende Rechtsgrundlagen hingewiesen werden?

Soll es schon bei Einholung der Einwilligung möglich sein, die Berufung auf die Rechtsgrundlage zu wechseln, so muss hierauf und auf die Folgen für den Betroffenen hingewiesen werden. Ergibt sich im Nachhinein die Notwendigkeit eines zulässigen Wechsels, so besteht zum frühestmöglichen Zeitpunkt die Notwendigkeit einer Information. (»» Kap. 7.3, Kap. 12.1)

Verantwortlichkeit und Zusammenarbeit

3. Für die Übermittlung von personenbezogenen sowie von personenbeziehbaren Daten bestimmen in der DSGVO die Regelungen zur gemeinsamen Verantwortlichkeit (Art. 26) sowie zur Auftragsverarbeitung (Art. 28) mögliche Rahmenbedingungen neben der Einzelverantwortlichkeit.

3.1 Wie sind die Regelungen zur gemeinsamen Verantwortlichkeit, zur Auftragsverarbeitung und zur Einzelverantwortlichkeit voneinander abzugrenzen?

Die gemeinsame Verantwortlichkeit lässt sich von der Auftragsverarbeitung dadurch abgrenzen, dass die Zwecke nicht allein durch einen Verantwortlichen festgelegt werden und keine verpflichtenden Weisungen ergehen können, sondern eine verbindliche Vereinbarung über die gemeinsamen Verarbeitungsschritte zwischen den verarbeitenden Stellen getroffen werden muss. Eine Einzelverantwortlichkeit besteht, wenn die Zwecke ausschließlich von einer Stelle festgelegt werden. Dies gilt auch bei Verarbeitungsketten, wenn die jeweilige Entscheidung über die Verarbeitung unabhängig ist von der vorangegangenen und folgenden Verarbeitung.

3.2 Welche Regelungsbedarfe sind in den jeweiligen vertraglichen Abreden besonders wichtig oder charakterisieren diese?

Die wesentlichen Inhalte eines Auftragsvertrags werden abschließend in Art. 28 DSGVO Abs. 3 aufgeführt. Mindestinhalte einer Vereinbarung über eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO sind Absprachen über die Behandlung von Betroffenenrechten, die Arbeitsteilung bei den Informationspflichten und die Festlegung der für Verarbeitungsverzeichnis relevanten Informationen gemäß Art. 30 Abs. 1 DSGVO.

3.3 Welche Vor- und Nachteile bieten die drei unterschiedlichen Varianten? Nach welchen Kriterien sollte der passende Regelungsansatz für einen praktischen Anwendungsfall bestimmt oder ausgewählt werden (z.B. in Form einer Checkliste darstellbar)?

Ob eine Einzelverantwortlichkeit oder einer gemeinsame Verantwortung besteht, ist abhängig von der tatsächlichen Verarbeitung. Werden gemeinsame Zwecke verfolgt, so ist die Vereinbarung einer gemeinsamen Verantwortung naheliegend; wenn dabei die Verarbeitungsschritte voneinander abhängig sind und sich ergänzen, ist eine gemeinsame Verantwortung zwingend.

Vorteile der Auftragsverarbeitung: einseitige Festlegung der Zwecke und der Bestimmung der Rechtsgrundlagen, Übertragung der technischen Verarbeitung an einen Dienstleister, Weisungsmöglichkeit durch den Verantwortlichen, klare Trennung der datenschutzrechtlichen Pflichten.

Vorteile der gemeinsamen Verantwortlichkeit: differenziertere Arbeitsteilung, Eigenständigkeit der Beteiligten, Einbeziehung von mehr als zwei nicht hierarchisch eingebundenen Stellen. (»» Kap. 5.2–5.7)

3.4 Müssen ein Datentreuhänder und die juristische Person, die für ein Forschungsvorhaben verantwortlich ist (z.B. Universität), gemeinsam Verantwortliche nach der DSGVO sein oder kann wie bisher auch das Konstrukt der „Funktionsübertragung" genutzt werden?

Es ist naheliegend, bei einer Einschaltung eines Treuhänders eine gemeinsame Verantwortlichkeit zu vereinbaren. Rechtlich möglich ist auch eine Auftragsverarbeitung, mit der aber die Vertraulichkeit der Treuhändertätigkeit beeinträchtigt würde. Eine Funktionsübertragung ist nicht zu empfehlen, da damit die Einbindung in einen gemeinsamen Zweck in Frage gestellt wäre. (»» Kap. 5.9)

3.5 Wie ist im Verhältnis zu diesen Regelungsansätzen das früher mit dem Begriff der „Funktionsübertragung" belegte Konstrukt generell einzuordnen?

Der Begriff der Funktionsübertragung ist entbehrlich. Er eignet sich aber weiterhin zur Abgrenzung von einer Auftragsverarbeitung. (»» Kap. 5.8)

3.6 Führt eine gemeinsame Verantwortlichkeit nach Art. 26 automatisch – wenn keine andere Rechtsform für die Zusammenarbeit gewählt wird (z.B. eingetragener Verein) – zu einer Gesellschaft bürgerlichen Rechts nach deutschem Recht?

Die gemeinsame Verantwortlichkeit begründet bei Fehlen einer anderen Rechtsform nicht automatisch eine Gesellschaft bürgerlichen Rechts. Die Rechtsbeziehung zwischen den Verantwortlichen kann, soweit sie sich nicht auf die Verantwortung für die Verarbeitung bezieht, frei gestaltet werden. (»» Kap. 5.5)

Auswirkung der Neufassung des § 203 StGB auf Forschungsvorhaben

4. In der medizinischen Forschung bestehen häufig Kooperationen zwischen niedergelassenen Ärzten und Forschungseinrichtungen. Wie muss vor diesem Hintergrund ein Anwendungsfall ausgestaltet sein, damit die Mitarbeiter einer Forschungseinrichtung „als sonstige mitwirkende Person" des Arztes im Sinne des § 203 Abs. 3 Satz 2 StGB sind und Daten ohne Verletzung der ärztlichen Schweigepflicht übermittelt werden können?

Mitarbeitende einer Forschungseinrichtung sind dann Mitwirkende eines Arztes, wenn sie diesen in seiner Tätigkeit, die neben seiner Beratungs- und Behandlungstätigkeit auch seine Forschungstätigkeit einschließt, unterstützen und diese Unterstützung erforderlich ist. (»» Kap. 6.6, Kap. 6.8)

4.1 Können die Mitarbeiter einer Forschungseinrichtung als „sonstige mitwirkende Person" i.S.d. § 203 Abs. 3 S. 2 StGB gelten, wenn sie einerseits den Arzt bei seiner Forschungstätigkeit unterstützen, andererseits ergänzend aber auch eigene Forschungsfragestellungen anhand der Daten bearbeiten? Könnte sich die Forschungs-

einrichtung bei der Bearbeitung eigener Fragestellungen auf eine datenschutzrechtlich legitimierte Zweckänderung (z.B. § 27 BDSG) berufen?

Mitarbeiter einer Forschungseinrichtung sind keine Mitwirkenden, soweit sie ausschließlich eigene Forschungsfragestellungen bearbeiten. (»» Kap. 6.6, Kap. 6.8)

4.2 Ist eine Auftragsverarbeitung gemäß Art. 28 DSGVO als datenschutzrechtlicher Rahmen zwingend für eine Mitwirkung einer Forschungseinrichtung bei der forschenden Tätigkeit eines Arztes gemäß § 203 StGB?

Die Einordnung einer Datenverarbeitung als Auftragsverarbeitung, gemeinsame Verantwortlichkeit oder Datenübermittlung spielt für die Auslegung der beruflichen Geheimhaltungsregeln keine Rolle. (»» Kap. 6.7)

Datenschutzkonzept und Datenschutz-Folgenabschätzung

5. Für medizinische Forschungsvorhaben, die mit sensiblen, personenbeziehbaren Gesundheitsdaten operieren, wird die Entwicklung und Abstimmung eines Datenschutzkonzepts empfohlen. Typischerweise enthalten solche Konzepte die Darstellung der Zwecke und Rechtsgrundlagen der Verarbeitung, die Regelung der Verantwortlichkeit, die Prozesse und Datenflüsse sowie insbesondere eine ausführliche Beschreibung der zum Schutz der Daten getroffenen technischen und organisatorischen Maßnahmen. Im Regelfall ist das Datenschutzkonzept damit auch Grundlage der in einem Verarbeitungstätigkeitenverzeichnis zu einem Projekt zu dokumentierenden Daten. Gesetzlich gefordert ist ein Datenschutzkonzept im Regelfall zwar nicht (für eine Ausnahme s. § 75 Abs. 1 SGB X), aber § 22 Abs. 2 BDSG bezieht sich beispielsweise im Wesentlichen auf die Inhalte eines Datenschutzkonzepts. Mit der DSGVO wurde der neue Begriff der Datenschutz-Folgenabschätzung (DSFA, Art. 35) eingeführt, der zwingend bei umfangreichen Verarbeitungen von besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) einzuhalten ist (vgl. Art. 35 Abs. 3b) DSGVO).

5.1 In welchem Verhältnis stehen die bisherigen Inhalte eines solchen Datenschutzkonzepts und die genannten gesetzlichen Regelungsansätze zur neu geregelten DSFA?

Die Pflicht, ein Datenschutzkonzept für ein Forschungsvorhaben vorzulegen, besteht nicht generell, sondern nur gemäß einigen speziellen Gesetzen. Eine entsprechende Pflicht kann generell allenfalls aus den Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO abgeleitet werden. Eine präzise Festlegung der notwendigen Inhalte ergibt sich aus den Gesetzen nicht. Als den Datenschutz umfassendes Dokument sollte es das Verarbeitungsverzeichnis, die Darstellung der technisch-organisatorischen Maßnahmen, die Datenschutz-Folgenabschätzung, die Einschränkung der Betroffenenrechte und die kompensierenden Garantien sowie, soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten. (»» Kap. 11.3, Kap. 11.4)

5.2 Gibt es aus rechtlicher oder ggf. auch praktischer Sicht Hinweise darauf, dass man notwendiger Weise zwei getrennte Dokumente braucht oder die beiden Texte in einem Dokument zusammengefasst werden sollten?

Die Datenschutz-Folgenabschätzung kann im Rahmen eines umfassenderen Datenschutzkonzeptes vorgenommen werden. Möglich sind auch separate Dokumente, wobei es dann sinnvoll ist, dass aufeinander Bezug genommen wird. (»» Kap. 11.4)

Betroffenenrechte

6. Wie ist der Begriff der *„durch den Betroffenen bereitgestellten"* Daten in Art. 20 DSGVO (Datenportabilität) im Kontext der wissenschaftlichen Forschung zu verstehen?

Bereitgestellte Daten des Betroffenen sind auch solche, die durch das Verhalten des Betroffenen generiert werden, nicht jedoch solche, die hieraus abgeleitet sind. (»» Kap. 12.6)

6.1 Fallen „Messdaten" (wie z.B. MRT-Bilder, EEG-Aufnahmen, Röntgenbilder), vom Betroffenen selbst abgegebene Biomaterialproben (z.B. Haarlocke, Blut) und durch Analysen daraus ermittelte genetische Daten unter den Tatbestand der „Bereitstellung durch den Betroffenen"?

Medizinische Messdaten und Bilder gehören ebenso wie Wearable-Daten zu den bereitgestellten Daten. Demgegenüber fallen Biomaterialproben nicht darunter, da es sich um Datenträger handelt und nicht um automatisiert verarbeitete Daten. Auch nicht darunter fallen die Ergebnisse von (genetischen) Analysen dieser Proben. (»» Kap. 12.6)

6.2 Es wird teilweise vertreten, dass die Datenportabilität für öffentliche Stellen (z.B. staatliche Hochschulen) im Forschungskontext ausgeschlossen sein soll (vgl. Artikel Prof. Roßnagel, ZD 4/2019, S. 163). Welche Argumente sprechen für und welche gegen diese Auslegung, insbesondere in den Fällen, in denen öffentliche Stellen mit einer Einwilligung der Betroffenen Daten verarbeiten?

An privilegierten Forschungsvorhaben, nicht nur solchen von Hochschulen, besteht ein öffentliches Interesse, weshalb hierauf die Regelung zur Datenübertragbarkeit nicht anwendbar ist. Soweit diese Voraussetzungen nicht gegeben sind, etwa bei kommerzieller Forschung oder bei einer Datenverarbeitung durch Krankenhäuser oder Arztpraxen, besteht grundsätzlich ein Anspruch auf Datenportabilität nach Art. 20 DSGV, soweit die Daten auf Grundlage einer Einwilligung oder eines Vertrags bereitgestellt sind. (»» Kap. 12.6)

7. Wie umfassend ist das Auskunftsrecht nach Art. 15 DSGVO zu verstehen?

7.1 Müssen bei einem Auskunftsersuchen alle Einzeldaten eines Betroffenen herausgegeben werden?

7.2 Schließt dies auch in einem Forschungsprojekt erst später gewonnene personenbezogene und personenbeziehbare Analyseergebnisse mit ein?

Der Auskunftsanspruch ist allumfassend in Bezug auf Daten mit Personenbezug und schließt, über die Ausgangsdaten hinausgehend, auch die individualisierbaren Forschungsergebnisse mit ein. (»» Kap. 12.3)

7.3 In welchen Fällen kann das Recht auf Auskunft in der Forschung gemäß § 27 Abs. 2 BDSG in Verbindung mit Art. 89 Abs. 2 DSGVO eingeschränkt werden? Wann sind die Voraussetzungen des Tatbestandes *„voraussichtlich die Verwirklichung der Forschungszwecke unmöglich machen oder ernsthaft beeinträchtigen"* erfüllt? Nennen Sie mögliche Beispiele.

Unmöglichkeit einer Auskunftserteilung ist gegeben, wenn eine Zuordnung zur anspruchstellenden Person, auch mit ihrer Unterstützung, nicht mehr möglich ist. Eine Auskunftserteilung macht ein Forschungsprojekt unmöglich, wenn im Fall einer Auskunftserteilung die legitime Zielsetzung des Projektes vereitelt würde. Ein Auskunftsverlangen beeinträchtigt ernsthaft die Verwirklichung der Forschungszwecke, wenn der dafür nötige Aufwand die zumutbare Kapazität des oder der Forschenden übersteigt, so dass ein Projekt nicht abgeschlossen werden kann. Für den Aufwand ist relevant, wie viele Betroffene es gibt, welchen Aufwand die jeweiligen Zuordnungen und die Glaubhaftma-

chungen der Identität verursachen, wie umfangreich die Datensätze sind und welche Kommunikationsform mit den Betroffenen möglich ist. (❯❯❯ Kap. 12.3)

7.4 Wie verhält sich das Recht auf Nichtwissen im Gegensatz zu den Auskunftsrechten der DSGVO? Müssen beispielsweise Patienten über für sie nicht vorhersehbare genetische Risikomarker für Demenz aufgrund eines Auskunftsersuchens nach Art. 15 DSGVO informiert werden? Oder dürfen solche sensiblen Informationen trotz eines Auskunftsersuchens zurückgehalten werden (s.a. Frage 7.3)? Welche Rolle spielt für die Umsetzung der Auskunftsrechte bei genetischen Daten in Forschungsprojekten das Gendiagnostikgesetz?

Die verfassungsrechtlich begründeten Rechte auf Nichtwissen bzw. auf Teilwissen, für die es keine ausdrückliche Erwähnung in der DSGVO gibt, sind bei Auskunftserteilungen zu berücksichtigen. Hierüber hat letztlich der Betroffene – eventuell nach einer eingehenden Beratung – selbst zu entscheiden. Die Regelungen des GenDG sind direkt oder entsprechend anzuwenden. Um das Recht auf Nichtwissen Dritter (z.B. biologischer Verwandter) zu wahren, ist der Betroffene auf entsprechende Implikationen bei der Auskunftserteilung hinzuweisen. (❯❯❯ Kap. 12.3)

8. In welcher Form kann den Transparenzanforderungen nach Art. 13 (und Art. 14) entsprochen werden, wenn die Verarbeitung nicht auf Basis einer informierten Einwilligungserklärung erfolgt? Wie müssen beispielsweise Betroffene dementsprechend über die Nutzung ihrer Daten zu Forschungszwecken informiert werden, wenn diese auf Basis der Forschungsregelungen in einem Landeskrankenhausgesetz erfolgt? Wie muss über ggf. später erfolgende Änderungen der gesetzlich geregelten Rechtsgrundlagen und sich daraus ergebende weitere Verarbeitungen informiert werden?

Die Informationspflichten werden in den Art. 12–14 DSGVO detailliert beschrieben. Sind Sekundärnutzungen, etwa auf Grundlage eines Landeskrankenhausgesetzes, bei der Erhebung bekannt, muss zu diesem Zeitpunkt informiert werden; ansonsten ist eine frühestmögliche Information, in jedem Fall vor der Verarbeitung, nötig. Die Voraussetzungen für einen Verzicht auf eine nachträgliche Information sind in Art. 14 Abs. 5 DSGVO beschrieben. (❯❯❯ Kap. 12.1)

9. Wie ist den Auskunftsrechten nach Art. 14 zu entsprechen, wenn die verantwortliche Stelle oder ein Auftragsverarbeiter die Daten im Forschungskontext beispielsweise lediglich pseudonym verarbeitet und keinen Zugriff auf eine Zuordnungsliste hat?

Ist es einem Verantwortlichen z.B. wegen einer ausschließlich pseudonymen Verarbeitung, nicht möglich, einem Betroffenenanspruch nach den Art. 12ff. DSGVO zu entsprechen, dann ist er hierzu auch nicht verpflichtet. Dies gilt auch für eine Information nach Art. 14 DSGVO und die Auskunft nach Art. 15 DSGVO. Unmöglichkeit ist aber nicht gegeben, wenn der Betroffene die zur Identifikation erforderlichen Informationen nachliefert (Art. 11 Abs. 2 S. 2 DSVO) oder wenn für den Verantwortlichen eine Zuordnung mit Hilfe eines Projektbeteiligten möglich ist. (❯❯❯ Kap. 12.3)

Sonderregelungen für die Forschung

10. Welche Konsequenzen ergeben sich aus dem Recht auf Löschung nach Art. 17 Abs. 3 lit. d DSGVO für die Aufbewahrung von Daten, die bereits im Rahmen einer wissenschaftlichen Publikation nach bisheriger Rechtslage veröffentlicht wurden?

Gemäß den Regelungen in deutschen Forschungsklauseln dürfen personenbezogene Daten im Rahmen der Forschung nur veröffentlicht werden, wenn der Betroffene eingewilligt hat oder dies für die

Darstellung der Forschungsergebnisse über Ereignisse der Zeitgeschichte unerlässlich ist. Möglich ist, dass die öffentliche Erreichbarkeit von Daten aus Gründen des Persönlichkeitsschutzes eingeschränkt werden muss. Sind die Voraussetzungen für eine zulässige Veröffentlichung gegeben, so dürfen veröffentlichte Forschungsdaten weitergenutzt werden. Fehlt es hieran, so ist auch die Weiterverwendung regelmäßig unzulässig. (»» Kap. 12.8)

10.1 Könnte diese Norm beispielsweise die weitere Aufbewahrung von Daten nach Widerruf/Löschungsverlangen rechtfertigen, wenn aufgrund der Daten bereits publiziert wurde und die gute wissenschaftliche Praxis zwecks Nachvollziehbarkeit von veröffentlichten Arbeiten eine Aufbewahrung von 10 Jahren empfiehlt?

Die Notwendigkeit, Forschungsergebnisse überprüfen zu können, kann die weitere Rechtfertigung von Daten legitimieren, selbst wenn Betroffene die Löschung verlangen oder der Verarbeitung widersprechen. Voraussetzung ist, dass die weitere Speicherung hierfür erforderlich ist. Rechtsgrundlage für die weitere Speicherung ist die ursprüngliche Rechtsgrundlage. Erforderlich ist die Speicherung in vielen dieser Fälle nur in pseudonymer Form. (Kap. 7.3, Kap. 12.8, Kap. 12.9)

11. Welche Rechte gewährt Art. 17 Abs. 3 lit. d DS-GVO dem Verantwortlichen generell? Inwieweit ist Art. 11 DSGVO im Forschungskontext anwendbar, beispielsweise bei pseudonymer Verarbeitung der Daten? Mit welchen konkreten Folgen/Erleichterungen (s. auch Frage 9)?

Bei der Datenverarbeitung für Forschungszwecke sind die Verantwortlichen nach Art. 89 Abs. 1 DSGVO zu einer frühestmöglichen Anonymisierung oder Pseudonymisierung verpflichtet. Können sie deshalb die Daten der Betroffenen nicht mehr zuordnen, so muss Betroffenenansprüchen nicht mehr entsprochen werden, wenn nicht der Betroffene zusätzliche Informationen bereitstellt, mit denen die Identifikation möglich ist. Nach Art. 17 Abs. 3 lit. d DSGVO kann auf eine Löschung, Anonymisierung oder Pseudonymisierung nur verzichtet werden, wenn damit die Verwirklichung der Ziele des Forschungsprojektes unmöglich oder ernsthaft beeinträchtigt würden. (»» Kap. 12.3, Kap. 12.8)

12. In Forschungsprojekten, in denen die erhobenen Daten relativ langfristig und für offene Forschungsfragen zur Verfügung gestellt werden, besteht im Sinne einer informationellen Gewaltenteilung die Anforderung, die Identitätsdaten und das Pseudonymmanagement unabhängig von der Verwaltung der eigentlichen Forschungsdaten im Sinne einer unabhängigen Treuhandstelle zu organisieren.

12.1 Besteht diese Anforderung der „informationellen Gewaltenteilung" auch nach der DSGVO und woraus leitet sie sich ab?

Das vom deutschen Bundesverfassungsgericht aus dem Grundgesetz abgeleitete Instrument der „informationellen Gewaltenteilung" ist auch unter der Anwendung europäischen Rechts weiterhin relevant, da der europäische Grundrechteschutz dem nationalen entspricht. Abweichungen durch die europäische Rechtsprechung sind nicht erkennbar. (»» Kap. 10.4)

12.2 Manchmal wird in solchen Fällen, insbesondere wenn die Daten nur aus einer Einrichtung kommen, keine externe Stelle genutzt, sondern die Treuhandfunktion dem behördlichen oder betrieblichen Datenschutzbeauftragten der verantwortlichen Stelle übertragen. Ist beim Vorliegen einer solcherart angelegten Doppelfunktion als Treuhandstelle und Datenschutzbeauftragter eine eigene Aufsicht für den Datenschutzbeauftragten notwendig bzw. nach welchen rechtlichen Kriterien und Gesetzen kann diese Frage beantwortet werden?

Bei der gleichzeitigen Wahrnehmung der Funktion eines Datenschutzbeauftragten und eines Datentreuhänders kann es zu Interessenkonflikten kommen, weshalb eine solche Verbindung nicht zu empfehlen ist (»» Kap. 10.4)

13. Auf welcher Rechtsgrundlage dürfen bereits unter früherem Recht erhobene und verarbeitete Biomaterialproben (sog. „Altproben"), die nach altem BDSG als anonym betrachtet werden konnten, nach der DSGVO und ggf. dem neuen BDSG verarbeitet werden? Was ergibt sich, wenn zu diesen Altproben keine direkt identifizierenden Daten einzelner Personen oder Patienten mehr gespeichert bzw. zugreifbar sind?

Altproben, die nach früherem Recht als anonym eingestuft wurden, unterliegen dem aktuellen Datenschutzrecht und der DSGVO, wenn sie zum Zeitpunkt der Verarbeitung dadurch personenbeziehbar sind, dass sie durch potenziell verfügbares Zusatzwissen einer Person zugeordnet werden können. (»» Kap. 10.1)

14. Es besteht zurzeit große Unsicherheit darüber, welche Rechtsgrundlagen anzuwenden sind, wenn Daten und ggf. Biomaterialproben aus einem Nicht-EU-Land (z.B. USA), in dem sie als anonym klassifiziert werden, an einen Forschungspartner in der EU geschickt werden und europäische Forschungseinrichtungen indes – auf Grundlage der DSGVO – von einem Personenbezug ausgehen müssten. Kann die rechtliche Qualifizierung an der Quelle als „anonym" unter der DSGVO weiter gelten? Wie sind Fälle zu beurteilen, in denen eine Zuordnung zu einer Person oder einem Patienten nur im Nicht-EU-Ausland möglich ist?

Durch die Vorgaben der DSGVO und deren Präzisierung durch den EuGH ist in abstrakter Weise klargestellt, wann eine Anonymisierung von Daten anzunehmen ist. Entscheidend ist der Aufwand, die Daten einer konkreten natürlichen Person zuzuordnen, und damit die Wahrscheinlichkeit, dass dies möglich ist. Eine anderweitige Bewertung in einem Nicht-EU-Land spielt für die Verarbeitung durch Stellen in der EU keine Rolle. Ist das für eine Identifizierung nötige Zusatzwissen ausschließlich im Drittausland verfügbar und ist es völlig unwahrscheinlich, dass dieses Zusatzwissen verfügbar gemacht werden kann, dann kann Anonymität angenommen werden. (»» Kap. 10.1, Kap. 13.6)

Evaluation der Forschungsvorschriften aus der EU-DSGVO

15. Bewerten Sie bitte den aktuellen Regelungsrahmen der DSGVO mit Blick auf die konkrete Anwendbarkeit in der medizinischen Forschung. Nutzen Sie hierfür die Analysen und Antworten zu den vorangehenden Fragen. Gehen Sie bei engem Bezug zur DSGVO, und soweit aus Ihrer Sicht die Notwendigkeit besteht, auch auf relevante Regelungen auf Bundes- und Landesebene ein.

15.1 Welche positiven Ansätze sehen Sie?

Die DSGVO bietet einen validen europarechtlichen Rahmen für einen Ausgleich zwischen dem Datenschutz und der Forschungsfreiheit, indem sie einerseits die Datenverarbeitung für Forschungszwecke privilegiert, andererseits geeignete Garantien für die Betroffenen notwendig macht. (»» Kap. 14.1)

15.2 Welche Regelungen sind aus Ihrer Sicht problematisch?

Dadurch, dass es die DSGVO über Öffnungsklauseln weitgehend den Mitgliedstaaten überlässt, die materiellen Regelung zur Datenverarbeitung, die organisatorischen und prozessualen Rahmenbedingungen sowie die Beschränkung der Betroffenenrechte zu regeln, besteht bisher kein einheitliches Datenschutzrecht für Forschungszwecke in der Europäischen Union. Die Gesetzgeber in Deutschland haben die Öffnungsklauseln bisher nicht dafür genutzt, eine inhaltliche Anpassung an die europäischen Vorgaben und eine nationale Harmonisierung vorzunehmen. Die Regeln genügen zudem nicht

den Anforderungen an eine moderne Forschungstätigkeit. Die bestehende Rechtsunsicherheit ist hinderlich sowohl für eine wirksame Forschungstätigkeit wie für den Datenschutz. (»» Kap. 14.1)

15.3 Welche Auslegungsprobleme oder Unklarheiten in der Anwendung sehen Sie?

Es ist unklar, welche Forschungsprojekte als privilegiert behandelt werden können. Die Unbestimmtheit der Regeln geben den Forschenden keine klaren Vorgaben. Es fehlt sowohl an Standards wie auch an einer einheitlichen Infrastruktur für Transparenz und wissenschaftliche Kooperation. (»» Kap. 14.2)

15.4 Welche Empfehlungen würden Sie dem europäischen Gesetzgeber sowie ggf. auch den nationalen Gesetzgebern auf Bundes- und Landesebene für die Weiterentwicklung des Rechtsrahmens mit auf den Weg geben?

Auf der Grundlage der DSGVO kann auf europäischer Ebene ein einheitliches Datenschutzrecht für die Forschung oder zumindest für die medizinische Forschung geschaffen werden, zumal es über die wesentlichen Regelungsinhalte einen weitgehenden Konsens geben dürfte. Solange es keine europarechtlichen Regelungen gibt, sind die deutschen Gesetzgeber gefordert, auf nationaler Ebene einheitliche Regelungen zu schaffen. Dies wäre – aber erst nach einer Änderung der Gesetzgebungszuständigkeit – durch ein Bundesgesetz möglich. Ohne Grundgesetzänderung bietet sich der Abschluss eines Bund-Länder-Staatsvertrags an. Bis dahin und zur Vorbereitung einer Gesetzgebung wird die Ausarbeitung von Verhaltensregeln empfohlen (»» Kap. 14.2)

Ausgewählte Literatur

Fett gedruckte Literaturhinweise werden in den Fußnoten verkürzt gemäß dem Klammerinhalt zitiert.

Albrecht, Jan Philipp/Jotzo, Florian, Das neue Datenschutzrecht der EU, 2017 (Albrecht/Jotzo).

Auernhammer (Begr.), s. Eßer/Kramer/von Lewinski (Auernhammer).

Baumann, Paul/Krahn, Philipp/Lauber-Rönsberg, Anne, Forschungsdatenmanagement und Recht, 2021 (BKLR).

Becker, Ulrich/Hatje, Armin/Schoo, Johann/Schwarze, Jürgen (Hrsg.), EU-Kommentar, 4. Aufl. 2019 (Schwarze).

Bergmann, Lutz (Begr.)/Möhrle, Roland/Herb, Armin (Hrsg.), Datenschutzrecht, Stand August 2019 (BMH).

Bernhardt, Ute/Ruhmann, Ingo/Weichert, Thilo, Die Forschungsklauseln im neuen Datenschutzrecht, 18.10.2018, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2018_forschungklauseln_181018.pdf (Bernhardt/Ruhmann/Weichert).

Bieresborn, Dirk, Sozialdatenschutz nach Inkrafttreten der EU-Datenschutzgrundverordnung, NZS 2017, 887–892, 926–933; 2018, 10–16.

Bischoff, Claudia/Wiencke, Julia, Datenschutzrechtliche Voraussetzungen klinischer Prüfungen, ZD 2019, 8–13.

Bizer, Johann, Forschungsfreiheit und Informationelle Selbstbestimmung, 1992 (Bizer).

Bizer, Johann, Der Datentreuhänder, DuD 1999, 392–395.

Callies, Christian/Ruffert, Matthias (Hrsg.), EUV/AEUV, 5. Aufl. 2016 (Callies/Ruffert)

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Bundesdatenschutzgesetz, 5. Aufl. 2016 (DKWW).

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-Datenschutz-Grundverordnung und BDSG, 2. Aufl. 2020 (DWWS).

Dammann, Ulrich/Simitis, Spiros, EG-Datenschutzrichtlinie, 1997 (Dammann/Simitis).

Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=5 (Datenethikkommission).

Datenschutzkonferenz (DSK), Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO v. 03.04.2019.

Datenschutzkonferenz (DSK), Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, Stand 19.03.2018.

Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, Stellungnahme, 2017, https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf (Deutscher Ethikrat).

Dierks, Christian, Rechtsgutachten zur elektronischen Datentreuhänderschaft, 2008 (Dierks 2008).

Dierks, Christian, Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, unter Mitarbeit von Kircher, Philipp/Engelke, Karsten/Haase, Martin, 15.09.2019 (Dierks 2019).

Dierks, Christian, Europäischer Datenschutzraum für die medizinische Forschung, 08.07.2020 (Dierks 2020).

Dierks, Christian/Roßnagel, Alexander, Sekundärnutzung von Gesundheits- und Sozialdaten – rechtliche Rahmenbedingungen, 2019 (Dierks/Roßnagel).

Dochow, Carsten, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, 2017 (Dochow).

Dreier, Horst, Grundgesetz Kommentar, Bd. I, 3. Aufl. 2013 (Dreier).

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO Datenschutz-Grundverordnung, Kommentar, 2. Aufl. 2018 (Ehmann/Selmayr).

Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hrsg.), DSGVO – BDSG, 6. Aufl. 2018 (Auernhammer).

European Data Protection Supervisor, EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019, https://edps.europa.eu/sites/edp/files/

publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf (EDPS 2019).

European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, 6 January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (EDPS 2020).

Europäischer Datenschutzausschuss, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b) vom 23. Januar 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_de.pdf (EDSA).

Friedewald, Michael/Obersteller, Hannah/Nebel, Maxi/Bieker, Felix/Rost, Martin, White Paper Datenschutz-Folgenabschätzung, Forum Privatheit, 2016, https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016-1.pdf (Friedewald u.a).

Geminn, Christian L., Wissenschaftliche Forschung und Datenschutz, DuD 2018, 640–646.

GMDS-Präsidiumskommission „Datenschutz in der Forschung", Hrsg.: Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V., Memorandum zum Datenschutz in der medizinischen Forschung (Mai 2017), https://gmds.de/fileadmin/user_upload/Publikationen/Empfehlungen_Veroeffentlichungen/170511_Memorandum_zum_Datenschutz.pdf (GMDS).

Gola, Peter (Hrsg.), DS-GVO, 2. Aufl. 2018 (Gola).

Gola, Peter/Heckmann, Dirk (Hrsg.), BDSG – Bundesdatenschutzgesetz, 13. Aufl. 2019 (Gola/Heckmann).

Golland, Alexander, Reichweite des „Joint Controllership": Neue Fragen der gemeinsamen Verantwortlichkeit, K&R 2019, 533–537.

Grosskopf, Lambert/Momsen, Carsten, Outsourcing bei Berufsgeheimnisträgern – strafrechtliche Verpflichtung zur Compliance? CCZ 2018, 98–108.

Härting, Niko, Datenschutz-Grundverordnung, 2016 (Härting).

Härting, Niko/Gössling, Patrick, Gemeinsame Verantwortlichkeit bei einer Facebook-Fanpage, NJW 2018, 2523–2526.

Hauser, Andrea/Haag, Ina, Datenschutz im Krankenhaus, 4. Aufl. 2012 (Hauser/Haag).

Health Ethics and Policy Lab, ETH Zürich, How the General Data Protection Regulation changes the rules for scientific research, European Parliamentary Research Service, July 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf (Health Ethics Policy Lab).

Hentschel, Anja/Hornung, Gerrit/Jandt, Silke (Hrsg.), Mensch – Technik – Umwelt, Verantwortung für eine sozialverträgliche Zukunft, Festschrift für Alexander Roßnagel zum 70. Geburtstag, 2020 (HHJ).

Hornung, Gerrit/Hofmann, Kai, Die Auswirkungen der europäischen Datenschutzreform auf die Markt- und Meinungsforschung, ZD Beilage 4/2017, 1–16.

Johannes, Paul C., Das Recht des Forschers auf Datenschutz, DuD 2012, 817–824.

Johannes, Paul C./Richter, Philipp, Privilegierte Verarbeitung im BDSG-E, DuD 2017, 300–305.

Jung, Alexander/Hansch, Guido, Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen, ZD 2019, 143–148.

Kingreen, Thorsten/Kühling, Jürgen (Hrsg.), Gesundheitsdatenschutz, 2015 (Kingreen/Kühling).

Kipker, Dennis-Kenji/Voskamp, Friederike (Hrsg.), Sozialdatenschutz in der Praxis, 2021 (Kipker/Voskamp).

Krawczak, Michael/Weichert, Thilo, Medizinforscher und Datenschützer fordern Bund-Länder-Staatsvertrag, DANA 2017, 193–201.

Kremer, Sascha, Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung? CR 2019, 225–234.

Kühling, Jürgen (unter Mitwirkung von Sackmann, Florian/Schildbach, Roman), Rechtsgutachten über den sozialdatenschutzrechtlichen Weiterentwicklungsbedarf im SGB V und SGB X im Hinblick auf Big-Data-Anwendungen, 04.09.2019, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/Rechtsgutachten-Big-Data.pdf (Kühling).

Kühling, Jürgen/Buchner, Benedikt (Hrsg.) DS-GVO – BDSG, Kommentar, 3. Aufl. 2020 (Kühling/Buchner).

Laue, Philip/Nink, Judith/Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016 (LNK).

Martini, Mario/Hohmann, Matthias, Der gläserne Patient: Dystopie oder Zukunftsrealität? NJW 2020, 3573–3578.

Mausbach, Julian, Europäischer Datenschutz und medizinische Forschung in der Schweiz, ZD 2019, 450–454.

Metschke, Rainer, Datenschutz in Wissenschaft und Forschung, Berliner Datenschutzbeauftragter (Hrsg.), Materialien zum Datenschutz 18, 1994 (Metschke).

Metschke, Rainer/Wellbrock, Rita, Datenschutz in Wissenschaft und Forschung, Hessischer Datenschutzbeauftragter (Hrsg.), 2002 (Metschke/Wellbrock).

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019 (Meyer/Hölscheidt).

Monreal, Manfred, Der Rahmen der Verantwortung und die klare Linie in der Rechtsprechung des EuGH zu gemeinsam Verantwortlichen, ZD 2019, 797–808.

Netzwerk Datenschutzexpertise, Plädoyer für ein medizinisches Forschungsgesetz, Autoren: Bernhardt, Ute/Ruhmann, Ingo/Weichert, Thilo, 22.02.2021, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021_02_medforschungdatens_final.pdf (Netzwerk Datenschutzexpertise).

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl. 2021 (Paal/Pauly).

Pohle, Jan/Ghaffari, Sheila, Die Neufassung des § 203 StGB – der Befreiungsschlag für IT-Outsourcing am Beispiel der Versicherungswirtschaft, CR 2017, 489–495

Prütting, Dorothea (Hrsg.), Fachanwaltskommentar Medizinrecht, 3. Aufl. 2014 (Prütting).

Rat für Informationsstrukturen, Datenschutz und Forschungsdaten, Aktuelle Empfehlungen, März 2017 (RfII).

Rat für Sozial- und Wirtschaftsdaten, Datenerhebung mit neuer Informationstechnologie, 2020, https://www.konsortswd.de/wp-content/uploads/RatSWD_Output6.6_Datenerhebung-neueIT.pdf (RatSWD).

Roßnagel, Alexander (Hrsg.), Europäische Datenschutz-Grundverordnung, 2017 (Roßnagel 2017).

Roßnagel, Alexander (Hrsg.), Das neue Datenschutzrecht, 2018 (Roßnagel 2018).

Roßnagel, Alexander, Datenschutz in der Forschung, ZD 2019, 157–164.

Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen, Digitalisierung für Gesundheit, Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, 2021, https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021_online.pdf (Sachverständigenrat).

Schaar, Katrin, DS-GVO: Geänderte Vorgaben für die Wissenschaft – Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen? ZD 2016, 224–226.

Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, 2017 (Schantz/Wolff).

Schönke, Adolf/Schröder, Horst/Cramer, Peter u.a., Strafgesetzbuch, 30. Aufl. 2019 (Schönke/Schröder).

Schneider, Uwe Klaus, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, 2015 (Schneider 2015).

Schneider, Uwe Klaus, Einrichtungsübergreifende elektronische Patientenakte, 2016 (Schneider 2016).

Schreiber, Kristina, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, ZD 2019, 55–60.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), DS-GVO/BDSG, Heidelberger Kommentar, 2018 (SJTK).

Schwarze, s. Becker/Hatje/Schoo/Schwarze (Schwarze).

Simitis, Spiros (Hrsg.), BDSG Bundesdatenschutzgesetz, 8. Aufl. 2014 (Simitis).

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (Hrsg.), Datenschutzrecht, 2019 (SHS).

Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019 (Specht/Mantz).

Specht-Riemenschneider, Louisa/Schneider, Ruben, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503–509.

Stern, Klaus/Sachs, Michael, Europäische Grundrechte-Charta, 2016 (Stern/Sachs).

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung, 2017 (Sydow-DSGVO).

Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (Koordination), „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 30.03.2020, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf (TMF).

Thüsing, Gregor/Rombey, Sebastian, Dateigebundene Verarbeitung und Datenverantwortung, NZA 2019, 6–11.

Thüsing, Gregor/Rombey, Sebastian, Forschung im Gesundheitswesen: Anforderungen an einen passgenauen Datenschutz, NZS 2019, 201–205.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Datentreuhänderschaft in der Biobank-Forschung, 30. April 2009 (ULD).

Weichert, Thilo, Big Data im Gesundheitsbereich, Gutachten im Rahmen des Projektes „Assessing Big Data" (ABIDA), 2018, https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf (Weichert 2018).

Weichert, Thilo, Verantwortlichkeiten bei Social-Media-Plattformen, DANA 2019, 4–10.

Weichert, Thilo, Die Forschungsprivilegierung in der DS-GVO, ZD 2020, 18–24.

Weichert, Thilo/Krawczak, Michael, Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland, MIBE 2019, Vol. 15(1), 1–8.

Werkmeister, Christoph/Schwaab, Michael, Auswirkungen und Reichweite des datenschutzrechtlichen Forschungsprivilegs, CR 2019, 85–90.

Wiebe, Andreas, Datenschutz, Big Data und KI im Gesundheitswesen, in: Specht-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian/Thomse, Oliver, Festschrift für Jürgen Taeger, 2020, 531–554 (Wiebe).

Abkürzungen

a.A.	andere Ansicht
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AMG	Arzneimittelgesetz
Anm.	Anmerkung
AnwBl	Anwaltsblatt (Zeitschrift)
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BArchivG	Bundesarchivgesetz
Bay	Bayern/Bayerisch
BB	Betriebsberater (Zeitschrift)
Bbg	Brandenburg
BDSG/aF	Bundesdatenschutzgesetz/alte Fassung
Begr.	Begründer
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH/Z	Bundesgerichtshof/Entscheidungssammlung Zivilrecht
BKAG	Bundeskriminalamtsgesetz
BKL-R	Baumann/Krahn/Lauber-Rönsberg (Monographie)
Bln	Berlin/Berliner
BMH	Bergmann/Möhrle/Herb (Kommentar)
BnotO	Bundesnotarordnung
BRAO	Bundesrechtsanwaltsordnung
BR-Drs.	Bundesrats-Drucksache
BremDSGVOAG	Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung
BT-Drs.	Bundestags-Drucksache
BVerfG/E	Bundesverfassungsgericht/Entscheidungssammlung
BZRG	Bundeszentralregistergesetz
BW	Baden-Württemberg
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift
CR	Computer und Recht (Zeitschrift)
CuA	Computer und Arbeit (Zeitschrift)
CuR	Computer und Recht (Zeitschrift)
DANA	DatenschutzNachrichten (Zeitschrift)
DB	Der Betrieb (Zeitschrift)
ders.	derselbe
d.h.	das heißt
DIN	Deutsche Industrienorm
DIZ	Datenintegrationszentrum
DKWW	Däubler/Klebe/Wedde/Weichert (Kommentar)
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DSG	Datenschutzgesetz
DSGVO	Europäische Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz

DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl	Deutsches Verwaltungsblatt
DWWS	Däubler/Wedde/Weichert/Sommer (Kommentar)
EG-DSRl	Europäische Datenschutzrichtlinie
EDPB	European Data Protection Board (Europäischer Datenschutzausschuss)
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
Einl	Einleitung
EIRD	Implantateregister-Errichtungsgesetz Deutschland
ErwGr	Erwägungsgrund (der DSGVO)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag der Europäischen Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
EWS	Europäisches Wirtschafts- und Steuerrecht (Zeitschrift)
f/ff	fort-/folgende
Fn.	Fußnote
G.	Gesetz
GenDG	Gendiagnostikgesetz
GG	Grundgesetz
GMDS	Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie
GRCh	Europäische Grundrechte-Charta
GVOBl.	Gesetzes- und Verordnungsblatt
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
Hess GVBl.	Hessisches Gesetzes- und Verordnungsblatt
HHJ	Hentschel/Hornung/Jandt (Festschrift)
h.M.	herrschende Meinung
Hmb	Hamburg/Hamburgisch
Hrsg.	Herausgeber
i.d.R.	in der Regel
IRegG	Implantateregistergesetz
IoT	Internet of Things (Internet der Dinge)
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
JR	Juristische Rundschau (Zeitschrift)
JZ	Juristenzeitung
Kap.	Kapitel
KJ	Kritische Justiz (Zeitschrift)
K&R	Kommunikation und Recht (Zeitschrift)
KriPoZ	Kriminalpolitische Zeitschrift
LBerufsG ZÄ	Landesberufsgericht der Zahnärztekammer
LDI NRW	Landesbeauftragte/r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LDSG	Landesdatenschutzgesetz/e
lit.	Buchstabe
LS	Leitsatz
LSA	Land Sachsen-Anhalt
LT-Drs.	Landtags-Drucksache
LVerfG	Landesverfassungsgericht
MBOÄ	Musterberufsordnung der Ärztekammern
MedR	Medizinrecht (Zeitschrift)
medstra	Die Zeitschrift für Medizinstrafrecht

MDR	Monatsschrift des Deutschen Rechts
MIBE	Medizinische Informatik, Biometrie und Epidemiologie (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
MV	Mecklenburg-Vorpommern
m.w.N.	mit weiteren Nachweisen
NDSG	Niedersächsisches Datenschutzgesetz
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NRW	Nordrhein-Westfalen
NStZ	Neue Zeitschrift für Strafrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZS	Neue Zeitschrift für Sozialrecht
o.g.	oben genannt
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
RDV	Recht der Datenverarbeitung (Zeitschrift)
RfII	Rat für InformationsInfrastrukturen
Rn.	Randnummer
Rspr.	Rechtsprechung
RP	Rheinland-Pfalz
S.	Seite/Satz
SächsDSG	Sächsisches Datenschutzgesetz
SDSG	Saarländisches Datenschutzgesetz
SGb	Die Sozialgerichtsbarkeit (Zeitschrift)
SGB	Sozialgesetzbuch
SH	Schleswig-Holstein
SHS	Simitis/Hornung/Spiecker genannt Döhmann (Kommentar)
SJTK	Schwartmann/Jaspers/Thüsing/Kugelmann (Kommentar)
s.o.	siehe oben
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StraFo	StrafverteidigerForum (Zeitschrift)
StrlSchG	Strahlenschutzgesetz
StVollzG	Strafvollzugsgesetz
s.u.	siehe unten
SZ	Süddeutsche Zeitung
TA	Technikfolgenabschätzung
TB	Tätigkeitsbericht
Thür	Thüringen/Thüringisch
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
TPG	Transplantationsgesetz
u.	und
u.a.	unter anderem/und andere
UAbs.	Unterabsatz
UAC	Use and Access Committee
u.U.	unter Umständen
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
US/A	United States/of America, Vereinigte Staaten/von Amerika
v.	von
VerfG/H	Verfassungsgericht/Verfassungsgerichtshof

VersR	Versicherungsrecht (Zeitschrift)
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
Vol.	Band (einer Zeitschrift)
VR	Verwaltungsrundschau (Zeitschrift)
VwGO	Verwaltungsgerichtsordnung
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WP	Working Paper
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZIP	Zeitschrift für Wirtschaftsrecht
ZPO	Zivilprozessordnung

TMF – Forscher vernetzen
Lösungen bereitstellen
Doppelarbeit vermeiden

Die TMF sorgt für Qualitäts- und Effizienzsteigerung in der medizinischen Forschung

Die moderne medizinische Forschung steht vor zunehmend komplexen Herausforderungen, für deren Lösung sich die Akteure aus Grundlagenforschung, klinischer Forschung, Versorgungseinrichtungen, Industrie und weiteren Partnern miteinander vernetzen und gemeinsame Strategien entwickeln müssen. Ein zentraler Ansatz ist die Effizienzsteigerung auf allen Ebenen der medizinischen Forschungs- und Entwicklungskette, um – bei gesicherter Qualität – Forschungsergebnisse auf schnellstem Wege in die Patientenversorgung zu übertragen und damit zu einem effizienten und leistungsfähigen Gesundheitswesen beizutragen. Im Sinne einer Qualitätssteigerung und der Entwicklung hin zu einer zunehmend personalisierten oder Präzisionsmedizin spielt die Zusammenführung von Daten aus verschiedenen Quellen und die Verknüpfung mit Bioproben eine immer wichtigere Rolle.

Die Bundesregierung unterstützt diesen Prozess unter anderem im Rahmen des Gesundheitsforschungsprogramms und fördert seit mehr als zehn Jahren konsequent die medizinische Verbundforschung. Erfolgreiche Beispiele sind die herausragenden Ergebnisse aus den Kompetenznetzen in der Medizin oder den Koordinierungszentren für Klinische Studien. Aufbauend auf diesen Erfahrungen sind neue Verbundprojekte und -einrichtungen initiiert worden, die immer mehr Partner miteinander vernetzen. Dazu gehören nicht zuletzt die Deutschen Zentren der Gesundheitsforschung, die Nationale Kohorte oder die zentralisierten Biobanken, die an Universitätskliniken in Deutschland aufgebaut und übergreifend vernetzt wurden. Neben diesen Großprojekten verfolgen auch zahlreiche weitere Einrichtungen und Projekte ähnliche Ziele.

In der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung (kurz: TMF) arbeiten sie zusammen, um gemeinsam und disziplinübergreifend die Herausforderungen zu lösen, die sich beim Aufbau der notwendigen Forschungs- und Dateninfrastrukturen in technischer, rechtlich-ethischer, organisatorischer sowie auch kommunikativer Hinsicht stellen. Sie übernimmt damit eine wesentliche nationale Aufgabe zur Qualitäts- und Effizienzsteigerung für die Forschung. Die TMF wird vom Bundesministerium für Bildung und Forschung (BMBF) sowie in zunehmendem Maße auch von der Deutschen Forschungsgemeinschaft (DFG) gefördert.

Im November 2015 hat das BMBF das Förderkonzept Medizininformatik initiiert. Ziel der Medizininformatik-Initiative ist die Verbesserung von Forschungsmöglichkeiten und der Patientenversorgung durch IT-Lösungen. Diese sollen den Austausch und die Nutzung von Daten aus Krankenversorgung, klinischer und biomedizinischer Forschung über die Grenzen von Institutionen und Standorten hinweg ermöglichen. Die übergreifende Zusammenarbeit wird von einer Begleitstruktur unterstützt, die gemeinsam von der TMF, dem Medizinischen Fakultätentag (MFT) und dem Verband der Universitätsklinika Deutschlands (VUD) betrieben wird.

Seit Oktober 2021 koordiniert die TMF zudem die vom Bundesministerium für Gesundheit (BMG) geförderte „Nationale Strategie für Genommedizin“ zum Aufbau einer bundesweiten Plattform zur medizinischen Genomsequenzierung „genomDE“. Ein Konsortium aus 14 nationalen Initiativen und Verbünden aus den Bereichen Onkologie, Seltene Erkrankungen sowie Patientenvertretungen hat als zentrales Anliegen, den Zugang möglichst vieler Patientinnen und Patienten zu sinnvollen klinischen Anwendungsmöglichkeiten einer Genomsequenzierung zu verbessern.

Ziele und Aufgaben

Als Dachorganisation für die medizinische Verbundforschung verfolgt die TMF das Ziel, die organisatorischen, rechtlichen-ethischen und technologischen Voraussetzungen für die klinische, epidemiologische und translationale Forschung zu verbessern. Sie hat die Aufgabe, die wissenschaftliche Arbeit der modernen medizinischen Forschung, die heutzutage überwiegend in kooperativen Projekten mit mehreren beteiligten Standorten stattfindet, zu unterstützen. Dazu stellt sie – öffentlich und gemeinfrei, also für jeden Forscher nutzbar – Gutachten, generische Konzepte, Leitfäden und IT-Anwendungen ebenso wie Schulungs- und Beratungsangebote bereit. Der überwiegende Teil der Produkte steht unter www.tmf-ev.de sowie www.toolpool-gesundheitsforschung.de zum Download zur Verfügung. Ausgewählte Ergebnisse werden in der Schriftenreihe der TMF publiziert.

Die Produkte werden – von der Forschung für die Forschung – von den Fachexperten der Mitgliedsverbünde entwickelt, die in den interdisziplinären Arbeitsgruppen der TMF zusammenkommen. Als Grundmuster und Leitmotiv der gemeinsamen Arbeit in den Arbeitsgruppen gilt der Anspruch, gemeinsame Probleme gemeinsam zu lösen, von vorhandenen Erfahrungen gegenseitig zu profitieren, Doppelarbeit zu vermeiden sowie professionelle Lösungen zu erarbeiten, zu diesen einen Konsens in der Forschergemeinschaft herzustellen und ihre konsequente Nutzung und langfristige Verfügbarkeit zu gewährleisten.

Geschichte

Die TMF wurde 1999 unter dem Namen „Telematikplattform für Medizinische Forschungsnetze“ als Förderprojekt des BMBF gegründet. Mit dem Ziel, die Struktur zu verstetigen und die gemeinsame Querschnittseinrichtung der medizinischen Verbundforschung noch stärker in die Hände der Forscher selbst zu legen, wurde 2003 der TMF e.V. gegründet. Seither ist die Zahl der Mitgliedsverbünde stark angewachsen. Damit zusammenhängend hat sich auch das thematische Spektrum der TMF verbreitert, die zunächst primär auf Fragen der IT-Infrastruktur ausgerichtet war. Die Themen reichen heute von rechtlichen und ethischen Rahmenbedingungen und Fragen der IT-Infrastruktur über Qualitätsmanagement und Standards für klinische Studien sowie den Themenkomplex Biobanken und molekulare Medizin bis hin zum Problem der Verzahnung von Forschung und Versorgung oder Fragen der Verbundkoordination und der Wissenschaftskommunikation.

2010 beschloss die Mitgliederversammlung eine Umbenennung der TMF, da der Begriff „Telematikplattform“ diesem breiten Spektrum nicht mehr gerecht wurde. Der seither geführte Name „TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.“ erfasst die Aufgaben und Themen der TMF auf spezifischere Weise.

Mitglieder

Mitglieder der TMF sind überregionale medizinische Forschungsverbünde, vernetzt arbeitende universitäre und außeruniversitäre Forschungsinstitute, Methodenzentren, regionale Verbundprojekte sowie kooperative Studiengruppen. Dazu gehören unter anderem

- die Deutschen Zentren der Gesundheitsforschung,
- die Nationale Kohorte,
- Kompetenznetze in der Medizin,
- Koordinierungszentren bzw. Zentren für Klinische Studien (KKS/ZKS),
- Integrierte Forschungs- und Behandlungszentren,
- Netzwerke für Seltene Erkrankungen,
- die Fraunhofer-Gesellschaft (mit dem Fraunhofer ITEM als direktem Mitglied),
- Forschungsnetz Zoonosen,
- zentralisierte Biomaterialbanken,
- Universitätsinstitute,
- Patientenorganisationen
- und zahlreiche weitere.

Über Mitgliedsverbünde sind bundesweit alle Universitätsklinika und zahlreiche außeruniversitäre Forschungsstandorte in unterschiedlicher Weise in die TMF eingebunden. Mit Kooperationspartnerschaften sorgt die TMF auch darüber hinaus für eine Einbindung der relevanten Institutionen im Gesundheitswesen.

Themen und Arbeitsweise

Die durch die Forschungsverbünde und -einrichtungen gemeinsam zu bearbeitenden Querschnittsaufgaben gehen weit über Fragen von Informations- und Kommunikationstechnologie im technischen Sinne hinaus. Die Wissenschaftler in den Forschungsprojekten brauchen Unterstützung und Erfahrungsaustausch in großer Breite:

- zu Fragen der konkreten Umsetzung von Datenschutz und ethischen Richtlinien,
- zum Aufbau von Forschungsinfrastrukturen wie Datenbanken für Forschungsregister und Biobanken,
- zur strategischen Nutzung von Informationstechnologie für die Prozessunterstützung wie für die wissenschaftliche Auswertung,
- zu Rechtsfragen in vielerlei Hinsicht, beispielsweise zum Vertragsrecht innerhalb von Netzwerken, zu Patienteneinwilligungen oder zu Verwertungsfragen,
- zu Fragen der Organisation und des Managements von Forschungsnetzen und ihren Projekten sowie
- zunehmend auch zu Fragen der Kommunikation, der Finanzierung und der Nachhaltigkeit von mit öffentlichen Geldern aufgebauten Netzwerkstrukturen.

Alle diese Fragen werden kontinuierlich in den Arbeitsgruppen der TMF bearbeitet, in denen sich die jeweiligen Fachleute aus den verschiedenen Projekten und Forschungsstandorten interdisziplinär zusammenfinden. Dabei entstehen strategische Anstöße und Impulse für die Forschungsinfrastruktur, vor allem aber konkrete Hilfen, Produkte und Services für den Forscher. Regelmäßig tagen einzelne Arbeitsgruppen auch gemeinsam, um auf diese Weise themenübergreifende Aspekte besser aufnehmen und Doppelaktivitäten der Arbeitsgruppen vermeiden zu können.

Arbeitsgruppen

Die Arbeitsgruppen initiieren Projekte und betreuen sie im Verlauf – bis hin zur Implementierung der Ergebnisse und zur Beratung von Forschungsprojekten auf dieser Basis. Neue Projektvorschläge durchlaufen ein mehrstufiges Auswahlverfahren – von der fachlichen Prüfung und Schärfung in den Arbeitsgruppen über Beratung in der Geschäftsstelle bis hin zur Begutachtung durch den Vorstand. Mit diesem Vorgehen wird sichergestellt, dass die in den Projekten adressierten Probleme für die Forschergemeinschaft relevant sind und dass die angestrebte Lösung einen breiten Konsens für die spätere Anwendung findet.

Arbeitsgruppen können in der TMF je nach aktuellem Bedarf neu eingerichtet, zusammengelegt oder auch aufgelöst werden, wenn ein Thema keine hohe Relevanz mehr hat. Derzeit gibt es zehn Arbeitsgruppen:

- Arbeitsgruppe Biomaterialbanken
- Arbeitsgruppe Datenschutz
- Arbeitsgruppe Datenqualität und Transparenz
- Arbeitsgruppe IT-Infrastruktur und Qualitätsmanagement
- Arbeitsgruppe Management klinischer Studien
- Arbeitsgruppe Medizintechnik
- Arbeitsgruppe Medizinische Bioinformatik und Systemmedizin
- Arbeitsgruppe Netzwerkkoordination
- Arbeitsgruppe Wissenschaftskommunikation
- Arbeitsgruppe Zoonosen und Infektionsforschung

Der interdisziplinäre Austausch wird über die Arbeitsgruppen hinaus durch zahlreiche Symposien und Workshops, durch den TMF-Jahreskongress sowie durch Foren ergänzt. Ferner unterstützt die TMF im Begleitprojekt zur BMBF-Fördermaßnahme zum Aufbau modellhafter Register für die Versorgungsforschung gemeinsam mit dem Deutschen Netzwerk für Versorgungsforschung (DNVF) aktuell die geförderten Register insbesondere im Bereich Qualitätsmanagement, Aufbau von IT-Infrastrukturen und Erarbeitung geeigneter Datenschutzkonzepte.

Lösungen stehen frei zur Verfügung

Die TMF stellt Gutachten, generische Konzepte, Leitfäden und IT-Anwendungen ebenso bereit, wie sie Schulungs- und Beratungsservices der Arbeitsgruppen, auch in Form von Einzelberatungen, anbietet. Die Ergebnisse der Arbeit in der TMF stehen öffentlich und gemeinfrei zur Verfügung.
Mit diesem offenen Ansatz verfolgt die TMF das Ziel,

- methodisches Know-how und Infrastrukturen für die vernetzte medizinische Forschung breit verfügbar zu machen,
- die Harmonisierung, die Interoperabilität und das Qualitätsmanagement in der vernetzten medizinischen Forschung durch entsprechende Infrastruktur, Leitfäden und Services zu stärken,
- die Kollaboration in der deutschen medizinischen Forschung sowie deutsche Forscher in internationalen Kooperationen zu stärken,

- die Verstetigung und Nachhaltigkeit akademischer medizinischer Forschungsprojekte zu unterstützen und
- einen Beitrag zu sinnvollem Mitteleinsatz in der öffentlich geförderten medizinischen Forschung zu leisten, indem sie Doppelentwicklungen zu vermeiden hilft und die Wiederverwendung vorhandener Lösungen organisiert.

Mit ihren Lösungen adressiert die TMF vor allem die nicht-kommerzielle, akademische – universitäre wie außeruniversitäre – Forschung in Deutschland. Unabhängig davon ist aber auch ein steigendes Interesse an den Angeboten aus der Industrie zu verzeichnen. Viele Lösungen der TMF sind zudem auch für das Ausland, insbesondere die deutschsprachigen Länder, relevant und werden in dortigen Forschungseinrichtungen bereits genutzt.

Alle Download-geeigneten Produkte und Ergebnisse stehen auf der TMF-Website zur Verfügung. Einzelne Software-Werkzeuge sind sehr komplex und bedürfen einer individuellen Anpassung und Erläuterung, so dass sie nur über den direkten Kontakt zur TMF-Geschäftsstelle erhältlich sind, die dann auch für die Betreuung bei der Implementierung und Nutzung des Produktes sorgt. Darüber hinaus fließen die Ergebnisse kontinuierlich auch in die Diskussionen in den Arbeits- und Projektgruppen ein, und sie werden in konkreten Beratungsgesprächen sowie in Schulungs- und Informationsveranstaltungen vermittelt.

TMF-Schriftenreihe

Wichtige Konzepte, Leitfäden und Hilfstexte veröffentlicht die TMF in ihrer Schriftenreihe, die sie seit mehreren Jahren bei der Medizinisch Wissenschaftlichen Verlagsgesellschaft herausgibt. So erschienen 2006 als erster Band die generischen Lösungen zum Datenschutz für die Forschungsnetze in Buchform (Reng et al.: Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, Berlin 2006 – Bd. 1). In der Zwischenzeit sind diese Konzepte einer grundlegenden Revision unterzogen und erneut mit den Bundes- und Landesdatenschützern abgestimmt worden. Die überarbeiteten Konzepte sind als Band 11 der TMF-Schriftenreihe für einen breiten Nutzerkreis verfügbar gemacht worden (Pommerening et al.: Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, Berlin 2014 – Bd. 11).

2015 erschien als Band 12 das Rechtsgutachten zur Sekundärnutzung klinischer Daten in Buchform. Forschung und Qualitätssicherung in der Medizin greifen zunehmend auf Daten aus der Versorgung zurück. Die rechtlichen Grundlagen hierfür sind jedoch sehr komplex und können sich unter anderem nach Standort und Trägerschaft der Einrichtung sowie nach dem Forschungszweck deutlich unterscheiden. Das Rechtsgutachten, das um ein Online-Suchwerkzeug ergänzt wurde, bietet hier eine Hilfestellung, mit der die jeweils relevanten rechtlichen Vorschriften schnell gefunden werden können.

Bereits 2006 erschien ein Rechtsgutachten zum Aufbau und Betrieb von Biomaterialbanken (Simon et al.: Biomaterialbanken – Rechtliche Rahmenbedingungen, Berlin 2006 – Bd. 2), das im Februar 2008 um einen weiteren Band zum Thema Qualitätssicherung von Biobanken ergänzt wurde (Kiehntopf/Böer: Biomaterialbanken – Checkliste zur Qualitätssicherung, Berlin 2008 – Bd. 5). Das Datenschutzkonzept, das ursprünglich als Band 6 der Schriftenreihe publiziert werden sollte, ist in die vorliegende Publikation der neuen Datenschutzkonzepte integriert worden.

Mit der Checkliste zur Patienteneinwilligung legte die TMF Ende 2006 ein Referenzwerk vor, das den Anwendern ermöglicht, auf der Basis von relevanten, dokumentierten und kommentierten Quellen Patienteninformationen und Einwilligungserklärungen für klinische Studien zu erstellen, die den regulatorischen Anforderungen entsprechen (Harnischmacher et al.: Checkliste und Leitfaden zur Patienteneinwilligung, Berlin 2006 – Bd. 3). Wie die meisten anderen Buchpublikationen auch, wird dieser Band durch weitere online verfügbare Materialien (z.B. Musterverträge) oder Services ergänzt.

2007 erschien die erste Auflage der Leitlinie zur Datenqualität in der medizinischen Forschung, die 2014 in einer aktualisierten und ergänzten Fassung neu aufgelegt worden ist. Die Leitlinie (Nonnemacher et al.: Datenqualität in der medizinischen Forschung, Berlin 2014 – Bd. 4) enthält Empfehlungen zum Management von Datenqualität in Registern, Kohortenstudien und Data Repositories.

Ein Rechtsgutachten zum Problemfeld der Verwertungsrechte in der medizinischen Forschung (Goebel/Scheller: Verwertungsrechte in der medizinischen Forschung, Berlin 2008 – Bd. 7) erschien 2008 als erste Veröffentlichung einer Reihe von Rechtsgutachten, die die TMF zu verschiedenen Fragen erstellen ließ, unter anderem zum Thema „elektronische Archivierung von Studienunterlagen".

Mit Band 8 (Mildner [Hrsg.]: Regulatorische Anforderungen an Medizinprodukte, Berlin 2011 – Bd. 8) hat die TMF 2011 erneut die Aufarbeitung eines im Umbruch befindlichen Feldes vorgelegt. Das Buch bietet eine Einführung in den regulatorischen Prozess bei der Entwicklung von Medizinprodukten und stellt Handlungshilfen bereit. Dabei wird der gesamte Bereich von der klinischen Bewertung bis zum Health Technology Assessment abgedeckt.

Praktische Empfehlungen für die Verarbeitung und Analyse von Daten, die bei der Hochdurchsatz-Genotypisierung anfallen, gibt Band 9 (Krawczak/Freudigmann [Hrsg.]: Qualitätsmanagement von Hochdurchsatz-Genotypisierungsdaten, Berlin 2011 – Bd. 9), der ebenfalls 2011 publiziert werden konnte. Dabei reichen die behandelten Fragen von Problemen der Validität und Plausibilität über die Erkennung und Vermeidung von Fehlern bis hin zu Anforderungen an Datenhaltung und Datentransfer.

An die TMF-Ergebnisse im Bereich Datenschutz und Patienteneinwilligung knüpft der 2012 erschienene Band 10 an (Goebel/Scheller: Einwilligungserklärung und Forschungsinformation zur Gewinnung tierischer Proben, Berlin 2012 – Bd. 10). Die Ergebnisse sind im Auftrag der Nationalen Forschungsplattform für Zoonosen erarbeitet worden. Sie dienen dazu, Forschenden Rechtssicherheit bei der Entnahme und Bearbeitung von Tierproben zu geben und sie bei der Erstellung der relevanten Einwilligungsunterlagen zu unterstützen.

Mit dem Sammelband zu Terminologien und Ordnungssystemen in der Medizin, der 2015 als Band 13 der Schriftenreihe erschien, hat die TMF eine aktuelle Bestandsaufnahme vorgelegt, die den aktuellen Stand der Nutzung medizinischer Terminologien zusammenfasst und Empfehlungen gibt, um einen internationalen Austausch von Informationen in der Medizin zu gewährleisten.

Band 14 mit dem Titel „Gesundheitsforschung kommunizieren, Stakeholder Engagement gestalten" legt den Fokus auf einen Aspekt, dessen Bedeutung in der wissenschaftlichen Community erst in der jüngeren Zeit zunehmend anerkannt und be-

achtet wird. Dies geht einher mit einer zunehmenden Professionalisierung in der Arbeit der Kommunikationsverantwortlichen, zu der das Buch einen Beitrag leisten möchte.

Band 16 bewertet die aktuellen Möglichkeiten für den Einsatz von Big Data im Gesundheitswesen und zeigt gleichzeitig Hürden und Risiken auf. Daraus abgeleitet werden Handlungsempfehlungen für eine bessere Nutzung von Gesundheitsdaten für die Patientenversorgung gegeben. Diese wurden in einem Workshop mit Akteuren aus den Bereichen Gesundheitsversorgung, klinische Forschung, Datenschutz, Data Science, Statistik, Industrie und Politik erarbeitet.

Band 17 bietet einen Überblick über den aktuellen Rechtsrahmen zur Nutzung von Sozial- und Gesundheitsdaten für die Forschung. Im ersten Teil wird der sozialrechtliche Rahmen zur Nutzung von Sozialdaten für die Forschung dargelegt. Im zweiten Teil wird ein Überblick zum Umgang mit Forschungsdaten nach Anwendung der DSGVO und entsprechender nationaler Anpassungen des Rechtsrahmens gegeben.

Band 18 verdeutlicht, wie Datenverarbeitung nach Inkrafttreten der EU-DSGVO 2018 in internationalen Kooperationsprojekten in der medizinischen Forschung ausgestaltet sein muss.

Mit dem vorliegenden Band 19 wird ein Rechtsgutachten veröffentlicht, das den datenschutzrechtlichen Rahmen der medizinischen Forschung umfassend darstellt. Dabei wird darauf eingegangen, wie praktikabel die aktuellen Regelungen sind und inwiefern sie medizinische Forschungsvorhaben sowie die Umsetzung des Persönlichkeitsschutzes ermöglichen.

Weitere Informationen und Kontakt

TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.
Charlottenstraße 42/Ecke Dorotheenstraße
10117 Berlin
Tel.: 030 – 22 00 24 7–0
Fax: 030 – 22 00 24 7–99
E-Mail: info@tmf-ev.de
Internet: www.tmf-ev.de

Stichwortregister

W

Z

Zur Schriftenreihe der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

In der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. arbeiten Netzwerke und vernetzt arbeitende Einrichtungen gemeinsam daran, die Fragestellungen und Herausforderungen von medizinischer Forschung an verteilten Standorten zu lösen, ihre Erfahrungen zu bündeln und damit zu mehr Transparenz und Effizienz im Gesundheitswesen beizutragen. Durch den Community-Ansatz erfahren die Ergebnisse der TMF eine breite inhaltliche Abstimmung in der medizinischen und medizininformatisch-biometrischen Fachwelt. Mit ihrer Schriftenreihe macht die TMF die Lösungen einer breiteren Leserschaft zugänglich.

Bisher in der Schriftenreihe erschienen:

Band 1:
Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin
von Carl-Michael Reng | Peter Debold
Christof Specker | Klaus Pommerening
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 2:
Biomaterialbanken – Rechtliche Rahmenbedingungen
von Jürgen Simon | Rainer Paslack | Jürgen Robienski
Jürgen W. Goebel | Michael Krawczak
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 3:
Checkliste und Leitfaden zur Patienteneinwilligung Grundlagen und Anleitung für die klinische Forschung
von Urs Harnischmacher | Peter Ihle | Bettina Berger
Jürgen Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006

Band 4:
Datenqualität in der medizinischen Forschung
von Michael Nonnemacher | Dorothea Weiland
Jürgen Stausberg
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2007

Band 4, 2. Auflage:
Datenqualität in der medizinischen Forschung
von Michael Nonnemacher | Daniel Nasseh | Jürgen Stausberg
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2014

Band 5:
Biomaterialbanken – Checkliste zur Qualitätssicherung
von Michael Kiehntopf | Klas Böer
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2008

Band 7:
Verwertungsrechte in der vernetzten medizinischen Forschung
von Jürgen W. Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2009

Band 8:
Regulatorische Anforderungen an Medizinprodukte
von Kurt Becker | Sandra Börger | Horst Frankenberger
Dagmar Lühmann | Thomas Norgall
Christian Ohmann | Annika Ranke | Reinhard Vonthein
Andreas Ziegler | Andreas Zimolong
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2011

Band 9:
Qualitätsmanagement von Hochdurchsatz-Genotypisierungsdaten
von Michael Krawczak | Mathias Freudigmann (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2011

Band 10:
Einwilligungserklärung und Forschungsinformation zur Gewinnung tierischer Proben
von Jürgen W. Goebel | Jürgen Scheller
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2012

Band 11:
Leitfaden zum Datenschutz in medizinischen Forschungsprojekten
von Klaus Pommerening | Johannes Drepper
Krister Helbing | Thomas Ganslandt
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2014

Band 12:
Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen
von Uwe K. Schneider
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015

Band 13:
Terminologien und Ordnungssysteme in der Medizin
von Otto Rienhoff | Sebastian C. Semler (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015

Band 14:
Gesundheitsforschung kommunizieren, Stakeholder Engagement gestalten
von Wiebke Lesch | Antje Schütt (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2016

Band 16:
Big Data im deutschen Gesundheitswesen – Handlungsempfehlungen
von Sebastian C. Semler | Karoline Buckow (Hrsg.)
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2019

Band 17:
Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen
von C. Dierks | A. Roßnagel
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2019

Band 18:
Data Privacy in European Medical Research: A Contemporary Legal Opinion
von C. Dierks | P. Kircher | C. Husemann
J. Kleinschmidt | M. Haase
MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2021