Schriftenreihe der TMF

C. Dierks | A. Roßnagel

Sekundärnutzung von Sozial- und Gesundheitsdaten

Rechtliche Rahmenbedingungen

Medizinisch Wissenschaftliche Verlagsgesellschaft

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

Band 17

Medizinisch Wissenschaftliche Verlagsgesellschaft

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

Band 17

C. Dierks | A. Roßnagel

Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen

Medizinisch Wissenschaftliche Verlagsgesellschaft

Die Autoren

Rechtsanwalt Prof. Dr. med. Dr. iur. Christian Dierks
Dierks+Company
HELIX HUB
Invalidenstraße 113
10115 Berlin

Unter Mitarbeit von
Rechtsanwalt Dr. iur. Philipp Kircher
Rechtsanwältin Dr. iur. Sabrina Neuendorf
Rechtsanwältin Taisija Taksijan, LL.M.

Prof. Dr. iur. Alexander Roßnagel
Universität Kassel
Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)
Pfannkuchstr. 1
34121 Kassel

Unter Mitarbeit von
Dr. iur. Christian Geminn

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

ISBN 978-3-95466-518-1 (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: Anna-Lena Spies, Berlin
Lekorat: 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

Mit Fragen des Datenschutzes in der vernetzten biomedizinischen Forschung beschäftigt sich die TMF schon seit ihrer Gründung im Jahr 1999. Knapp 20 Jahre später steht die biomedizinische Forschung in Deutschland vor zwei großen Herausforderungen, die auch den Hintergrund der vorliegenden Publikation bilden: zum einen die beschleunigte Digitalisierung im Gesundheitswesen, mit den daraus resultierenden Chancen und Risiken für Versorgung und Forschung, zum anderen die notwendige Anpassung der IT-Verfahren und -Infrastrukturen in der Medizin an den umfassend geänderten Rechtsrahmen des Datenschutzes – von der EU-Datenschutzgrundverordnung (DSGVO) bis zu nationalen Anpassungs- und Umsetzungsgesetzen (z.B. Bundesdatenschutzgesetz[1], Sozialgesetzbuch X[2]).

Mit der vorliegenden Veröffentlichung im Rahmen ihrer Schriftenreihe stellt die TMF der Öffentlichkeit zwei diesbezüglich von ihr beauftragte Rechtsgutachten zur Verfügung. Darin untersuchen auf diesem Gebiet führende juristische Experten in Deutschland, Prof. Dr. Dr. Christian Dierks und Prof. Dr. Alexander Roßnagel, aktuelle und komplexe Rechtsfragen zur Nutzung von Krankenkassen- und weiteren Gesundheitsdaten. Mit der Publikation der Ergebnisse setzt die TMF ihre Tradition fort, aktuelle rechtliche Fragen aus der medizinischen Forschung fundiert juristisch klären und aufbereiten zu lassen.

Anlass für die Erstellung der Gutachten war das Projekt „Smart Analysis – Health Research Access“ (SAHRA, 2015-2018), das vom Bundeswirtschaftsministerium im Rahmen des Technologieprogramms „Smart Data – Innovationen aus Daten“ gefördert wurde. SAHRA hatte das Ziel, eine technische Infrastruktur für die rechtskonforme Verknüpfung von Daten der gesetzlichen Krankenversicherung mit weiteren Behandlungs- und Forschungsdaten zu schaffen, um sie so interessierten Akteuren in Forschung und Gesundheitswesen zur Verfügung stellen zu können. Kernanliegen des Projekts war der Aufbau einer Datenplattform, die unterschiedlichen Nutzern (z.B. Forschern, öffentlichen Einrichtungen und der Gesundheitswirtschaft) unter strengen Bedingungen Zugang zu den anonymen Ergebnissen von Auswertungen der Daten ermöglicht. Die Konsortialführung des SAHRA-Projekts lag beim Gesundheitswissenschaftlichen Institut Nordost (GeWINO) der AOK Nordost; als technische Projektpartner waren das Hasso-Plattner-Institut (HPI) und die data experts

1 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44.

2 Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 49.

GmbH eingebunden. Bis zum Ende der Projektlaufzeit wurde die SAHRA-Plattform für drei verschiedene Anwendungsfälle genutzt.[3]

Die TMF hatte im Arbeitspaket „Datenschutz und Rechtssicherheit" des SAHRA-Projekts die Aufgabe, die vielfältigen datenschutzrechtlichen Fragen bezüglich einer Nutzung von Sozial- und Gesundheitsdaten zu prüfen und aufzuarbeiten. Im Zuge dessen ist ein Fragenkatalog entstanden, der nicht nur auf die Besonderheiten einer Nutzung von Sozialdaten auf langfristig angelegten Forschungsplattformen eingeht, sondern auch allgemeinere, für die medizinische Forschung relevante Aspekte der Auslegung der DSGVO und der deutschen Anpassungsgesetze beinhaltet. Einige Anregungen zur Verbesserung der Übermittlungsgrundlage von Sozialdaten für die Forschung (z.B. geregelt in § 75 Sozialgesetzbuch X) sind im Gesetzgebungsverfahren aufgegriffen worden und haben Eingang in die reformierte Fassung der Norm[4] gefunden.

Der den Rechtsgutachten zugrunde liegende Fragenkatalog wurde seitens der TMF von Valérie Kempter und Dr. Johannes Drepper erarbeitet und anschließend mit den SAHRA-Projektpartnern sowie mit den Forschungsvertretern und Experten der AG Datenschutz der TMF eingehend abgestimmt.

Das Gutachten von Rechtsanwalt Prof. Dr. Dr. Christian Dierks (Teil I) wurde Ende 2018 fertiggestellt und enthält letzte Anpassungen an den Gesetzentwurf der Bundesregierung zum 2. Datenschutzanpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU[5]). Das Gutachten von Prof. Dr. Alexander Roßnagel (Teil II) berücksichtigt den Stand der Gesetzgebung bis zum 31. März 2018.

Für das Gutachten von Prof. Dr. Dr. Dierks zum Umgang mit den Abrechnungsdaten gesetzlicher Krankenversicherungen wurden die drei unten zusammengefassten Szenarien entwickelt, die eine Nutzung der Daten in mehr oder weniger enger Kooperation mit den Kassen beschreiben. Hinsichtlich der praktischen Umsetzung einer Datennutzung mit bzw. ohne Einwilligung der betroffenen Patienten war für alle drei Szenarien der jeweilige Rechtsrahmen zu untersuchen und detailliert zu beschreiben.

1. Die Datennutzung erfolgt im Rahmen eines Kooperationsprojekts einer gesetzlichen Krankenversicherung mit einem externen Partner. Die Fragestellung für die Datenauswertung wird gemeinsam entwickelt oder vom externen Partner vorgegeben. Die Sozialdaten bleiben in der Einrichtung der gesetzlichen Krankenversicherung und werden hier ausgewertet. Lediglich anonyme Auswertungsergebnisse werden an den externen Partner übermittelt, es verlassen keine Sozialdaten die Einrichtung der gesetzlichen Krankenversicherung.

3 https://www.sahra-plattform.de/

4 Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 49.

5 Gesetzentwurf der Bundesregierung, BT Drucksache 19/4674, 1.10.2018, http://dipbt.bundestag.de/dip21/btd/19/046/1904674.pdf

2. Auch hier kooperieren eine gesetzliche Krankenversicherung und eine externe Einrichtung. Die Sozialdaten werden für ein bestimmtes Vorhaben an die externe Einrichtung übermittelt, die diese im Sinne des Vorhabens verarbeitet und auswertet.
3. In diesem Szenario werden Sozialdaten von einer oder mehreren Einrichtungen der gesetzlichen Krankenversicherung für übergeordnete Zwecke (z.B. medizinische Forschung oder Qualitätssicherungsaspekte) an eine externe Einrichtung (Datenplattform) übermittelt. Die externe Einrichtung wiederum stellt die Sozialdaten für bestimmte Vorhaben Dritten zur Verfügung, entweder in Form einer weiteren Übermittlung oder durch die Herausgabe anonymer Auswertungsergebnisse zu konkreten Fragestellungen.

Die deutsche Gesundheitsgesetzgebung hat sich in den letzten Jahren deutlich dynamisiert. Davon ist auch das hier untersuchte Regelungsgebiet der Nachnutzung von Versichertendaten der GKV betroffen. Prof. Dr. Dr. Dierks wurde daher gebeten, seiner Analyse eine aktualisierte Bewertung des Rechtsrahmens anzuhängen und Vorschläge für dessen Weiterentwicklung zu formulieren. Dieser Teil des Gutachtens kann daher auch als Argumentationshilfe im politischen Raum dienen, wenn es zukünftig darum geht, die datengetriebene biomedizinische Forschung in Deutschland rechtssicher und transparent auszugestalten.

Im zweiten Gutachten des vorliegenden Bandes prüfte Prof. Dr. Roßnagel grundlegende forschungsrelevante Fragen, die sich aus der Anwendung der DSGVO und der daran angepassten Bundesgesetze (wie z.B. dem Bundesdatenschutzgesetz) sowie weiterer gesetzlicher Neuerungen (z.B. zur ärztlichen Schweigepflicht) ergeben. Dabei ging es u.a. um die Abgrenzung der Begriffe „Pseudonymisierung" und „Anonymisierung" sowie um das Verhältnis der Löschpflicht zur Anonymisierung. Daneben thematisiert das Gutachten die Auslegung des Begriffs der gemäß DSGVO privilegierten „wissenschaftlichen Forschungszwecke" und den Umfang ihrer Privilegierung, z.B. bezüglich Auskunftsrechte und Löschpflichten. Und schließlich geht das Gutachten von Prof. Dr. Roßnagel auch auf die ärztliche Schweigepflicht ein und untersucht, inwiefern sich die in § 203 Strafgesetzbuch neu eingeführte „Mitwirkung" auf den Forschungskontext ausdehnen lässt.

Beide Gutachten wurden einem externen Review unterzogen, das von Rechtsanwalt Prof. Dr. Niko Härting (Härting Rechtsanwälte PartGmbH) unter Mitwirkung von Patrick Gössling (für Teil II) bzw. Prof. Dr. Alexander Roßnagel (für Teil I) sowie von Mitarbeitern der TMF-Geschäftsstelle (Dr. Johannes Drepper, Valérie Kempter, Sebastian Straub, Tim Schneider, Irene Schlünder), durchgeführt wurde. Am 16.01.2018 fand in der TMF-Geschäftsstelle zudem ein Workshop statt, bei dem die Fragestellungen und wesentlichen Ergebnisse der Gutachten von den Autoren und Reviewern mit dem Sprecher der AG Datenschutz der TMF, Prof. Dr. Klaus Pommerening, und Mitarbeitern der

Geschäftsstelle der TMF diskutiert wurden. Workshop und Review haben substantiell zur Abrundung der Gutachten beigetragen.

Der Dank der TMF gilt allen, die in der einen oder anderen Form zum vorliegenden Band beigetragen haben, insbesondere den beiden Gutachtern, Prof. Dr. Dr. Dierks und Prof. Dr. Roßnagel, für ihre sehr umfassende und systematische Arbeit. Großer Dank gebührt zudem Dr. Philipp Kircher, Dr. Sabrina Neuendorf, Taisija Taksijan und Dr. Christian Geminn für ihre fachliche Unterstützung der Gutachter. Ohne ihre Hilfe wäre die Erstellung der Gutachten in der kurzen, dafür zur Verfügung stehenden Zeit nicht möglich gewesen. Den Partnern aus dem SAHRA-Projekt sowie den Mitarbeitern der TMF-Geschäftsstelle ist für die Entwicklung und Abstimmung des vorangegangenen Pflichtenhefts sowie für die Begleitung des Projekts zu danken, ebenso allen Teilnehmern des Workshops für die konstruktive und detaillierte Diskussion und den Review-Teams für die ausführliche und hilfreiche Kommentierung der Texte. Für die umfangreiche redaktionelle Arbeit gilt neben den bereits genannten Mitarbeitern der TMF-Geschäftsstelle insbesondere Sophie Haderer großer Dank.

Die TMF freut sich, beide Gutachten nun im Rahmen ihrer Schriftenreihe allen an der datenschutzkonformen Nachnutzung von Sozial- und Gesundheitsdaten Interessierten in Buchform zur Verfügung stellen zu können – und zwar nicht nur auf Papier, sondern parallel (wie die gesamte TMF-Schriftenreihe bei der Medizinisch Wissenschaftlichen Verlagsgesellschaft ab 2019) auch als *open access* E-Book.

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

Sebastian Claudius Semler
(Geschäftsführer)

Prof. Dr. Michael Krawczak
(Vorstandsvorsitzender)

Inhalt

Rechtsgutachten zur Nutzung von Sozial- und Gesundheitsdaten (SAHRA-Projekt)

RA Prof. Dr. med. Dr. iur. Christian Dierks
Unter Mitarbeit von RA Dr. iur. Philipp Kircher,
RA'in Dr. iur. Sabrina Neuendorf und
RA'in Taisija Taksijan, LL.M., Fachanwältin für Medizinrecht

erstellt am 23.09.2017, überarbeitet zum 19.10.2018

1 Bewertung der Rechtslage ab 25.05.2018

1.1 Einleitung

Das Bundesministerium für Wirtschaft und Energie (BMWi) fördert das Projekt „Smart Analysis – Health Research Access" (SAHRA) der AOK Nordost. Über die webbasierte SAHRA-Plattform sollen Sozialdaten der AOK Nordost kombiniert, referenziert und validiert und schließlich zugunsten von Wissenschaft, Versorgung und Industrie verwendet werden.

Die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) hat im Rahmen des SAHRA-Projekts im Mai 2017 den Auftrag für ein Rechtsgutachten zur Nutzung von Sozial- und Gesundheitsdaten ausgeschrieben.

Das vorliegende Gutachten wurde ursprünglich zum 23.09.2017 eingereicht und beachtete die bis dahin bekannten Reformvorhaben. Punktuelle Änderungen redaktioneller Art wurden bis 18.12.2017 vorgenommen. Vor dem Hintergrund anhaltender datenschutzrechtlicher Reformen, insbesondere in den für dieses Gutachten maßgeblichen fachspezifischen Bereichen der Gesetzlichen Krankenversicherung, wie sie im Sozialgesetzbuch Fünftes Buch (SGB V) verankert sind, wurde nunmehr eine Aktualisierung bis zum 19.10.2018 vorgenommen. Trotz der zwischenzeitlichen Geltungserlangung der Datenschutz-Grundverordnung (DSGVO) und des Inkrafttretens des neuen BDSG sowie des neuen Sozialdatenschutzrechts nach § 35 SGB I i.V.m. §§ 67ff. SGB X

sind die Reformen des SGB V zur Anpassung an die DSGVO bei Redaktionsschluss nicht abgeschlossen.

Die Autoren bedauern diesen Umstand, hoffen mit der aktuellen Bearbeitung jedoch den Entwicklungen angemessen Rechnung tragen zu können.

1.1.1 Problemstellung und Zielsetzung

Forschungsprojekte, Qualitätssicherungsanalysen, Planungsvorhaben und sonstige statistische Auswertungen, die auf der Verarbeitung personenbezogener Daten basieren, unterliegen den Beschränkungen des Datenschutzrechts. Handelt es sich bei den Datensätzen um solche, die sensible Daten, wie etwa Gesundheitsdaten oder Sozialdaten, umfassen, so bestehen besonders hohe Hürden. Während das Datenschutzrecht durch ein Verbot mit Zulässigkeitsvorbehalt und das Gebot der Zweckbindung die Verwendung personenbezogener Daten auf ein unerlässliches Maß reduzieren möchte, ist Forschung zunehmend von der Verfügbarkeit und Validität umfassender Datenbestände abhängig. Diesem Bedürfnis liegt unter anderem eine Veränderung methodischer Forschungsansätze zugrunde. So erfordern insbesondere explorative Datenanalysen im Bereich des sog. Big Data große Datenvorräte, die nicht erst nach Formulierung einer konkreten, im Rahmen eines Forschungsprojekts zu untersuchenden These zielgerichtet erhoben werden können. Aber auch im Bereich der klassischen Forschungsvorhaben wirkt das Datenschutzrecht als ein Hemmnis. Dieses besteht aber nicht im Wesentlichen in den Anforderungen zum Schutz der betroffenen Personen, sondern in der Inkompatibilität paralleler Datenschutzgesetze auf Bundes- und Landesebene und der sektoralen Begrenzung bereichsspezifischen Datenschutzrechts.

Mit der Datenschutz-Grundverordnung (DSGVO)[1] war eine weitgehende Vollharmonisierung des Datenschutzrechts in der Europäischen Union beabsichtigt. Im Verordnungstext sowie in den Erwägungsgründen ist ein forschungsfreundlicheres Grundverständnis angelegt. Gleichzeitig beinhaltet die DSGVO Öffnungsklauseln, die sowohl hinsichtlich ihrer Zahl als auch ihres Umfangs weitgehende Regelungen durch die Mitgliedsstaaten ermöglichen oder erfordern, ohne dabei von den wesentlichen Grundsätzen der DSGVO abzuweichen. Im Spannungsfeld der Intention der DSGVO und dem sich abzeichnenden Bestreben des Bundesgesetzgebers, das bestehende Datenschutzrecht weitgehend aufrechtzuerhalten, stellt sich die Frage nach einer rechtssicheren Ausgestaltung vernetzter Forschung sowie nach Qualitätssicherungs- und Planungsmechanismen, wie sie mit der SAHRA-Plattform beabsichtigt sind.

1 Hierzu siehe Kap. 1.1.1.

1.1.2 Gang der Untersuchung

Die TMF hat als Auftraggeber des vorliegenden Gutachtens ein Pflichtenheft erstellt, das konkrete Fragen enthält. Das vorliegende Gutachten umfasst die Ausarbeitung der im Pflichtenheft als „Los 1" zusammengefassten Kapitel I–III. „Los 2", das Kapitel IV des Pflichtenhefts umfasst, wird anderweitig bearbeitet.

Die Fragen zu Los 1 beziehen sich weitgehend auf drei Sachverhaltsgestaltungen (Szenarien), anhand derer die künftige Rechtslage nach bisher bekanntem Gesetzgebungsstand zur zukünftigen Rechtslage (Kapitel I) und dem aktuellen rechtlichen Status quo (Kapitel II) untersucht werden sollen. Im Anschluss sind Reformüberlegungen anzustellen (Kapitel III). Diese Gliederung weicht insofern von den Vorgaben des Pflichtenheftes ab, als die künftige Rechtslage nunmehr in Kapitel I und nicht in Kapitel II dargestellt werden soll, was der besseren Lesbarkeit geschuldet ist. Dieses Vorgehen wurde im Rahmen der Vorgespräche zur Vergabe des Gutachtens mit dem Auftraggeber abgestimmt.

1.1.3 Stand der Gesetzgebung

Das Gutachten wird zu einem Zeitpunkt anhaltender Reformen des Datenschutzrechts erstellt. Auftraggeber und Gutachter haben sich darauf geeinigt, die reformierte Rechtslage bis zum 19. Oktober 2018 zu berücksichtigen, soweit mindestens öffentlich einsehbare Gesetzentwürfe als parlamentarische Drucksachen vorliegen. Der Stand der Reformen gestaltet sich wie folgt:

1.1.3.1 Bereits geltende Rechtslage

Die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)"[2] (**DSGVO**) wurde am 04. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht und trat am 24. Mai 2016 in Kraft. Sie ist seit dem 25. Mai 2018 in allen Mitgliedsstaaten unmittelbar anwendbar.

Der deutsche Bundesgesetzgeber ist in der Zwischenzeit tätig geworden und hat die Anpassung sowohl des allgemeinen Datenschutzrechts in Form des Bundesdatenschutzgesetzes (**BDSG**) als auch des allgemeinen Teils des bereichsspezifischen Datenschutzrechts des Sozialgesetzbuchs, der als Sozialdatenschutzrecht in **§ 35 SGB I i.V.m. §§ 67ff. SGB X** geregelt ist, vorgenommen; die

2 Abl. L 119 vom 04.05.2016, 1; korrigiert durch Abl. L 314 vom 22.11.2016, 72.

Änderungen sind gleichzeitig mit der Wirkungserlangung der DSGVO zum 25.05.2018 in Kraft getreten.[3]

Das BDSG a.F. ist mit dem „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)" vom 30. Juni 2017[4] von einem neuen Bundesdatenschutzgesetz (**BDSG**) abgelöst worden (vgl. Art. 8 DSAnpUG-EU).

In vergleichbarer Weise ist mit dem „Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften" vom 17. Juli 2017[5] auch das sog. **Sozialdatenschutzrecht** (§ 35 **SGB I** a.F. i.V.m. §§ 67ff. **SGB X** a.F.) umfassend neu geregelt (vgl. Art. 19 und Art. 23 des Gesetzes) worden.

Parallel zu den vorgenannten Gesetzgebungsvorhaben zur Anpassung der Rechtslage an die DSGVO hat der Bundestag die Änderung der Schweigepflichten von Berufsgeheimnisträgern beschlossen. Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen" vom 30.10.2017[6] wurde die **Schweigepflicht aus § 203 StGB** dahingehend geändert, dass die Beteiligung von „sonstigen Mitwirkenden" ermöglicht wird, was insbesondere im Bereich des Outsourcings und der Auftrags(daten)verarbeitung neue Handlungsoptionen der Berufsgeheimnisträger schaffen soll.

1.1.3.2 Ausstehende Änderungen und Gesetzesentwürfe

Änderungen weiterer bereichsspezifischer Datenschutzgesetze stehen zum Zeitpunkt der Erstellung dieses Gutachtens noch aus. Es besteht daher eine rechtliche Ungewissheit, die mit Blick auf das vorliegende Gutachten insbesondere die datenschutzrechtlichen Regelungen des SGB V betrifft.

1.1.3.2.1 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU (Entwurf)

Der Gesetzentwurf eines Zweiten Gesetzes 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)[7] enthält umfangreiche Änderungen diverser datenschutz-

3 Weiterhin wurde das allgemeine Landesdatenschutzrecht in den jeweiligen Landesdatenschutzgesetzen aller 16 Bundesländer an die DS-GVO angepasst. Das bereichsspezifische Landesdatenschutzrecht ist noch nicht vollständig überarbeitet. Landesdatenschutzrecht kann für die vorliegende Begutachtung aber außer Betracht bleiben.

4 BGBl. I 2017, 2097.

5 BGBl. I 2017, 2541.

6 BGBl. I 2017, 3618.

7 Gesetzentwurf der Bundesregierung Entwurf eines Zweiten Gesetzes 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), BR-Drs. 430/18; vgl. BT-Drs. 19/4674.

rechtlicher Normen, insbesondere solcher des BDSG, SGB I, SGB V und SGB X. Zum Zeitpunkt der Begutachtung lag der Kabinettsentwurf dem Bundesrat zur Beratung vor und die Ausschüsse hatten bereits ihre Empfehlungen[8] abgegeben. Der diesbezügliche Beschluss des Bundesrates vom 19.10.2018[9] sieht keine Änderung des Entwurfs für die hier in Betracht kommenden Regelungsbereiche des BDSG oder der bereichsspezifischen Normen des SGB I, SGB V oder SGB X vor. Der Gesetzentwurf enthält im Wesentlichen sprachliche Anpassungen an die DSGVO. Die Begriffe „erheben", „nutzen" und „verarbeiten" sollen regelmäßig durch den umfassenderen Begriff „verarbeiten" im Sinne der DSGVO ersetzt werden, ohne damit aber inhaltliche Änderungen zu veranlassen. Weiterhin sollen etwa bisher streng formulierte Schriftformerfordernisse für datenschutzrechtliche Einwilligungen im SGB V dahingehend gelockert werden, dass auch elektronische Einwilligungen zulässig sein sollen.

Während § 67b Abs. 2 SGB X bislang lediglich eine Soll-Vorschrift beinhaltet, wonach zu Nachweiszwecken nach Art. 7 DSGVO eine Einwilligung in die Verarbeitung von personenbezogenen Daten schriftlich oder elektronisch erfolgen „soll", dies gleichwohl keine Wirksamkeitsvoraussetzung für eine Einwilligung ist, wird nun vorgeschlagen, durch einen neuen Satz 2 zu regeln, dass Einwilligungen zur Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (oder Betriebs- und Geschäftsgeheimnissen) zwingend schriftlich oder elektronisch zu erfolgen haben, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Aus der Begründung des Gesetzentwurfs ergibt sich, dass es sich hierbei nicht nur um ein Nachweiserfordernis, sondern um ein Wirksamkeitserfordernis handelt: Unter Bezugnahme auf die Öffnungsklausel des Art. 9 Abs. 4 DSGVO wird nur für die vorgenannten Datenkategorien eine strengere Form verlangt, was dazu dienen soll, das Schutzniveau der Altregelung des § 67b Abs. 2 S. 2 SGB X a.F. im zulässigen Umfang zu erhalten.[10] Gleichzeitig sieht der Gesetzentwurf vor, dass in § 67b Abs. 3 SGB X für Verarbeitungen zu Forschungszwecken geregelt werden soll, dass ein besonderer Umstand, unter dem ein Abweichen von der vorgenannten Formvorgabe möglich ist, dann vorliege, wenn durch die Einholung einer schriftlichen oder elektronischen Einwilligung der Forschungszweck erheblich beeinträchtigt würde. Die Gründe hierfür sollen schriftlich festgehalten werden. Die vorgeschlagenen Regelungen sind zwar europarechtlich zulässig, sie führen jedoch zu zusätzlichen Hindernissen und ggf. zu weiterem Begründungsaufwand. Auf weitere Änderungen im SGB X wird an den entsprechenden Stellen des Gutachtens hingewiesen, sofern sich hieraus nach bisheriger Einschätzung relevante Änderungen ergeben können.

Die daneben bestehenden Änderungen des SGB V spielen für das vorliegende Gutachten nach bisherigem Erkenntnisstand hingegen keine Rolle. Sie

8 BR-Drs. 430/1/18.
9 BR-Drs. 430/18(B), Beschlussdrucksache.
10 BT-Drs. 19/4674, S. 400.

betreffen etwa die Streichung der Pflicht zur Löschung von personenbezogenen Daten nach Zweckerreichung gem. § 284 Abs. 1 S. 4 und Abs. 4 S. 4 SGB V, die jedoch wegen der unmittelbaren Geltung von Art. 5 Abs. 1 lit. e) und Art. 17 Abs. 1 lit. a) DSGVO nicht zu einer inhaltlichen Änderung führt.[11] Zentrale forschungsrelevante Vorschriften (wie § 287 SGB V) sollen nicht geändert werden.

1.1.3.2.2 Terminservice- und Versorgungsgesetz – TSVG (Entwurf)

Der Entwurf eines Gesetzes für schnellere Termine und bessere Versorgung (Terminservice- und Versorgungsgesetz – TSVG) hat am 26.09.2018 das Kabinett passiert und liegt zum Zeitpunkt des Redaktionsschlusses entsprechend nur als Kabinettsentwurf vor. Der Gesetzentwurf enthält umfangreiche Änderungen des SGB V, aber keine Anpassungen an die DSGVO. Mit dem Gesetzesvorhaben soll etwa das Mindestsprechstundenangebot der niedergelassenen Ärzte erhöht werden. Außerdem sollen Krankenkassen nach dem Gesetzentwurf ihren Versicherten spätestens ab 2021 eine elektronische Patientenakte (ePA) zur Verfügung stellen – ein Zugriff auf die in der elektronischen Akte gespeicherten medizinischen Daten soll auch mittels Smartphone oder Tablet möglich sein. Außerdem sind Änderungen im Bereich der Datenverarbeitungsbefugnisse der Krankenkassen nach § 284 SGB V und zum Umgang mit Daten zu Qualitätssicherungszwecken nach § 299 SGB V vorgesehen. Diese Änderungen haben nach Ansicht der Gutachter aber keinen Einfluss auf die vorliegenden Fragestellungen.

1.2 Darstellung des Rechtsrahmens

1.2.1 Unionsrechtlicher Rechtsrahmen

Der unionsrechtliche Rahmen des Datenschutzrechts gliedert sich zunächst in das Primärrecht, das das Verfassungsrecht der Europäischen Union bildet, und das Sekundärrecht, das der europäische Gesetzgeber aufgrund der ihm im Sinne einer begrenzten Einzelermächtigung übertragenen Gesetzgebungskompetenz selbst erlassen kann.

1.2.2 Primärrechtlicher Rechtsrahmen (EUV, AEUV, GRCh)

Zum europäischen Primärrecht zählen der Vertrag über die Europäische Union (EUV) und der Vertrag über die Arbeitsweise der Europäischen Union (AEUV).[12]

11 BT-Drs. 19/4674, S. 140, 370.

12 Vertrag über die Europäische Union (konsolidierte Fassung) und Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung), ABl. C 326 vom 26.10.2012, 1.

Weiterhin ist hiervon die Charta der Grundrechte der Europäischen Union (GRCh) umfasst (Art. 6 Abs. 1 Hs. 2 EUV).[13]

Art. 16 Abs. 2 AEUV beinhaltet eine unionsrechtliche Gesetzgebungskompetenz für das Datenschutzrecht. Aus Art. 16 Abs. 1 AEUV sowie aus Art. 8 GRCh folgen zudem subjektiv-öffentliche Rechte in Form eines Datenschutzgrundrechts. Maßgeblich ist nach herrschender Meinung allein Art. 8 GRCh.[14] Unmittelbar aus Art. 8 Abs. 2 S. 1 GRCh ergeben sich bereits die wesentlichen Erfordernisse der Verarbeitung nach „Treu und Glauben", der Zweckbindung und eines Legitimationstatbestandes, welcher entweder in einer Einwilligung oder einer sonstigen gesetzlich geregelten legitimen Grundlage bestehen kann (Verbot mit Zulässigkeitsvorbehalt).[15]

1.2.3 Sekundärrechtlicher Rechtsrahmen (DSGVO)

Sekundärrechtlich war das Datenschutzrecht bisher durch die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"[16] (RL 95/46/EG), die Datenschutzrichtlinie (DSRL), umgesetzt. Die Handlungsform der Richtlinie war zwar hinsichtlich des zu erreichenden Ziels verbindlich, überließ jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel bei der Umsetzung, vgl. Art. 288 Abs. 3 AEUV (ex-Art. 189 Abs. 3 EGV)[17].

Nunmehr hat sich der europäische Gesetzgeber für eine andere Handlungsform entschieden. Das neue sekundärrechtliche Datenschutzrecht ist als Verordnung im Sinne des Art. 288 Abs. 2 AEUV ausgestaltet. Die Verordnung (EU) 2016/679 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" (DSGVO) hat allgemeine Geltung, ist in allen ihren Teilen verbindlich und gilt in jedem Mitgliedsstaat unmittelbar. Als „Grund"-Verordnung regelt sie die wesentlichen Teile selbst, enthält allerdings eine Vielzahl von Öffnungsklauseln, die den Mitgliedsstaaten Gesetzgebungsspielräume eröffnen. Die DSGVO präsentiert sich dadurch als „Hybrid" zwischen Verordnung und Richtlinie.[18]

Die Öffnungsklauseln beschränken sich dabei nicht darauf, den Mitgliedsstaaten lediglich die optionale Möglichkeit des gesetzgeberischen Tätigwerdens einzuräumen (fakultative Öffnungsklausel), sondern sehen mitunter

13 Ruffert, in: Callies/Ruffert, EUV/AEUV, 5. Aufl., 2016, Art. 1 AEUV Rn. 8.
14 Kingreen, in: Callies/Ruffert, EUV/AEUV, 5. Aufl., 2016, Art. 8 GRCh Rn. 3 (m.w.N.).
15 Ein solches Verbot mit Zulässigkeitsvorbehalt (häufig als „Verbot mit Erlaubnisvorbehalt" bezeichnet) ergibt sich für öffentliche Stellen bereits aus dem allgemeinen Parlamentsvorbehalt.
16 ABl. L 281 vom 23.11.1995, S. 31.
17 Vertrag zur Gründung der Europäischen Gemeinschaft, Abl. C 224 vom 31.08.1992, 1.
18 *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 1.

Regelungsbefehle vor, mithin Verpflichtungen zum gesetzgeberischen Tätigwerden der Mitgliedsstaaten (obligatorische Öffnungsklausel).[19]

Im hier relevanten öffentlichen Bereich bestehen weitreichende Öffnungsklauseln, die den Erlass von Rechtsgrundlagen und die Regelung von Einzelheiten der Verarbeitung ermöglichen (vgl. Art. 6 Abs. 1 UAbs. 1 lit. c), e), Abs. 2, 3 DSGVO).[20] Sofern auch besondere Kategorien personenbezogener Daten (insb. Gesundheitsdaten) betroffen sind, sieht Art. 9 Abs. 2, 3, 4 DSGVO besondere Öffnungsklauseln vor. Neben der Möglichkeit, die Einwilligung in die Verarbeitung im jeweiligen Mitgliedsstaat auszuschließen (Art. 9 Abs. 2 lit. a) DSGVO), betreffen die Öffnungsklauseln speziell in Art. 9 Abs. 2 lit. b), g), h) und i), Abs. 4 DSGVO das öffentliche Gesundheitswesen sowie Art. 9 Abs. 2 lit. j) i.V.m. Art. 89 DSGVO insb. den Bereich der wissenschaftlichen Forschung und damit den der medizinischen Forschung.

Im Ergebnis besteht bei einer Zusammenschau der Öffnungsklauseln ein umfangreicher Gestaltungsspielraum für die Mitgliedsstaaten im Bereich der öffentlichen Gesundheit.[21] Eine strikte Trennung zwischen den Öffnungsklauseln des Art. 6 und des Art. 9 DSGVO ist nicht zwingend erforderlich, da sie ggf. auch gemeinsam zur Anwendung gebracht werden können, sofern sie nicht im Widerspruch zueinanderstehen. Ein durch eine Öffnungsklausel den Mitgliedsstaaten überantworteter Regelungsbereich wird nicht dadurch negiert, dass er Schnittmengen mit einer weiteren Öffnungsklausel hat. Vielmehr kann dies den Regelungsspielraum erweitern.

1.2.4 Deutsches Datenschutzrecht

Das deutsche Datenschutzrecht ist zunächst vom Fehlen einer Gesetzgebungskompetenz des Bundes geprägt. Die Regelung des Datenschutzrechts stellt sich vielmehr als Kompetenz kraft Sachzusammenhang oder Annexkompetenz dar, sodass je nach zu Regeln der Hauptmaterie entweder der Bund im Falle des Eingreifens einer ausschließlichen oder konkurrierenden Gesetzgebungskompetenz (Art. 71ff. GG) oder aber die Länder als grundsätzlich Gesetzgebungsbefugte (Art. 70 GG) tätig werden können. Das führt zu einem Nebeneinander sowohl von allgemeinem Datenschutzrecht als auch von bereichsspezifischem Datenschutzrecht auf Bundes- wie auf Landesebene. Hinzu kommen Regelungsbefugnisse der Kirchen in ihren eigenen Angelegenheiten.[22]

19 *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 9ff.
20 *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 13f.
21 Vgl. *Weichert*, in: Kühling/Buchner, DS-GVO, 2017, Art. 9 Rn. 170.
22 Hierzu vertiefend: *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 81ff.

1.2.4.1 Allgemeines Datenschutzrecht (BDSG; ggf. Landesdatenschutzgesetze)

Als allgemeines Datenschutzrecht galt bisher auf Bundesebene das Bundesdatenschutzgesetz (BDSG a.F.). Alle 16 Bundesländer haben zusätzlich Landesdatenschutzgesetze erlassen. Das BDSG a.F. fand grundsätzliche Anwendung auf öffentliche Stellen des Bundes sowie auf nicht-öffentliche Stellen. Die Landesdatenschutzgesetze fanden Anwendung für die öffentlichen Stellen der Länder.

Mit dem BDSG hat der Bundesgesetzgeber sich dafür entschieden, die bisherige Struktur soweit wie möglich beizubehalten. Zwar folgen die wesentlichen Grundsätze nunmehr unmittelbar aus der DSGVO, das BDSG bildet jedoch auch in Zukunft das allgemeine Datenschutzrecht auf nationaler Ebene.

Gleiches gilt für die Landesdatenschutzgesetze; die allgemeinen Landesdatenschutzgesetze wurden sämtlich an die DSGVO angepasst.

1.2.4.2 Bereichsspezifisches Datenschutzrecht (Sozialdatenschutzrecht nach SGB I/X-neu, sozialrechtliches Fachrecht, sonstige bereichsspezifische Regelungen)

Mit dem Sozialdatenschutzrecht nach § 35 SGB I a.F. i.V.m. §§ 67ff. SGB X a.F. hatte der Bund aufgrund seiner Gesetzgebungskompetenz aus Art. 74 Abs. 1 Nr. 12 i.V.m. Art. 72 Abs. 1 GG eine weitere datenschutzrechtliche „Vollregelung“[23] als allgemeinen Teil des bereichsspezifischen Datenschutzrechts geschaffen, die durch die speziellen Regelungen der sozialrechtlichen Fachbücher, wie etwa den §§ 284ff. SGB V, ergänzt wurde. § 35 SGB I a.F. enthielt als „Grundnorm des Sozialdatenschutzes“[24] den Anspruch, dass Sozialdaten nicht unbefugt von Leistungsträgern und den weiteren abschließend in § 35 Abs. 1 SGB I a.F. genannten Stellen verarbeitet werden. Gemäß § 35 Abs. 2 SGB I a.F. richtete sich die Erhebung, Verarbeitung und Nutzung von Sozialdaten nach dem zweiten Kapitel des SGB X a.F. Diese §§ 67ff. SGB X a.F. normierten von Begriffsdefinitionen, über Zulässigkeitstatbestände, Betroffenenrechte und Sanktionen alle wesentlichen datenschutzrechtlichen Inhalte und bedurften keines Rückgriffs auf das BDSG a.F. als allgemeinen Teil des deutschen Datenschutzrechts.

Durch das neue Sozialdatenschutzrecht nach § 35 SGB I i.V.m. §§ 67ff. SGB X wird auch im Sozialgesetzbuch die bisherige Struktur im Wesentlichen beibehalten. Auch hier gilt, dass der Bundesgesetzgeber lediglich solche Änderungen vorgenommen hat, die sich nach seiner Einschätzung als notwendig erwiesen, um dem unmittelbaren Geltungsanspruch der DSGVO gerecht zu werden. Die gewachsenen Strukturen des Sozialdatenschutzrechts sollten aber möglichst weitgehend beibehalten werden. Eine Zusammenschau des neuen

23 *Dix*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 1 Rn. 160.
24 *Binne*, NZS 1995, 97 (100); BT-Dr. 8/4022, S. 80.

Sozialdatenschutzrechts zeigt, dass nahezu alle Normen geändert wurden, wobei ein großer Teil der Änderungen redaktioneller Art ist und beispielsweise eine Anpassung an die neuen Begriffsdefinitionen des Art. 4 DSGVO, beinhaltet. Unmittelbar aus den Änderungen des SGB, aber auch mittelbar aus der geänderten sekundärrechtlichen Gewährleistung der DSGVO, folgen insgesamt inhaltliche Änderungen, wobei die wesentlichen Strukturen innerhalb des SGB aufrechterhalten bleiben.

Ausdrücklich normiert hat der Gesetzgeber in § 35 Abs. 2 Satz 1 SGB I nunmehr, dass die „Bücher des Sozialgesetzbuchs" die „Verarbeitung von Sozialdaten abschließend" regeln, soweit nicht die DSGVO unmittelbar gilt. Damit wird klargestellt, dass die DSGVO zwar unmittelbar Geltung erlangt, dort aber wo der deutsche Bundesgesetzgeber auf eine Öffnungsklausel zurückgreifen kann und dies auch getan hat, die Regelungen des Sozialdatenschutzrechts abschließend gelten sollen. Weiterhin wird durch die Klarstellung Bezug auf die Regelung des § 1 Abs. 2 S. 2 BDSG genommen, wonach ein Rückgriff auf das BDSG als allgemeines deutsches Bundesdatenschutzrecht nur möglich ist, sofern eine spezielle bundesrechtliche Vorschrift nicht abschließend regelt. Es gilt also neben der DSGVO ausschließlich das Sozialgesetzbuch für die Verarbeitung von Sozialdaten. Der Anspruch des SGB, die Sozialversicherung als Vollregelung umfassend zu regeln, wird nur insoweit eingeschränkt, als der europarechtliche Anwendungsvorrang der DSGVO dies erfordert.

Aus der Gesetzesbegründung zur Änderung des SGB I und SGB X wird deutlich, dass die Bundesregierung die neuen Bestimmungen sämtlich auf die Öffnungsklauseln der Art. 6 Abs. 2 und 3 sowie Art. 9 Abs. 2 DSGVO stützt.[25] Art. 6 Abs. 2 DSGVO eröffnet den Mitgliedsstaaten den größten Spielraum. Er ist dann einschlägig, wenn die Verarbeitung gemäß Art. 6 Abs. 1 lit. e) DSGVO für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt, oder die in Ausübung öffentlicher Gewalt erfolgt. Die Öffnungsklausel ermöglicht damit den Erlass oder die Beibehaltung von Regelungen im Bereich der sozialen Sicherheit sowohl für Behörden, für die dies eine Aufgabe in Ausübung öffentlicher Gewalt darstellt, sowie für Private, die eine im öffentlichen Interesse liegende Aufgabe wahrnehmen. Werden besondere Kategorien personenbezogener Daten – beispielsweise Gesundheitsdaten – verarbeitet, sind die Öffnungsklauseln des Art. 9 Abs. 2 lit. b), g), h) und i) DSGVO zu beachten. Ein vollständiges systematisches Regelungsregime im Bereich der sozialen Sicherheit ist daher auf Art. 6 Abs. 2 DSGVO zu stützen. Diese Öffnungsklausel hat sich insbesondere Deutschland im Rat erkämpft, um eigene gewachsene Systeme beibehalten zu können, die den spezifischen hiesigen Eigenheiten im öffentlichen Bereich Rechnung tragen. Damit bleibt es bei einem geschlossenen System des Sozialdatenschutzes.[26]

25 Vgl. BT-Drs. 18/12611, S. 104f.

26 So auch Hoidn, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018, S. 294f.

Regelungen der DSGVO, die unmittelbar Anwendung finden, sind beispielsweise die Grundprinzipien der Datenverarbeitung[27] oder die grundlegenden Prinzipien der Datensicherheit sowie die Pflicht des Verantwortlichen zur Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, die „Selbstregulierung" mittels Verhaltensregeln nach Art. 40, 41 DSGVO und Zertifizierungen nach Art. 42, 43 DSGVO.[28]

An dieser Stelle sei allerdings darauf hingewiesen, dass mit dem neu eingeführten § 35 Abs. 6 SGB I der persönliche Anwendungsbereich des Sozialdatenschutzrechts im Vergleich zur alten Fassung so verstanden werden könnte, dass er auf solche Stellen ausgeweitet wurde, die nicht bereits in § 35 Abs. 1 SGB I genannt sind. So heißt es in § 35 Abs. 6 Satz 1 SGB I:

> *„Die Absätze 1 bis 5 finden **neben den in Absatz 1 genannten Stellen** auch Anwendung auf solche Verantwortliche oder deren Auftragsverarbeiter,*
>
> *1. die Sozialdaten im Inland verarbeiten, sofern die Verarbeitung nicht im Rahmen einer Niederlassung in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgt, oder*
>
> *2. die Sozialdaten im Rahmen der Tätigkeiten einer inländischen Niederlassung verarbeiten." [Hervorhebung nicht im Original]*

In Zusammenschau mit der Begriffsdefinition des § 67 Abs. 2 S. 1 SGB X könnte sich ein Zirkelschluss ergeben, der nur schwer auflösbar scheint. § 67 Abs. 2 S. 1 SGB X lautet:

> *„Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung [EU] 2016/679), die **von einer in § 35 des Ersten Buches genannten Stelle** im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden." [Hervorhebung nicht im Original]*

Entweder liefe § 35 Abs. 6 SGB I leer, weil die nicht explizit in Absatz 1 des § 35 SGB I genannten Stellen gemäß der Definition des § 67 Abs. 2 SGB X keine Sozialdaten verarbeiten können, oder aber Absatz 6 ist geeignet, die Anwendbarkeit des Sozialdatenschutzrechts nahezu unbegrenzt auszuweiten. Letzteres wäre etwa dann der Fall, wenn man nunmehr davon ausgehen müsste, dass eine Transformation eines personenbezogenen Datums in ein Sozialdatum zukünftig irreversibel ist. Jedes Sozialdatum würde bei einer weiteren Verarbeitung – und nicht nur bei einer zweckgebundenen Weiterverarbeitung nach einer Übermittlung durch eine in § 35 Abs. 1 SGB I genannte Stelle – immer dem Sozialdatenschutzrecht unterliegen, womit die Bestimmung des

27 Hierzu s. Kap. 1.3.
28 Vgl. Bieresborn, NZS 2017, 887 (889).

einschlägigen Datenschutzrechts nicht mehr an der verantwortlichen Stelle ansetzen würde, sondern am Charakter des Datums. Das wäre hochproblematisch, da einem Datum seine Herkunft in aller Regel nicht anzusehen ist. Aus den Gesetzgebungsunterlagen ergibt sich lediglich ein Hinweis auf § 78 Abs. 1 S. 2 (sic!) SGB X[29], wonach Dritte, denen Sozialdaten übermittelt wurden, diese Daten in gleichem Umfang geheim zu halten haben, wie die in § 35 SGB I genannten Stellen. Die Gesetzesbegründung verweist also auf einen falschen Satz, der seinerseits dem Wortlaut nach nur die Rechtsfolge einer Geheimhaltungspflicht beinhaltet, inhaltlich aber wohl die Anwendbarkeit des Sozialdatenschutzrechts bedeuten könnte. Insgesamt muss hier von einer nachlässigen Gesetzgebungsarbeit ausgegangen werden, die einer Ermittlung der legislativen Absicht entgegensteht. Da sich aus den Gesetzgebungsmaterialien jedenfalls keine Absichten entnehmen lassen, den Geltungsbereich des Sozialdatenschutzrechts auszuweiten, ist eine restriktive Auslegung des § 35 Abs. 6 SGB I geboten.[30]

1.2.5 Verhältnis zu Geheimnis- und Schweigepflichten (Insb. § 203 StGB)

Nach bisheriger Rechtslage war das Verhältnis zwischen Datenschutzrecht und Geheimnis- oder Schweigepflichten in § 1 Abs. 3 S. 2 BDSG a.F. geregelt. Demnach blieb die Verpflichtung zur Wahrung gesetzlicher Geheimnispflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt. Mit anderen Worten waren Datenschutzrecht und Geheimnispflichten parallel anzuwenden (sog. Zwei-Schranken-Prinzip). Durchbrechungen dieses Prinzips bestanden nur in wenigen Ausnahmefällen.

Das BDSG enthält ebenfalls eine ausdrückliche Regelung zum Verhältnis der beiden Rechtsinstrumente zueinander. Gemäß § 1 Abs. 2 S. 2 BDSG bleibt auch in Zukunft die Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt. Zum Zweck der Klarstellung wurde eine gleichlautende Regelung nunmehr auch für das Sozialdatenschutzrecht in § 35 Abs. 2a SGB I aufgenommen. Hierbei ist darauf hinzuweisen, dass das Sozialgeheimnis nach § 35 Abs. 1 S. 1 SGB I selbst keine solche Geheimhaltungspflicht beinhaltet, sondern lediglich einen Anspruch auf Einhaltung datenschutzrechtlicher Anforderungen formuliert. Die Bezeichnung als Sozialgeheimnis ist daher irreführend und lediglich noch historisch zu erklären,[31] wenngleich eine Notwendigkeit zur Aufrechterhaltung dieses Instruments für die Anpassungsgesetzgebung an die DSGVO nicht mehr besteht.

29 Gemeint war wohl § 78 Abs. 1 S. 3 SGB X oder § 78 Abs. 1 S. 2 SGB X a.F.

30 Siehe hierzu auch Kapitel 1.5.4.1.2.

31 *Mrozynski*, SGB I, 5. Aufl., 2014, § 35 Rn. 9; Kircher, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 46f., 113f.

Über die bloße parallele Geltung hinaus, sieht das Sozialdatenschutzecht mitunter die „Verlängerung" der ärztlichen Schweigepflicht nach § 203 StGB vor und bestimmt so, dass auch Empfänger der Daten diese entsprechend geheim halten müssen (vgl. § 76 Abs. 1 SGB X[32]). Das hat zur Folge, dass zusätzlich zur datenschutzrechtlichen Zulässigkeit eine Offenbarungsbefugnis nach den Maßstäben des Strafrechts erforderlich ist, wenn ein Empfänger die Daten seinerseits weitergeben möchte.[33] Diese Anforderung perpetuiert sich aus der sog. Erstübermittlung mit jeder weiteren Übermittlung.[34]

Am Vorrang der Geheimnispflichten ändert auch die Reform des § 203 StGB nichts. Durch die nunmehr bestehende Möglichkeit, „sonstige Mitwirkende" befugt an einem Geheimnis teilhaben lassen zu können, ist zwar die Möglichkeit geschaffen worden, externe Dienstleister beispielsweise im Rahmen eines Auftragsverarbeitungsverhältnisses in eine berufliche Tätigkeit einzubinden. Auf eine zwischenzeitlich diskutierte Lösung, datenschutzrechtliche Vorschriften als Befugnisnorm im Sinne des § 203 StGB auszugestalten, wurde jedoch verzichtet. Gleichzeitig knüpft auch der neue § 203 StGB nicht an datenschutzrechtliche Kategorien oder Instrumente, wie die Auftragsverarbeitung, an. Die strafrechtlichen Voraussetzungen für die Einbeziehung Mitwirkender ergeben sich vielmehr unmittelbar aus dem Wortlaut des nunmehr geltenden § 203 StGB.

Im Bereich der Heilberufe ist zu beachten, dass auch die Reform der strafrechtlichen Schweigepflicht die jeweiligen Berufsordnungen unberührt lässt. Auch wenn also eine Offenbarung gegenüber „sonstigen Mitwirkenden" strafrechtlich befugt sein mag, so kann sie (derzeit) dennoch berufsrechtswidrig sein.

1.3 Wesentliche Prinzipien des Datenschutzrechts

Die DSGVO benennt in Art. 5 vorab neun allgemeine Grundsätze, die für die Verarbeitung personenbezogener Daten maßgeblich sind. Diese Grundsätze werden durch die konkreten Vorschriften der DSGVO sowie einzelner bereichsspezifischer Datenschutzregelungen konkretisiert und durch weitere nicht explizit genannte Grundsätze ergänzt. Diese nachfolgend kurz skizzierten Grundsätze sind bei jeder Form der Verarbeitung personenbezogener Daten zu beachten und bei der Auslegung datenschutzrechtlicher Gesetze heranzuziehen.

1.3.1 Rechtmäßigkeit der Verarbeitung und Verbot mit Zulässigkeitsvorbehalt

Grundlegendes Prinzip der Verarbeitung personenbezogener Daten ist, dass diese auf rechtmäßige Weise erfolgen muss (Art. 5 Abs. 1 lit. a) DSGVO). Hand

32 Gleiches galt bereits nach alter Rechtslage gem. § 76 Abs. 1 SGB X.
33 Vgl. *Diering/Seidel*, in: Diering/Timme, SGB X, 4. Aufl., 2016, § 76 Rn. 7.
34 Hierzu *Meier*, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003, S. 235ff.

in Hand mit diesem Prinzip geht das auch im Rahmen der DSGVO geltende Prinzip des Verbots mit Erlaubnisvorbehalt. Entsprechend diesen Prinzipien ist eine Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn die Verarbeitung ist entsprechend Art. 6 DSGVO sowie Art. 9 DSGVO durch einen gesetzlichen Erlaubnistatbestand oder die Einwilligung des Betroffenen legitimiert.

1.3.2 Zweckbindung

Einen weiteren wesentlichen Pfeiler der Verarbeitung personenbezogener Daten bildet der Zweckbindungsgrundsatz. Gemäß Art. 5 Abs. 1 lit. b) DSGVO dürfen Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden. Demnach hat bereits im Vorfeld der Datenerhebung eine Zweckfestlegung zu erfolgen. Dieser festgelegte Zweck begrenzt die Datenverarbeitungsmöglichkeiten und bestimmt die Einzelheiten der Verarbeitung. Dabei ist zu beachten, dass der ursprünglich festgelegte Verarbeitungszweck eine Verarbeitung zu anderen Zwecken nicht generell ausschließt. Vielmehr kann eine Datenverarbeitung auch zu anderen Zwecken erfolgen. Nach einer Ansicht erfordert dies, dass die Weiterverarbeitung zum Sekundärzweck auf eine gesonderte Rechtsgrundlage gestützt werden kann und zudem mit dem ursprünglichen Zweck der Datenerhebung vereinbar ist.[35] Nach anderer Ansicht bedarf es bei Vereinbarkeit des Sekundärzwecks mit dem Primärzweck keiner eigenen Rechtsgrundlage.[36] Letzterer Ansicht ist zuzustimmen. Zum einen stimmt sie mit der Aussage des Erwägungsgrundes 50 überein, nach dessen Satz 2 für eine zweckvereinbare Weiterverwendung keine „andere gesonderte" Rechtsgrundlage erforderlich ist. Zum anderen würde die Zweckvereinbarkeitsprüfung weitgehend leerlaufen, wenn es dennoch einer neuen Rechtsgrundlage bedürfte.[37]

Bei der Frage der Vereinbarkeit mit dem ursprünglichen Zweck spielen unterschiedliche Faktoren eine Rolle, die im Rahmen einer wertenden Betrachtung einzubeziehen sind. Neben Nähe und Kontext des neuen zum ursprünglichen Zweck sind auch die Art der Daten, die Folgen der Weiterverarbeitung sowie ein Wechsel des Verantwortlichen von entscheidender Bedeutung.[38] Insbesondere im Bereich der Verarbeitung besonderer Kategorien personenbezogener Daten sind der Zweckvereinbarung enge Grenzen gesetzt.[39] Für den Bereich der wissenschaftlichen Forschung stellt Art. 5 DSGVO jedoch die Vermu-

35 Heberlein, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 5 Rn. 19f.; Herbst, in: Kühling/Buchner, DS-GVO, 2017, Art. 5 Rn. 24ff.
36 *Frenzel*, in: Paal/Pauly, DS-GVO, 2017, Art. 5 Rn. 30f.; vgl. Erw.Gr. 50 Abs. 1 S. 2.
37 Vgl. *Nebel*, Erlaubnis zur Datenverarbeitung, in: Roßnagel (Hrsg.), Europäische Datenschutz-Grundverordnung, 2017, § 3 Rn. 97.
38 *Herbst*, in: Kühling/Buchner, DS-GVO, 2017, Art. 5 Rn. 44.
39 *Herbst*, in: Kühling/Buchner, DS-GVO, 2017, Art. 5 Rn. 44.

tung auf, dass dieser neue Zweck mit dem ursprünglichen Zweck vereinbar ist, sofern die Verarbeitung entsprechend Art. 89 Abs. 1 DSGVO erfolgt.

Für Sozialdaten greift § 67c SGB X den Zweckbindungsgrundsatz auf und regelt, dass Sozialdaten grundsätzlich nur zur Erfüllung der gesetzlich übertragenen Aufgaben verarbeitet werden dürfen, sofern die Daten hierfür erforderlich sind und für diesen Zweck erhoben wurden. Eine Datenverarbeitung zu anderen Zwecken ist nur in engen Grenzen zulässig (vgl. z.B. § 284 Abs. 3 SGB V, § 67c Abs. 2 Nr. 2 SGB X, § 75 SGB X). Dem Bereich der wissenschaftlichen Forschung kommt in diesem Zusammenhang eine gewisse Privilegierung zu (vgl. Erw.Gr. 33).

1.3.3 Treu und Glauben

Das Gebot der Verarbeitung personenbezogener Daten entsprechend Treu und Glauben ist der Übersetzung der DSGVO ins Deutsche geschuldet und ist weniger im Sinne des in der deutschen Rechtsprechung und Literatur zu § 242 BGB entwickelten Verständnisses, sondern vielmehr im Sinne der Gewährleistung einer „fairen" Verarbeitung zu verstehen.[40] Im Übrigen entspricht dies jedoch der Terminologie des Art. 8 Abs. 2 GRCh. Über diesen Auffangtatbestand soll in jedem Fall ein Ausgleich der widerstreitenden Interessen der betroffenen Personen und der Verantwortlichen sowie die Herstellung des Kräftegleichgewichts möglich sein[41]. Dementsprechend sind in den unterschiedlichen Datenverarbeitungsschritten, etwa bei der Information des Betroffenen, im Rahmen der Bewertung der Freiwilligkeit der Einwilligung oder von Art und Umfang der Datenverarbeitung sowie der Abwägung widerstreitender Interessen oder der Festlegung von Verhaltensregeln nach Art. 40 Abs. 2 lit. a) DSGVO die vernünftigen Erwartungen der betroffenen Person zugrunde zu legen (Erw.Gr. 47 S. 1, Erw.Gr. 50 S. 6).

1.3.4 Datenminimierung (Datenvermeidung und Datensparsamkeit)

Neben der Zweckbindung gibt Art. 5 Abs. 1 lit. c) DSGVO vor, dass die Verarbeitung entsprechend der Zweckbestimmung auf ein notwendiges Maß zu beschränken ist. Dementsprechend darf eine Verarbeitung personenbezogener Daten nicht erfolgen, wenn der Zweck auch auf andere Weise, etwa auf Grundlage anonymisierter Daten, zu erreichen ist[42]. Dieser Grundsatz wird in Art. 25 DSGVO konkretisiert, gemäß dem geeignete technische und organisatorische Maßnahmen – etwa privacy by design und privacy by default – zu ergreifen sind. Für den Bereich der wissenschaftlichen Forschung stellt sich in diesem

40 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 5 Rn. 9; Plath, in: BDSG/DSGVO, 2017, § 5 Rn. 9.
41 *Herbst*, in: Kühling/Buchner, DS-GVO, 2017, Art. 5 Rn. 17.
42 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 5 Rn. 22.

Zusammenhang folglich regelmäßig die Frage, inwiefern die Verarbeitung personenbezogener Daten tatsächlich erforderlich ist oder ob nicht vielmehr auch die Arbeit mit anonymisierten oder zumindest pseudonymisierten Daten ausreicht.

1.3.5 Transparenz

Gemäß Art. 5 Abs. 1 lit. a) DSGVO sollen personenbezogene Daten in einer für den Betroffenen transparenten, nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass der Betroffene umfassend über die Art und den Umfang der Verarbeitung, die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie über Risiken, Vorschriften, Garantien und seine Rechte im Zusammenhang mit der Verarbeitung seiner personenbezogenen Daten unterrichtet wird (Erw.Gr. 39). Darüber hinaus sind diese Informationen dem Betroffenen in klarer, leicht verständlicher Form und ohne Zugangshindernisse zur Verfügung zu stellen. Dieser allgemeine Transparenzgrundsatz wird durch die spezifischen geregelten Informationspflichten der Verantwortlichen (Art. 12–14 DSGVO) sowie Auskunftsrechte der Betroffenen (Art. 15 DSGVO) konkretisiert und durch technische Maßnahmen wie etwa datenschutzfreundliche Einstellungen und Zertifizierungsverfahren flankiert.

1.3.6 Richtigkeit der Daten

Was im BDSG a.F. über die Rechte auf Löschung und Berichtigung personenbezogener Datenverbürgt war, hat nunmehr in Art. 5 Abs. 1 lit. e) DSGVO eine ausdrückliche Regelung erfahren. Danach müssen personenbezogene Daten sachlich richtig sein und auf dem neuesten Stand gehalten werden. Die Durchsetzung dieses Grundsatzes ist auch nach der DSGVO durch Ansprüche auf Berichtigung und Löschung gewährleistet.

1.3.7 Speicherbegrenzung

Art. 5 Abs. 1 lit. e) DSGVO bestimmt, dass die Speicherdauer auf den für die Zweckerfüllung zwingend erforderlichen Zeitraum zu begrenzen ist. Zwar bedeutet das nicht, dass die Speicherfrist kalendermäßig bestimmt sein muss. Jedoch muss sich die Dauer der Speicherung zumindest anhand eines Ereignisses oder einer Bedingung bestimmen lassen. Für Daten, die für Zwecke der wissenschaftlichen Forschung verarbeitet werden, gilt jedoch wiederum eine Ausnahme von dieser Regelung, sofern Garantien vorliegen, über die sichergestellt wird, dass geeignete technische und organisatorische Maßnahmen bestehen, mit denen die Einhaltung der Datenverarbeitungsgrundsätze gewährleistet und die Rechte und Interessen der Betroffenen geschützt werden.

1.3.8 Integrität und Vertraulichkeit

Um die Integrität und Vertraulichkeit personenbezogener Daten zu gewährleisten, verpflichtet Art. 5 Abs. 1 lit. f) DSGVO den Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu treffen, die die Daten vor einem unautorisierten Zugriff – etwa durch Zugangs- und Zugriffskontrollen – oder dem Verlust – durch entsprechende Sicherungsmaßnahmen – bewahren.

1.3.9 Rechenschaftspflicht

Nach Art. 5 Abs. 2 DSGVO wird dem Verantwortlichen die Gesamtverantwortung für eine rechtmäßige Datenverarbeitung und die Einhaltung der übrigen Datenverarbeitungsgrundsätze auferlegt und darüber hinaus eine diesbezügliche Nachweispflicht geregelt. Im Rahmen dieser Gesamtverantwortung sind im Vorfeld der Datenverarbeitung im Einzelfall Risikoanalysen und Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) vorzunehmen und ein Verarbeitungsverzeichnis (Art. 30 DSGVO) anzulegen. Während der Verarbeitung sind die Daten durch technische und organisatorische Maßnahmen (Art. 32 DSGVO) – wie etwa Zugangs- und Zugriffskontrollen sowie Back-ups – im Rahmen eines umfassenden Datenschutzmanagements zu sichern. Zudem sind Reaktions- und Meldesysteme für Fälle von Datenschutzverletzungen (Art. 33, 34 DSGVO) vorzusehen. All diese Maßnahmen sind in regelmäßigen Abständen auf Aktualität und Suffizienz zu überprüfen und zum Zwecke des Nachweises (Art. 5 Abs. 2 DSGVO) zu dokumentieren. Dabei erstrecken sich die Verantwortung für die Verarbeitung und die Nachweispflicht nicht nur auf die Verarbeitung durch den Verantwortlichen selbst, sondern umfassen auch die Verarbeitung durch Auftragsverarbeiter.

1.3.10 Direkterhebung

Der noch in § 4 Abs. 2 BDSG a.F. ausdrücklich normierte Grundsatz der Direkterhebung ist in der DSGVO nicht mehr explizit geregelt. Auch wenn es an einer ausdrücklichen Regelung fehlt, bleibt dieser Grundsatz im Rahmen der Datenverarbeitungsgrundsätze zur Transparenz und der Datenminimierung sowie der Erforderlichkeit der Datenverarbeitung auch im Anwendungsbereich der DSGVO von Bedeutung[43]. Für den Bereich des Sozialdatenschutzrechts wurde der Grundsatz der Direkterhebung auch nach der Reform ausdrücklich in § 67a Abs. 2 S. 1 SGB X aufgenommen, sodass Sozialdaten nur in den gesetzlich geregelten Ausnahmefällen (§ 67a Abs. 2 S. 2 SGB X) bei Dritten erhoben werden dürfen.

43 *Bäcker*, in: Kühling/Buchner, DS-GVO, 2017, Art. 13 Rn. 3.

1.3.11 Erforderlichkeit

Auch wenn dieser Grundsatz nicht ausdrücklich in Art. 5 DSGVO genannt ist, wird er an mehreren Stellen des Gesetzes verwendet (etwa in Art. 6 Abs. 1 lit. b)–f) DSGVO). In Verbindung mit anderen Datenverarbeitungsgrundsätzen – etwa der Datenminimierung und der Speicherbegrenzung – stellt das Erforderlichkeitsprinzip eine wesentliche Säule des Datenschutzes dar. Die Datenverarbeitung muss sich in Art und Umfang auf ein Maß beschränken, das zur Erreichung des Zwecks notwendig und ausreichend ist (siehe hierzu die Ausführungen im Gutachtenteil von Roßnagel im vorliegenden Band.).[44]

1.4 Beurteilung von Szenario 1

Im Folgenden wird auf die einzelnen Szenarien eingegangen. Entsprechend der Ausführungen in Kapitel 1.1.1 wird die Rechtslage nach der DSGVO sowie dem bislang bekannten nationalen Datenschutzrecht beurteilt. In Ermangelung einer Neufassung der datenschutzrechtlichen Normen der fachspezifischen Sozialgesetzbücher (insb. SGB V) kann hier nur auf die geltende Rechtslage abgestellt werden.

1.4.1 Darstellung des Szenarios

Die Datennutzung geschieht im Rahmen eines Kooperationsprojekts einer gesetzlichen Krankenkasse („Leistungsträger" i.S.d. Sozialversicherungsrechts) mit einer externen Einrichtung. Die Fragestellungen für die Datenauswertung werden gemeinsam entwickelt oder von der externen Einrichtung vorgegeben. Die Sozialdaten bleiben in der Einrichtung der gesetzlichen Krankenkasse und werden hier ausgewertet. Lediglich anonyme Auswertungsergebnisse werden an den externen Partner übermittelt, es verlassen keine Sozialdaten die Einrichtung der gesetzlichen Krankenversicherung.

1.4.2 Rechtfertigungsbedürftige Datenverarbeitungsvorgänge

Vorab ist festzuhalten, dass die Weitergabe der anonymen Auswertungsergebnisse durch den Leistungsträger nicht rechtfertigungsbedürftig ist, denn aus Sicht des Empfängers werden anonyme Daten weitergegeben. Unter der Prämisse, dass die Daten durch den Leistungsträger im Rahmen des § 284 Abs. 1 S. 1 SGB V erhoben und gespeichert wurden, sind die Erhebung und Speicherung der Daten insofern gerechtfertigt und nicht Gegenstand nachfolgender Prüfung.

44 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO, 2017, Art. 6 Rn. 15.

Datenschutzrechtsrelevante Datenumgänge, deren Zulässigkeit nachfolgend zu prüfen ist, sind somit im *Szenario 1* allein die **Auswertungen der Daten** durch den Leistungsträger zu Zwecken der wissenschaftlichen Forschung, der Planung im Sozialleistungsbereich und der Qualitätssicherung.

1.4.3 Zulässigkeit der Datenumgänge durch den Leistungsträger (hinsichtlich des jeweiligen Zwecks: Wissenschaftliche Forschung, Planung im Sozialleistungsbereich oder Qualitätssicherung)

Zulässig ist die Auswertung der Sozialdaten nur im Falle eines einschlägigen Erlaubnistatbestandes und bei Vorliegen aller seiner Voraussetzungen. Im Rahmen der nachfolgenden Prüfung ist angesichts der zahlreichen Verortungen von datenschutzrechtlichen Vorschriften zunächst der Prüfungsmaßstab unter Berücksichtigung des einschlägigen Datenschutzregimes zu klären (s. Kap. 1.4.3.1). Sodann ist zu untersuchen, ob bzw. welche Erlaubnistatbestände des einschlägigen Datenschutzregimes greifen (s. Kap. 1.4.3.2 und Kap. 1.4.3.3).

1.4.3.1 Prüfungsmaßstab/Identifikation des einschlägigen Datenschutzregimes

Die Frage, welches Datenschutzregime im Einzelnen Anwendung findet, richtet sich danach, welche Stelle für die Verarbeitung personenbezogener Daten verantwortlich ist.

Im vorliegenden Szenario werden personenbezogene Daten ausschließlich von einer Krankenkasse verarbeitet. Krankenkassen unterliegen als Leistungsträger im Sinne des § 35 Abs. 1 SGB I i.V.m. § 21 Abs. 2 SGB I dem Sozialgeheimnis. Sie sind somit an das umfassend regelnde Sozialdatenschutzrecht nach § 35 SGB I i.V.m. §§ 67ff. SGB X gebunden, sofern sie personenbezogene Daten im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch (SGB), also Sozialdaten im Sinne des § 67 Abs. 2 S. 1 SGB X, verarbeiten. Weiterhin müssen zusätzlich die fachspezifischen Datenschutzregelungen im SGB V (insb. §§ 284ff. SGB V) beachtet werden. Nach dem Wortlaut des § 35 Abs. 2 S. 1 SGB I regeln die Vorschriften des Sozialdatenschutzrechts und der übrigen Bücher des SGB die Verarbeitung von Sozialdaten abschließend, soweit nicht die DSGVO unmittelbar gilt. Das heißt, dass also zunächst die unmittelbar geltende DSGVO Anwendung findet; auf nationaler Ebene sind dann die datenschutzrechtlichen Regelungen im SGB zu beachten. Ein Rückgriff auf das allgemeine Bundesdatenschutzrecht im BDSG kommt hingegen nicht in Betracht (vgl. § 1 Abs. 2 S. 2 BDSG). Das BDSG kann nur dann noch Anwendung finden, wenn eine Norm des SGB ausdrücklich auf das BDSG verweist.[45] Der Anspruch des SGB, die Verarbeitung von Sozialdaten abschließend zu regeln, gilt aber auch

45 Vgl. BT-Drs. 18/12611, S. 96.

im Verhältnis zur DSGVO, wenn im Sozialdatenschutz aufgrund einer Öffnungsklausel der DSGVO eine spezifische Regelung getroffen wird.[46]

Lediglich im Falle der Einwilligung und in Fällen der Verarbeitung zum Schutz lebenswichtiger Interessen kann sich die Rechtfertigung – ohne Rückgriff auf das Sozialgesetzbuch – unmittelbar aus Art. 9 Abs. 2 lit a) und c) DSGVO ergeben. Da zur Regelung der allgemeinen Einwilligung keine Öffnungsklausel mehr besteht und hinsichtlich der Öffnungsklausel zum Ausschluss der Einwilligung in die Verarbeitung sensibler Daten kein Gebrauch gemacht wurde, erscheint es folgerichtig, dass in Zukunft – abweichend von den grundsätzlichen Erwägungen des BSG[47] – auch hinsichtlich der Möglichkeit der Einholung von Einwilligungserklärungen auf allgemeines Datenschutzrecht in Form der DSGVO zurückgegriffen werden kann.[48]

1.4.3.1.1 Verbot mit Zulässigkeitsvorbehalt

Entsprechend Art. 6 Abs. 1 sowie Art. 9 Abs. 2 DSGVO gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt. Eine Verarbeitung personenbezogener Daten ist daher nur zulässig, sofern sie sich auf einen entsprechenden Erlaubnistatbestand stützen kann.

Dieser Regelungsansatz spiegelt sich im nationalen Datenschutzrecht ebenfalls wider. Das Sozialrecht bringt die bereichsspezifische Ausprägung des Verbots mit Zulässigkeitsvorbehalt in § 67b Abs. 1 S. 1, 2 SGB X und § 284 Abs. 3 SGB V mit engeren Voraussetzungen zum Ausdruck. § 67b Abs. 1 S. 1 SGB X setzt für die Zulässigkeit einer Verarbeitung das Eingreifen einer Erlaubnisnorm nach dem SGB voraus und wiederholt somit gewissermaßen das allgemeine Verbot mit Zulässigkeitsvorbehalt im Hinblick auf die Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung sowie Löschung von Sozialdaten und begrenzt gleichzeitig die in Betracht kommenden Rechtfertigungstatbestände.[49] Diese können sich demnach nur aus dem Sozialgesetzbuch ergeben. Satz 2 bezieht dies auch auf besondere Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO.

Auch die bereichsspezifische Norm des § 284 SGB V, die die zentrale Zweckbindungsnorm für Datenumgänge bei den Krankenkassen darstellt, macht deutlich, dass eine Verarbeitung von Sozialdaten nur zulässig ist, sofern dies – abgesehen von der ausdrücklichen Einwilligung des Betroffenen – durch eine Rechtsvorschrift des Sozialgesetzbuchs legitimiert ist. So dürfen Sozialdaten

46 Vgl. BT-Drs. 18/12611, S. 96.

47 BSG, Urteil vom 10.12.2008 – B 6 KA 37/07 R, juris-Rn. 35.

48 An dieser Stelle sei darauf hingewiesen, dass mit dem Entwurf zum 2. DSAnpUG-EU bei der Verarbeitung von biometrischen, genetischen oder Gesundheitsdaten formelle Wirksamkeitsvoraussetzungen für Einwilligungserklärungen geschaffen werden sollen, vgl. BT-Drs. 19/4674, S. 153. Hierzu bereits oben in Kap. 1.1.3.2.1.

49 Vgl. *Bieresborn*, in: von Wulffen/Schütze, SGB X, 8. Aufl., 2014, § 67b Rn. 3; *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 209.

gemäß § 284 Abs. 3 S. 1 Hs. 1 SGB V grundsätzlich nur zu den Zwecken verarbeitet werden, zu denen sie gemäß § 284 Abs. 1 SGB V erhoben wurden. Darüber hinaus ist eine Verarbeitung der Sozialdaten zu anderen Zwecken nur zulässig, sofern eine Rechtsvorschrift des Sozialgesetzbuchs dies gestattet. Damit sind neben den Regelungen des SGB V (z.B. § 287 SGB V) auch solche des allgemeinen Sozialdatenschutzrechts umfasst (z.B. § 76c Abs. 2 Nr. 2 SGB X).[50] Angesichts der Regelung in Art. 5 Abs. 1 lit. b) 2. HS DSGVO hat der Bundesgesetzgeber hier die Möglichkeit, das Zweckbindungsgebot zu lockern.

1.4.3.1.2 Verhältnis von SGB V zum allgemeinen Sozialdatenschutzrecht (SGB I und SGB X)

Vor dem Hintergrund der Existenz eines allgemeinen (SGB I und SGB X) und eines speziellen (SGB V) bereichsspezifischen Datenschutzrechts stellt sich die Frage, ob die spezielleren Normen aus dem bereichsspezifischen Sozialdatenschutzrecht der Fachbücher des SGB (hier SGB V) eine Sperrwirkung hinsichtlich des Rückgriffs auf die Regelungen im allgemeinen Sozialdatenschutzrecht entfalten. Eine allgemeine Sperrwirkung der zulasten der Vorschriften des Sozialdatenschutzrechts im SGB X kommt nicht in Betracht, da die Normen des SGB V nur vereinzelte Datenumgänge regeln. Eine solche Sperrwirkung aus den nur punktuellen Regelungen des SGB V gegenüber dem allgemeinen Sozialdatenschutzrecht ergibt sich im Übrigen auch nicht aus der Rechtsprechung des Bundessozialgerichts vom 10.12.2008[51]. Das Gericht schloss lediglich einen Rückgriff auf das BDSG a.F. oder Landesdatenschutzrecht aus,[52] während es die Anwendung der allgemeinen Vorschriften des bereichsspezifischen Datenschutzrechts nach dem SGB X a.F. durchaus erwogen hat und nur deshalb im konkreten Fall nicht zur Anwendung gebracht hat, da es sich bei den betroffenen Leistungserbringern nicht um Stellen nach § 35 SGB I a.F. handelt.[53] Eine Sperrwirkung infolge eines Vorrangs nach dem Grundsatz „lex specialis derogat legi generali“ kann sich ausschließlich für den jeweils mit der Norm des SGB V konkret geregelten Bereich ergeben. Im Übrigen sind die Normen des SGB V und des allgemeinen Sozialdatenschutzrechts gleichrangig.[54]

Tatbestände des allgemeinen Sozialdatenschutzrechts nach § 35 SGB I und §§ 67ff. SGB X werden durch die fachspezifischen Datenschutzregelungen des SGB V ergänzt und hinsichtlich des spezifischen Regelungsgegenstandes der jeweiligen SGB V-Norm verdrängt.

50 Vgl. *Didong/Koch*, in: Schlegel/Voelzke, juris PK-SGB V, 3. Aufl. 2016, § 284 Rn. 18.
51 BSG, Urteil vom 10.12.2008 – B 6 KA 37/07 R.
52 BSG, Urteil vom 10.12.2008 – B 6 KA 37/07 R, juris-Rn. 33ff.
53 BSG, Urteil vom 10.12.2008 – B 6 KA 37/07 R, juris-Rn. 23, 33, 35.
54 BSG, Urteil vom 02.11.2010 – B 1 KR 12/10 R, juris-Rn. 18.

1.4.3.1.3 Art der Daten

Die vom Leistungsträger erhobenen Abrechnungs- und Behandlungsdaten enthalten Informationen, die sich auf einen Versicherten und auf den jeweiligen Leistungserbringer und damit auf identifizierte oder identifizierbare natürliche Personen beziehen. Aus den Daten mit Versichertenbezug lassen sich Informationen über den Gesundheitszustand des Versicherten ableiten. Es handelt sich damit um **Gesundheitsdaten** im Sinne des Art. 4 Nr. 15 DSGVO, die als besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO wegen ihrer unterstellten besonderen Sensibilität nur unter erhöhten Voraussetzungen verarbeitet werden können.

1.4.3.1.4 Auswertung als Datenverarbeitung

Die Auswertung der Sozialdaten durch den Leistungsträger stellt einen Datenverarbeitungsvorgang im Sinne des § 67b SGB X dar. Hierbei ist zu berücksichtigen, dass anstelle der bisher in § 67b SGB X a.F. verwendeten Begriffe „Verarbeitung" und „Nutzung" (vgl. § 67 Abs. 6, 7 SGB X a.F.) in der neuen Fassung von der „Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung" die Rede ist, weil „Verarbeitung" nunmehr gemäß Art. 4 Nr. 2 DSGVO als Oberbegriff für alle Datenumgänge umfassender definiert ist als:

> *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung"*

Die Auswertung der Sozialdaten durch den Leistungsträger beinhaltet insbesondere das Auslesen und Verwenden der Daten, um bestimmte Auswertungsergebnisse und Statistiken zu erzielen. Insoweit fällt die Auswertung der Sozialdaten jedenfalls unter den Verarbeitungsbegriff der DSGVO.

§ 67b SGB X soll nach der Gesetzesbegründung alle Verarbeitungsvorgänge „außerhalb der Erhebung" erfassen.[55] Bei der Anpassung des Sozialdatenschutzrechts an die DSGVO sollte der bisherige Anwendungsbereich der Ermächtigungsnorm beibehalten werden.[56] Nach bisherigem Recht war in § 67 Abs. 7 SGB X a.F. der Begriff „Nutzung" neben den Begriffen „Erheben" und „Verarbeiten" als Auffangtatbestand enthalten. Wurden Sozialdaten mit einer

55 Vgl. BT-Drs. 18/12611, S. 111f.
56 Vgl. BT-Drs. 18/12611, S. 111.

Zweckbestimmung ausgewertet, zusammengestellt oder auf sonstige Art zur Kenntnis genommen, lag ein Nutzen von Sozialdaten vor.[57] Die neue Vorschrift ist daher so zu verstehen, dass die Auswertung der Sozialdaten durch den Leistungsträger jedenfalls unter den Begriff der **Nutzung im Sinne des § 67b SGB X** fällt. Dass Art. 4 Nr. 2 DSGVO den Begriff der Nutzung nicht ausdrücklich erwähnt, dürfte unschädlich sein, da die dort genannten Unterfälle lediglich beispielhaft („wie") sein dürften und die abweichende Begriffsnutzung im SGB jedenfalls dem Verarbeitungsbegriff unterfällt und daher den Anwendungsbereich der DSGVO nicht einschränkt.

1.4.3.2 Gesetzliche Ermächtigung

1.4.3.2.1 Nutzung zu Forschungszwecken (§ 287 SGB V)

§ 287 SGB V erlaubt den Krankenkassen – unter Einhaltung der nachfolgend weiter beschriebenen Voraussetzungen – die leistungserbringer- oder fallbeziehbare, selbst durchgeführte Auswertung ihrer Datenbestände für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben. § 287 SGB V lautet:

> *„(1) Die Krankenkassen und die Kassenärztlichen Vereinigungen dürfen mit Erlaubnis der Aufsichtsbehörde die Datenbestände leistungserbringer- oder fallbeziehbar für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben, insbesondere zur Gewinnung epidemiologischer Erkenntnisse, von Erkenntnissen über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen oder von Erkenntnissen über örtliche Krankheitsschwerpunkte, selbst auswerten oder über die sich aus § 304 ergebenden Fristen hinaus aufbewahren.*
>
> *(2) Sozialdaten sind zu anonymisieren."*

Forschungsvorhaben

Unter **Forschung** versteht man die geistige Tätigkeit, mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise **neue** Erkenntnisse zu gewinnen.[58] Sie erfasst insbesondere die Fragestellung der Methodik sowie die Bewertung des Forschungsergebnisses und seine Verarbeitung und bewirkt den Fortschritt der Wissenschaft. Wissenschaft ist wiederum jede Tätigkeit, die nach ihrem Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist.[59] § 287 SGB V nennt beispielhaft und somit nicht abschließend als zulässige Zwecke von Forschungsvorhaben die Gewinnung von

57 Vgl. Bieresborn, in: von Wulffen/Schütze, SGB X, 8. Aufl., 2014, § 67 Rn. 29.

58 Vgl. BT-Drs. V/4335, S. 4; *Sifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 3 m.w.N.

59 BVerfG, Urteil vom 29.05.1973, Az.: 1 BvR 424/71.

- epidemiologischen Erkenntnissen,
- Erkenntnissen über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen,
- von Erkenntnissen über örtliche Krankheitsschwerpunkte.

Nichtmedizinische Fragestellungen

Die Frage, ob **auch nichtmedizinische Fragestellungen** Gegenstand der Forschungsvorhaben sein können, wird unterschiedlich beantwortet. Nach *Kranig* ist dies grundsätzlich zu bejahen, falls das Forschungsvorhaben geeignet ist, Erkenntnisse zu gewinnen, die die Krankenkassen bei Erfüllung ihrer gesetzlichen Aufgaben unterstützen. So seien Forschungen zur Wirksamkeit und Effizienz gesetzgeberischer Neuerungen, z.B. bei Vereinbarungen zur integrierten Versorgung (§§ 140a ff. SGB V) oder bei Einführung der elektronischen Gesundheitskarte (§ 291a SGB V) als zulässig anzusehen. Als Forschungszweck kämen demnach etwa die Verbesserung der getroffenen Maßnahmen oder das Erkennen von Nachbesserungsbedarf durch den Gesetzgeber in Betracht.[60]

Hornung verneint dagegen die Erstreckung auf nichtmedizinische Vorhaben mit der Begründung, dass diese nicht den verfassungsrechtlichen Rechtfertigungsgrund der Vermeidung von Krankheiten erfüllen, spezielle gesetzliche Regeln nicht umgangen werden dürfen und der Gesetzgeber mit den genannten Beispielen eine Typisierung vorgenommen habe.[61] Dieser Rechtsauffassung kann u.E. jedoch aus folgenden Gründen nicht gefolgt werden:

Angesichts der ausdrücklich als nicht abschließend aufgezählten Regelbeispiele („insbesondere") müssen diese gerade nicht als typisierende Einschränkungen verstanden werden. Angesichts der Aufgaben der gesetzlichen Krankenversicherung sowie der Kassen(zahn)ärztlichen Vereinigungen, zu denen auch die Sicherstellung einer wirtschaftlichen Versorgung der Versicherten sowie eines effektiven Leistungsgeschehens gehören, legitimieren die Bestimmungen des § 287 SGB V eine Auswertung (und längere Aufbewahrung) auch für nichtmedizinische Forschung.[62]

Dies gilt auch angesichts der schwierigen Abgrenzbarkeit zwischen medizinischen und nichtmedizinischen Forschungszwecken in diesem Bereich, wie beispielsweise Politikfolgenforschung, die etwa auf Untersuchungen über

- Veränderungen in der Inanspruchnahme von Leistungen (z.B. nach Einführung der Praxisgebühr),
- Veränderungen in der Verordnungsweise (z.B. Wechsel zu verschreibungspflichtigen Präparaten aufgrund veränderter Erstattungsregelungen) oder

60 *Kranig*, in: Hauck/Noftz, SGB V, Stand: 08/2017, § 287 Rn. 6.
61 *Hornung*, in: Hänlein/Schuler, LPK-SGB V, 5. Aufl., 2016, § 287 Rn. 3.
62 *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 4.

- Verlagerungseffekte zwischen dem stationären und ambulanten Sektor (z.B. nach Einführung der DRGs)

gerichtet sind.[63] Es werden hierdurch einerseits Erkenntnisse über die Wirksamkeit und Effizienz von Maßnahmen auf der regulatorischen, nicht-medizinischen Ebene gesammelt. Andererseits lassen sich auf Grundlage dieser Erkenntnis medizinisch begründete Maßnahmen zur Optimierung der medizinischen Versorgung einleiten. Dies gilt etwa auch für die sog. Wissenstransferforschung, die sich etwa mit der Frage befasst, wie schnell und durch welche Arztgruppen neue Verfahren und Behandlungsempfehlungen aufgegriffen werden bzw. welche Patientengruppen diese Behandlung erhalten.[64]

Insbesondere auch angesichts der Vorgaben der DSGVO zur weiten Auslegung der Forschungszwecke dürften auch nichtmedizinische Forschungszwecke vorliegend erfasst sein, soweit Erkenntnisse zur Förderung der öffentlichen Gesundheit gewonnen werden sollen und sonstige Voraussetzungen für die Datenverarbeitung erfüllt werden.

Interne Fragestellungen

Fraglich ist, ob eine Grenze im Rahmen des § 287 SGB V hinsichtlich zulässiger Forschungsvorhaben dort zu ziehen ist, wo die Krankenkasse die Erkenntnisse, die im Rahmen der Vorhaben gewonnen werden, nicht selbst bei Erfüllung ihrer gesetzlichen Aufgaben nutzen kann. Der Wortlaut der Norm erfasst zunächst nur, dass die tatsächliche Durchführung einer Auswertung durch die Krankenkasse selbst passieren muss, sodass jedenfalls eine Auswertung durch Dritte unzulässig ist.[65] Ob die Forschungsfrage ausschließlich krankenkassenintern sein muss, ergibt sich hieraus nicht. Nach Ansichten in der Literatur regelt § 287 SGB V aber die Selbstauswertung der Daten durch die gesetzlichen Krankenkassen zu internen, eigenen Forschungsvorhaben.[66]

Unter anderem wird vertreten, dass Externe als wissenschaftliche Begleitung des (internen) Forschungsprojekts des Leistungsträgers – etwa im Rahmen der Auftragsverarbeitung – hinzugezogen werden.[67] Dies erscheint jedenfalls für Auftragsverarbeiter konsequent, da diese dem Verantwortlichen zugerechnet

63 Vgl. hierzu *Schubert/Köster/Küpper-Nybelen/Ihle*, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, 1095 (1100).

64 Vgl. *Schubert/Köster/Küpper-Nybelen/Ihle*, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, 1095 (1100).

65 *Michels*, in: Becker/Kingreen, SGB V, 5. Aufl., 2017, § 287 Rn. 3.

66 Vgl. *Kranig*, in: Hauck/Noftz, SGB V, Stand: 08/2017, § 287 Rn. 6; *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 4; *Michels*, in: Becker/Kingreen, SGB V, 5 Aufl., 2017, § 287 Rn. 1.

67 Auftrags(daten)verarbeitung als zulässig ansehend: Hornung, in: Hänlein/Schuler, LPK-SGB V, 5. Aufl., 2016, § 287 Rn. 2.; a.A. *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 5. Forschungsinstitute, die von den Krankenkassen oder Kassenärztlichen Vereinigungen getragen werden, nicht als Dritte im Sinne der Norm ansehend: Wenner, in: Eichenhofer/Wenner, SGB V, 2013, § 287 Rn. 4; *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 5.

werden können. Jedenfalls ist es unschädlich, dass vorliegend die konkrete Fragestellung für die Datenauswertung gemeinsam mit der externen Einrichtung entwickelt oder von dieser vorgegeben werden soll. Hierzu führt etwa *Didong* wie folgt aus:

> *„Die in § 287 SGB V vorgesehene eigene Auswertung der Datenbestände durch die Krankenkasse schließt eine wissenschaftliche Begleitung und Auswertung durch beigezogene Dritte nicht aus. Da der Gesetzgeber in § 65 SGB V die wissenschaftliche Auswertung von Modellvorhaben nach den §§ 63, 64 SGB V durch unabhängige Sachverständige vorgesehen hat, ist kein Grund ersichtlich, warum im Rahmen von Forschungsvorhaben nach § 287 SGB V die Auswertung allein durch Mitarbeiter der Krankenkassen oder Kassenärztlichen Vereinigung und nicht in Zusammenarbeit mit fachkundigen Dritten erfolgen soll. Hierdurch kann auch das Ziel von Forschungsvorhaben besser erreicht werden."*[68]

Damit spricht erst recht nichts gegen die Einschaltung von externen Dritten zur Definition des Forschungsvorhabens. Die Auswertung soll vorliegend allein durch die Mitarbeiter des Leistungsträgers ohne Einschaltung Dritter erfolgen.

Datenbestände

Der Leistungsträger darf gemäß § 287 SGB V ausschließlich auf **bereits vorhandene** Datenbestände zurückgreifen. Der Zugriff ist damit auf die bereits zu anderen Zwecken (nach § 284 SGB V) in zulässiger Weise erhobenen und gespeicherten Daten beschränkt.[69] Der Leistungsträger ist nicht befugt, darüberhinausgehende Daten zum Zweck der Forschung zu erheben. § 287 SGB V beschränkt die auswertbaren Daten ferner auf **leistungserbringerbeziehbare und fallbeziehbare** Daten. Leistungserbringerbeziehbar sind Daten, die den Leistungserbringer nicht unmittelbar erkennen lassen, aber bestimmbar machen. Fallbeziehbar sind Daten eines Versicherten, außer den Angaben über persönliche oder sachliche Verhältnisse, welche die Bestimmung des Versicherten erlauben. Eine versichertenbeziehbare Auswertung für Forschungszwecke ist damit ausgeschlossen. Das bedeutet, dass nur Daten ausgewertet werden dürfen, die keine Rückschlüsse auf bestimmte Versicherte erlauben.[70] Es reicht nicht aus, dass die Ergebnisse der Auswertung keine Rückschlüsse darauf zulassen. Selbstredend ist aus der Kombination von Angaben über einen Leistungserbringer und einen konkreten Fall – auch wenn identifizierende Daten wie Name, Adresse und Versichertennummer eines Versicherten nicht in die Auswertung einbezogen werden – eine Bestimmung dieser Person nicht

68 *Didong*, in: jurisPK-SGB V, 3. Aufl., 2016, § 287 Rn. 8.
69 Vgl. *Didong*, in: jurisPK-SGB V, 3. Aufl., 2016, § 287 Rn. 9.
70 *Didong*, in: jurisPK-SGB V, 3. Aufl., 2016, Rn. 9 m.w.N.

völlig ausgeschlossen. Jedenfalls aber ist es auf Basis dieser Angaben nicht zulässig, Versichertenprofile auszuwerten, sondern nur einzelne Behandlungsfälle.

Anonymisierung, § 287 Abs. 2 SGB V

Die Sozialdaten müssen daher anonymisiert werden, wie es § 287 Abs. 2 SGB V fordert.[71] Hierdurch soll insbesondere erreicht werden, dass sie nicht mehr versichertenbeziehbar sind und damit keine Bestimmung eines Versicherten erlauben.[72] Der Zeitpunkt der Anonymisierung ist im Gesetz nicht bestimmt. Entsprechend dem Regelungszweck, bei Forschungsvorhaben nur mit anonymisierten Daten zu arbeiten, ist aber davon auszugehen, dass die Anonymisierung der Sozialdaten spätestens dann erfolgen muss, sobald sie zum Zwecke der Auswertung in das Forschungsvorhaben einbezogen werden.[73]

Die Anonymisierung der Daten muss also **vor** der Auswertung erfolgen, die Daten dürfen nicht personenbezogen ausgewertet werden.[74]

Auslegung des Begriffs der Anonymisierung

Es ist angesichts der Anforderungen an eine Anonymisierung[75] zu berücksichtigen, dass vorliegend die Auswertung der Daten durch die Stelle erfolgt, die diese Daten – mit Personenbezug – selbst erhoben hat.

Eine auch nur *faktische* Anonymisierung der Daten durch Aufhebung des Personenbezugs ist – selbst bei relativem Verständnis des Personenbezugs – nicht möglich, da der Leistungsträger in seiner Gesamtheit grundsätzlich stets Zugriff auf alle seine Datenbestände hat und also die Möglichkeit einer De-Anonymisierung stets gegeben sein wird. D.h., wenn der Leistungsträger vollständige, personenbezogene Datensätze zu einem Zweck vorliegen hat und diese Daten nun zusätzlich in einen zweiten, davon getrennten Datensatz zu Forschungszwecken ohne identifizierende Daten speichert, den ggf. ein anderer Mitarbeiter oder eine andere Abteilung bearbeitet, kann dies nach dem bisherigen Verständnis des Begriffs der Anonymisierung (vgl. § 67 Abs. 8 SGB X a.F.) nicht ausreichen, da das Wissen der gesamten verantwortlichen Stelle maßgeblich ist und nicht nur das einzelner Mitarbeiter. Eine Anonymisierung ist deswegen nur hinsichtlich solcher Daten möglich, die der Leistungsträger für die erhobenen Zwecke nicht mehr benötigt und deswegen

71 Dieses Erfordernis könnte bereits hinsichtlich der Daten, die den Krankenkassen nach § 295 Abs. 1b S. 1 SGB V übermittelt werden, aus § 284 Abs. 3 S. 2 Hs. 2 SGB V folgen, wonach ein „Versichertenbezug vorher" – also vor der zweckändernden Weiterverwendung – „zu löschen" ist. Das betrifft Daten, die nicht über die Kassenärztlichen Vereinigungen, sondern unmittelbar von Leistungserbringern an die Krankenkassen übermittelt werden.

72 Vgl. *Kranig*, in: Hauck/Noftz, SGB V, Stand: 08/2017, § 287 Rn. 8.

73 Leber, in: Orlowski/Rau/Schermer/Wasem/Zipperer, GKV-Kommentar, SGB V, Stand: 08/2017, § 287 Rn. 9.

74 *Michels*, in: Becker/Kingreen, SGB V, 5 Aufl., 2017, § 287 Rn. 5.

75 Vgl. den entsprechenden Abschnitt im Gutachtenteil von Roßnagel im vorliegenden Buch.

löschen kann bzw. muss. Nur wenn davon ausgegangen werden kann, dass das zurechenbare Wissen nicht mehr bei der jeweiligen Krankenkasse vorhanden ist, kann nach bisherigem Verständnis des Begriffs der Anonymisierung eine Auswertung auf Grundlage des § 287 SGB V erfolgen. Wann eine solche Löschung regelmäßig durchzuführen ist, bestimmt § 304 SGB V. Danach sind die Sozialdaten grundsätzlich zu löschen, soweit ihre Kenntnis für die Aufgabenerfüllung des Leistungsträgers nicht mehr erforderlich ist. Lediglich eine Anonymisierung von Daten aus bereits abgeschlossenen Vorgängen und damit von „Altbeständen" ist daher möglich. Dies eröffnet jedoch ausschließlich die Möglichkeit der Nutzung von Altbeständen für Forschungsvorhaben, die sich auf die in Vergangenheit abgeschlossene Fälle beziehen.[76] Eine Anonymisierung der aktuellen Daten des Leistungsträgers, die laufend neu erhoben werden, ist angesichts der Forderung nach jedenfalls faktischer Anonymisierung nicht möglich.

Aus dieser Problematik ergeben sich zwei gegenläufige Rechtsauffassungen über die Reichweite der Erlaubnisnorm in § 287 SGB V:

1. Die Erlaubnisnorm soll nur die Auswertung von Altdatenbeständen ermöglichen.
2. Die Erlaubnisnorm ermöglicht auch die Auswertung nicht abgeschlossener Sachverhalte.

Die erstgenannte Ansicht orientiert sich strikt an dem Wortlaut („Anonymisierung") und wird etwa von *Schifferdecker* vertreten, der hierzu ausführt, dass die Forschungsvorhaben sich nur auf bereits abgeschlossene Vorgänge beziehen können.[77] Andere schließen sich der zweitgenannten Ansicht an und sehen die Auswertung aller – auch aktueller – Datenbestände als zulässig an, wobei – auch unter den Befürwortern dieser Ansicht – grundsätzlich Einigkeit insofern besteht, als auch diese Daten dem Forschungsprojekt nur in anonymisierter Form zugeführt werden dürfen.[78]

Modifiziertes Verständnis der Anonymisierung

Im Sinne der zweitgenannten Ansicht wird zur Ermöglichung der Auswertung aktueller Fälle, in denen laufend neue Daten erhoben werden, ein **modifiziertes Verständnis** von der Anonymisierung im Sinne des § 287 Abs. 2 SGB V entwickelt.

Vorgeschlagen wird insbesondere ein Verschlüsselungsverfahren, bei dem die Verschlüsselungskennziffern den Personen, die im Forschungsvorhaben selbst tätig sind, nicht zur Verfügung gestellt werden dürfen. Die Daten sind dann

76 Vgl. *Kranig*, in: Hauck/Noftz, SGB V, Stand: 08/2017, § 287 Rn. 10.
77 *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 8.
78 Vgl. *Didong*, in: jurisPK-SGB V, 3. Aufl., 2016, Rn. 12.

aus Sicht dieser natürlichen *Person* – im Sinne eines relativen Personenbezugs – anonymisiert. Die am Forschungsprojekt tätigen Personen dürfen hierfür keine Zugriffsrechte auf die Kennziffer und kein rechtliches Mittel zur De-Anonymisierung haben. Hierzu führt *Kranig* wie folgt aus:

> *„Es erscheint hingegen möglich, durch Verwendung von leistungserbringer- oder fallbeziehbaren Kennziffern oder mittels anderer Verschlüsselungsverfahren den Datenfluss vom laufenden Behandlungsfall zum Forschungsvorhaben sicherzustellen, ohne dass Personen, die im Forschungsvorhaben tätig sind, den konkreten Bezug zu einem bestimmten Leistungserbringer oder sogar zu einem bestimmten Versicherten herstellen können."*[79]

Mit ähnlicher Intention führt *Michels* in diesem Zusammenhang aus:

> *„Bei der Zusammenführung unterschiedlicher Datenbestände und in Fällen der zeitlich befristeten Verlaufskontrolle wäre damit eine Zusammenführung leistungserbringer- o. fallbezogener Daten nur im Wege einer Pseudonymisierung (...) außerhalb des Forschungsvorhabens mögl."*[80]

Gegen ein solches, modifiziertes Verständnis der Anonymisierung im Sinne des § 287 Abs. 2 SGB V, wonach eine Pseudonymisierung genügte, argumentiert etwa *Hornung* wie folgt:

> *„Für Forschungsvorhaben an derartigen noch nicht abgeschlossenen Fällen wird teilweise eine* ***Pseudonymisierung*** *vorgeschlagen, z.B. durch Verschlüsselung der Versicherungsnummer (Maaßen/Piepersberg, BArbBl Nr. 4 1989, 48; Kranig in Hauck/Noftz, § 287 Rn 11), ggf. mit Absicherung der Reindividualisierung gemäß § 286 Abs. 3 (s.a. Roß, 3. Auflage, Rn 4). Dies ist* ***strikt abzulehnen*** *(wie hier Krauskopf-Waschull, SozKV, § 287 Rn 20; Fischinger in Spickhoff, Medizinrecht, § 287 Rn 3; Schäfer in Berchtold/Huster/Rehborn, § 287 Rn 6). Schon definitorisch ist zwischen Anonymisieren (§ 67 Abs. 8 SGB X) und Pseudonymisieren (§ 67 Abs. 8a SGB X) zu unterscheiden. Wenn sich der Gesetzgeber dazu entschieden hat, explizit eine der beiden Varianten zuzulassen, so kann dies nicht mit Argumenten praktischer Notwendigkeit überspielt werden (s. Hornung/Roßnagel, 395ff.)."*[81]

Auch *Spindler* verlangt eine strikte Anonymisierung und lässt eine Pseudonymisierung im Rahmen des § 287 Abs. 2 SGB nicht genügen.[82]

79 *Kranig*, in: Hauck/Noftz, SGB V, Stand: 08/2017, § 287 Rn. 11.
80 *Michels*, in: Becker/Kingreen, SGB V, 5 Aufl., 2017, § 287 Rn. 5.
81 Hornung, in: Hänlein/Schuler, LPK-SGB V, 5. Aufl., 2016, § 287 Rn. 7.
82 Vgl. Spindler, MedR 2016, 691 (698).

Stellungnahme

Ließe man eine Pseudonymisierung im Rahmen des § 287 Abs. 2 SGB V nicht genügen, würde die Auswertung der Daten zu Forschungszwecken hinsichtlich nicht abgeschlossener Fälle und damit insbesondere hinsichtlich verlaufsbezogener Untersuchungen und Langzeitstudien in der Regel ausscheiden. Dies wiederum widerspräche den vom Gesetzgeber genannten Beispielen, die gem. § 287 Abs. 1 SGB V erfasst sein sollen. Hierzu führt *Kranig* aus:

> *„Derartige verlaufsbezogene Forschungsvorhaben sind gerade für die beispielhaft im Gesetz genannten Zwecke der epidemiologischen Untersuchungen der Untersuchung arbeitsbedingter Erkrankungen besonders wichtig. Es kann nicht davon ausgegangen werden, dass der Gesetzgeber diese verlaufsbezogenen Forschungsvorhaben unterbinden wollte. Weder ist dies daraus zu schließen, dass nur die Auswertung (vorhandener) Datenbestände zulässig ist (vgl. Rz 7), denn dies soll nur die Datenerhebung eigens für Forschungsvorhaben verhindern; noch ergibt sich dies daraus, dass die Forschungsvorhaben zeitlich befristet sein müssen; vielmehr deutet gerade die zeitliche Befristung von Forschungsvorhaben darauf hin, dass diese sich nicht auf in der Vergangenheit abgeschlossene Fälle beschränken müssen. Sind mithin verlaufsbezogene Forschungsvorhaben grundsätzlich zulässig, so müssen sie auch – unter Wahrung der datenschutzrechtlichen Gesichtspunkte – sinnvoll durchführbar sein. Wenn Kramer, GK-SGB V, § 287 Rz 4, im Anschluss an die Ausführungen zur Anonymisierung der Daten ausführt, ‚eine sinnvolle leistungserbringerbeziehbare Auswertung der Datenbestände (komme) damit praktisch kaum in Betracht', so wird dies dem Willen des Gesetzgebers, interne Forschungsvorhaben der Krankenkassen und Kassen(zahnärztlichen) Vereinigung unter Wahrung des Datenschutzes zu ermöglichen, nicht gerecht."*[83]

Die Argumentation ist insofern überzeugend, als gerade die epidemiologischen Untersuchungen und solche über arbeitsbedingte Erkrankungen verlaufsbezogene Forschung unter Zugriff auf die laufende leistungserbringer- oder fallbezogene Datenerhebung erfordern. Es geht hierbei um Untersuchungen hinsichtlich Verbreitung sowie Ursachen und Folgen von gesundheitsbezogenen Zuständen und Ereignissen in Bevölkerungen und Populationen. So schreiben Schubert/Köster/Küpper-Nybelen/Ihle zu Nutzungsmöglichkeiten der GKV-Routinedaten im Rahmen der Forschung u.a.:

> *„Mithilfe von versichertenbezogenen pseudonymisierten Bestandsdaten lassen sich aufgrund des vorhandenen Bevölkerungsbezugs administrative Prävalenz- und Inzidenzschätzungen nach soziodemographischen Variablen – in der Linie nach Alter und Geschlecht – anhand der ambulanten und/oder stationären Diagnosen vornehmen und auf Vergleichspopulationen standardisieren. (...) Auf der Basis kontinuierlich erhobener Daten sind Fortschreibungen dieser administrativen Prävalenzen und*

83 Kranig, in: Hauck/Noftz, SGB V, Stand: 08/2017, § 287 Rn. 11 m.w.N.

Inzidenzen und – bei Betrachtung mehrerer Jahre – Berechnungen des Alterseffektes möglich.“[84]

sowie:

„Des Weiteren sind Versorgungsmuster von Interesse, zu deren Darstellung es längsschnittlich erhobener Daten über einen längeren Zeitraum bedarf (z.B. Definition und Beobachtung einer Kohorte von Versicherten).“[85]

und:

„Versorgungsforschung befasst sich sowohl mit den Folgen gesetzlicher und ordnungspolitischer Maßnahmen für das Versorgungssystem (Stichwort: Politikfolgenforschung) als auch mit dem Transfer wissenschaftlicher Erkenntnisse in den Alltag der Versorgung. Hier kommt den über einen längeren Zeitraum vorliegenden Routinedaten ebenfalls ein hoher Stellenwert zu, da auch nach Einführung einer Maßnahme (z.B. DMP, DRG, Praxisgebühr, Warnhinweise für Arzneimittel, Implementierung von Leitlinien, Rabattverträge) Daten für einen Zeitraum oder Zeitpunkt vor der Maßnahme/dem zu beobachtenden Ereignis (rückwirkend) erhoben und die Auswirkungen auf die Inanspruchnahme oder Art der Leistungen beschreiben und je nach Studiendesign auch kausal erklärt werden können.“[86]

Diese Ausführungen zeigen beispielhaft, dass die Bestandsdaten des Leistungsträgers gerade auch durch den Rückgriff auf den fortwährenden Bestand mit jeweils neuen Daten besondere Vorteile im Rahmen von verlaufsbezogenen Forschungen bieten, dadurch die Gesetzgeber intendierten Langzeitbeobachtungen überhaupt erst möglich sind sowie retro- und prospektive Beobachtungen durchgeführt werden können. Dabei liegt der Vorteil der Daten von gesetzlichen Krankenkassen insbesondere auch in ihrer Vollständigkeit und in der fehlenden Selektion in Bezug auf etwa eine Verweigerung der Datennutzung, sodass über alle Versicherten Aussagen getroffen werden können.[87] Hierzu *Leber*:

*„**Eine – je nach den Besonderheiten des Forschungszwecks unter Umständen sogar unverzichtbare – reversible Anonymisierung ist daher zulässig.** Die Verpflichtung zur Anonymisierung von Sozialdaten erschwert die Durchführung von Forschungsvorhaben, die behandlungsfallbezogene Verlaufsbeobachtungen über einen*

84 *Schubert/Köster/Küpper-Nybelen/Ihle*, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, 1095 (1096).

85 *Schubert/Köster/Küpper-Nybelen/Ihle*, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, 1095 (1098).

86 *Schubert/Köster/Küpper-Nybelen/Ihle*, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, 1095 (1100).

87 *Schubert/Köster/Küpper-Nybelen/Ihle*, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, 1095 (1102).

längeren Zeitraum hinweg zum Gegenstand haben, da die Zuordnung neu hinzutretender Behandlungsdaten zu bereits anonymisierten Daten des Behandlungsfalls ohne Kenntnis des Personenbezugs nicht möglich ist. Insoweit ist eine datentechnisch mögliche Verschlüsselung des Personenbezuges – etwa durch getrennt zu speichernde personenbezogene Merkmale – geboten, die eine Deanonymisierung ausschließlich zum Zwecke der behandlungsfallbezogenen Zuordnung unter datenschutzrechtlich abgesicherten Vorkehrungen gegen Missbrauchsmöglichkeiten zulässt. Die Einzelheiten eines solchen Verfahrens sind vor allem im Hinblick auf einen ausreichenden Schutz der Sozialdaten mit der Aufsichtsbehörde (...) – zweckmäßigerweise unter Beteiligung des zuständigen Datenschutzbeauftragten – abzustimmen."[88] *[Hervorhebung nicht im Original]*

Vor diesem Hintergrund erscheint es u.E. sachgerecht, die Frage nach den Anforderungen der Anonymisierung im Sinne des § 287 Abs. 2 SGB V jeweils aus dem Blickwinkel der die Daten auswertenden Person bzw. Abteilung zu beurteilen. Wird den Personen bzw. der Abteilung, die das Forschungsvorhaben durch die Auswertung der Daten durchführen, kein Mittel zur Re-Identifizierung (De-Anonymisierung) der Daten zur Verfügung gestellt, so handelt es sich aus deren Sicht um anonyme Daten. Dieses Ergebnis entspricht nicht nur den oben erwähnten praktischen Bedürfnissen, sondern auch der real gelebten Wirklichkeit innerhalb eines Leistungsträgers mit unterschiedlichen Abteilungen, die jeweils unterschiedliche Aufgaben zu erfüllen haben.

Zudem ist eine entsprechende Handhabung, bei der zwischen unterschiedlichen Stellen und Personen innerhalb eines Amtes unterschieden wird, etwa aus den Vorgaben zur Geheimhaltung über Personendaten, die für eine Bundesstatistik gemacht werden, grundsätzlich bekannt (§ 16 Abs. 2 S. 1 Bundesstatistikgesetz).

Zu fordern ist aber angesichts der bestehenden Unsicherheiten in jedem Fall eine räumlich, organisatorisch und personell eigenständige Forschungsabteilung des Leistungsträgers. In dieser Forschungsabteilung tätigen Personen dürfen etwa nicht auch in den anderen Abteilungen des Leistungsträgers eingesetzt werden und im Zusammenhang mit anderen Aufgaben Zugriff auf die nicht anonymisierten Daten haben.

Erlaubnis der Aufsichtsbehörde

Die Auswertung der Daten für Forschungsvorhaben bedarf der vorherigen Erlaubnis der Aufsichtsbehörde. Dies wird ausführlich in Kapitel 1.4.5 behandelt.

88 *Leber* in: Orlowski/Rau/Schermer/Wasem/Zipperer, GKV-Kommentar, SGB V, Stand: 08/2017, § 287 Rn. 9f.

Zwischenergebnis und Vereinbarkeit mit der DSGVO

Unter Beachtung der aufgezeigten Voraussetzungen ist die Datenverarbeitung durch den Leistungsträger für Forschungszwecke damit gemäß § 67b Abs. 1 S. 1, 2 SGB X i.V.m. § 284 Abs. 3, § 287 SGB V zulässig.

Art. 9 Abs. 2 DSGVO erlaubt gerade für den Gesundheitssektor die Verarbeitung sensibler Daten bei einem erheblichen öffentlichen Interesse, wozu insbesondere wissenschaftliche Forschung (lit. j) gehört. Die dargestellten strengen Anforderungen an die Auswertung der Daten durch den Leistungsträger sowie die von diesem nach Art. 89 Abs. 1 DSGVO zu gewährenden Garantien tragen der besonderen Sensibilität dieser Daten bei der Verarbeitung zu Forschungszwecken Rechnung.

Es gibt keine Anhaltspunkte für eine Unvereinbarkeit der Erlaubnisvorschrift in § 287 SGB V mit der DSGVO und daher auch keinen Anlass für Änderungen des § 287 SGB V zur Anpassung an die DSGVO.[89] Insbesondere dürfen die Mitgliedsstaaten den Schutzstandard der DSGVO verändern und die Verarbeitung gesundheitsbezogener Daten beschränken (Art. 9 Abs. 4 DSGVO).

Die Bundesrepublik Deutschland wäre aber auch nicht daran gehindert, die Bestimmungen des § 287 SGB V zugunsten der medizinischen Forschung – wiederum unter Berücksichtigung der Vorgaben der DSGVO (insbesondere des Art. 89 DSGVO) – zu lockern.[90] Angesichts der in Folge der aufgezählten Beschränkungen restriktiven Möglichkeiten der Datenauswertung im Rahmen dieser Erlaubnisvorschrift hat bereits *Leber* 2005 unter Verweisung auf die geschafften verbesserten Bedingungen für die Beteiligten zur Datenverarbeitung und -nutzung nach den Datentransparenzregelungen in §§ 303a bis 303f SGB V die praktische Bedeutung von § 287 SGB V infrage gestellt.[91]

Jedenfalls wäre es wünschenswert, wenn der Gesetzgeber den Streit um die Bedeutung der Anonymisierung gemäß § 287 Abs. 2 SGB beilegen würde und die Anforderungen hieran dahingehend klarstellte, dass die nicht abgeschlossenen Sachverhalte erfasst sind und beispielsweise nicht mehr der Begriff der Anonymisierung verwendet wird. Stattdessen könnte eine umschreibende Formulierung verwendet oder der Begriff der „formalen" Anonymisierung, dem Vorbild des § 5a Abs. 3 Bundesstatistikgesetzes folgend, eingeführt werden.

1.4.3.2.2 Weitergehende Nutzung zu Forschungszwecken (§ 67c Abs. 2 Nr. 2 SGB X)

Es stellt sich die Frage, ob eine Nutzung der Sozialdaten zu Forschungszwecken durch die Krankenkassen auch über den Rahmen des § 287 SGB V hinaus

89 Vgl. auch *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 2.
90 Auch *Spindler*, MedR 2016, 691 (699).
91 *Leber*, in: Orlowski/Rau/Schermer/Wasem/Zipperer, GKV-Kommentar, SGB V, Stand: 08/2017, § 287 Rn. 10.

zulässig ist. In Betracht käme hier eine Verarbeitung personenbezogener Sozialdaten nach § 67c Abs. 2 Nr. 2 SGB X.

Wie oben bereits ausgeführt, kommt den spezielleren Normen aus dem bereichsspezifischen Sozialdatenschutzrecht der Fachbücher des SGB (insb. SGB V) keine generelle Sperrwirkung bezüglich der Vorschriften des SGB I und SGB X zu. Vielmehr gehen die Regelungen des SGB V den allgemeinen Bestimmungen nur vor, soweit sie einen einzelnen Teilbereich spezifisch regeln. In diesem Zusammenhang ist fraglich, inwieweit § 287 SGB V eine Sperrwirkung für den Bereich der wissenschaftlichen Forschung mit Sozialdaten durch die Krankenkassen bewirkt und eine parallele Anwendbarkeit des § 67c Abs. 2 Nr. 2 SGB X ausschließt. § 287 SGB X regelt die Voraussetzungen für die Verwendung der vorhandenen Datenbestände durch den Leistungsträger selbst. Nach verbreiteter Meinung der Literatur stellt § 287 SGB V eine lex specialis für den Bereich der Eigenforschung der Krankenkassen mit Sozialdaten, insbesondere im Verhältnis zu § 67c Abs. 5 SGB X dar.[92] Ein Rückgriff auf die allgemeinen Verarbeitungstatbestände zur Legitimation der Verarbeitung weiterer personenbezogener Daten zu Forschungszwecken schiede damit aus.

Das Verhältnis der beiden Normen ließe sich auch anders interpretieren, denn der Grundsatz des „lex specialis derogat legi generali" fordert eine Tatbestandskongruenz. Nur dann kann die allgemeinere Regel nicht mehr zur Anwendung gebracht werden. Da § 287 SGB V aber nicht nur erhöhte Anforderungen an die Verarbeitung zu Forschungszwecken aufstellt, sondern zugleich eine „leistungserbringer- oder fallbeziehbare" Auswertung ermöglicht und zudem nur den Fall der Selbstauswertung regelt, könnte angenommen werden, dass der Fall einer nicht „leistungserbringer- oder fallbezogenen" Fremdforschung durch die Norm gerade nicht geregelt und daher auch ein Rückgriff auf die allgemeinen Forschungstatbestände des SGB X nicht ausgeschlossen sein muss. Von der Literatur wird eine solche Auslegung bisher nicht gestützt, allerdings wird ihr auch nicht direkt widersprochen.

Betrachtet man dies vor dem Hintergrund der geänderten datenschutzrechtlichen Rahmenbedingungen durch die DSGVO, die eine weitgehende Privilegierung der wissenschaftlichen Forschung zum Leitprinzip erklärt, könnte auch dieser neue Rechtsrahmen Anlass zu einer verarbeitungsfreundlicheren Interpretation des § 287 SGB V bieten. Vom Willen des deutschen Gesetzgebers kann diese Interpretation freilich noch nicht gedeckt sein. Im Zuge einer zu erwartenden Anpassungsgesetzgebung könnte der Gesetzgeber aber den Weg für eine weitergehende Verarbeitung öffnen. Bis dahin wird man mit der wohl herrschenden Meinung einen Rückgriff auf § 67c SGB X bezüglich Forschungsvorhaben verneinen können. Infolge dieser Sperrwirkung käme § 67c Abs. 2

92 Vgl. *Schifferdecker*, in: Kasseler Kommentar, Sozialversicherungsrecht, 2017, § 287 SGB V Rn. 2; Leber, in: Orlowski/Rau/Schermer/Wasem/Zipperer, GKV-Kommentar, SGB V, Stand: 08/2017, § 287 Rn. 1.

Nr. 2 SGB X vorliegend lediglich für die Auswertung der Sozialdaten **zur Planung im Sozialleistungsbereich** in Betracht.

1.4.3.2.3 Nutzung zu Planungszwecken (§ 67c Abs. 2 Nr. 2 SGB X)

Gemäß § 67c Abs. 2 Nr. 2 SGB X dürfen die nach Abs. 1 gespeicherten Daten von dem Leistungsträger für andere als die gespeicherten Zwecke genutzt werden, wenn es zur Durchführung eines bestimmten Vorhabens der Planung im Sozialleistungsbereich **erforderlich** ist und die **Voraussetzungen des § 75 Abs. 1, 2 oder 4a S. 1 SGB X**[93] vorliegen.[94]

Planung im Sozialleistungsbereich

§ 67c Abs. 2 Nr. 2 SGB X ermöglicht die Nutzung zu bestimmten Vorhaben der Planung im Sozialleistungsbereich. Sozialleistungen sind die im SGB vorgesehenen Dienst-, Sach- und Geldleistungen. Der Begriff der Planung umschreibt die Festlegung künftigen Verhaltens auf der Grundlage der Abschätzung künftiger Tatsachen anhand gegenwärtiger oder vergangener Tatsachen. Die Auswertung der Tatsachen muss stets zu einem bestimmten Zweck erfolgen.[95]

Erforderlichkeit

Die Nutzung der zu anderen Zwecken erhobenen und gespeicherten Daten kann für ein bestimmtes Planungsvorhaben im Sozialleistungsbereich erfolgen, wenn sie für das Planungsvorhaben erforderlich ist. Angesichts der

93 § 75 Abs. 1 SGB X lautet: *„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."
§ 75 Abs. 2 SGB X lautet: „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."
§ 75 Abs. 4a Satz 1 SGB X lautet: *„Ergänzend zur Übermittlung von Sozialdaten zu einem bestimmten Forschungsvorhaben nach Absatz 1 Satz 1 kann die Verwendung dieser Sozialdaten auch für noch nicht bestimmte, aber inhaltlich zusammenhängende Forschungsvorhaben des gleichen Forschungsbereiches beantragt werden."*

94 Dem Rückgriff auf § 67c Abs. 2 Nr. 2 SGB X steht auch § 284 Abs. 3 S. 1 SGB V nicht entgegen, da dieser keine Sperrwirkung hinsichtlich allgemeinerem Datenschutzrecht des SGB X entfaltet.

95 Vgl. *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 18.

weiten Fassung der Erlaubnisvorschrift kommt der Prüfung der Erforderlichkeit eine besondere Bedeutung zu.[96]

Aus der Erforderlichkeit ergibt sich bereits die Eingrenzung des Datenumfangs. So ist die Nutzung individualisierbarer Daten nicht zulässig, soweit eine Anonymisierung bzw. Aggregierung der Daten zumutbar ist. Diese Voraussetzung wird im Rahmen des Szenarios bereits dadurch eingehalten, dass die Daten vor der Auswertung anonymisiert werden (im Sinne des modifizierten Verständnisses der Anonymisierung innerhalb des Leistungsträgers, hierzu s.o.).

Ferner verlangt die Erforderlichkeit die Begrenzung auf Sozialdaten, die der Planer in der betreffenden Phase des Planungsvorhabens unbedingt haben muss.[97]

Interessenabwägung (§ 75 Abs. 1 S. 1 SGB X)

Für die Nutzung zu Planungszwecken müssen die Voraussetzungen von § 75 Abs. 1 SGB X vorliegen. Insbesondere dürfen schutzwürdige Interessen des Betroffenen nicht beeinträchtigt sein **oder** das öffentliche Interesse an der Planung muss das Geheimhaltungsinteresse der betroffenen Person erheblich überwiegen. Abzuwägen sind daher nicht nur Beeinträchtigungen des einzelnen Betroffenen, sondern auch aller Betroffenen zusammen gegen den Nutzen, der aus der Durchführung des Planungsvorhabens zu erwarten ist.[98]

Bei Vorliegen entsprechender Anhaltspunkte ist in jedem Einzelfall eine mögliche Beeinträchtigung zu prüfen.[99] Zu berücksichtigen sind sowohl objektive als auch subjektive Gesichtspunkte. Hierbei ist eine Prognose über mögliche Folgen einer Datennutzung für den Betroffenen zu stellen. Schutzwürdige Belange können demnach beeinträchtigt werden, wenn aus objektiver Sicht unter Zugrundelegung durchschnittlicher Verhältnisse Nachteile für den Betroffenen zu befürchten sind (z.B. als sensitive Zusatzinformationen, dass der Aufenthalt des Betroffenen in einem Landekrankennaus feststellbar ist).[100] Eine Beeinträchtigung kommt auch in Betracht, wenn aufgrund besonderer Umstände Nachteile entstehen können, z.B. wenn der Informationsgehalt dieser Daten für den Betroffenen unter Berücksichtigung seiner psychischen Belange kritisch ist.

Grundsätzlich kommt auch bei Beeinträchtigung schutzwürdiger Interessen die Zulässigkeit der Datennutzung in Betracht, wenn das öffentliche Interesse das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. Allerdings kann dieser Ausnahmetatbestand nur bei Forschungsvorhaben greifen.

96 Vgl. *Bieresborn*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 6.
97 Vgl. *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 22.
98 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 25.
99 Vgl. *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 25.
100 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 28.

Soweit das öffentliche Interesse an der Planung angesprochen ist, dürfte ein Redaktionsversehen vorliegen, da die Planung im Sozialleistungsbereich durch den Leistungsträger stets im öffentlichen Interesse erfolgt.[101]

Vorrang der Einwilligung (§ 75 Abs. 1 S. 2 SGB X)

§ 75 Abs. 1 S. 2 SGB X bestimmt, dass vor einer Übermittlung eine Einwilligung der betroffenen Person einzuholen ist. Da die Verweisung in § 67c Abs. 2 Nr. 2 SGB X ausdrücklich „§ 75 Absatz 1, 2 oder 4a Satz 1" benennt, ist davon auszugehen, dass mit der Verweisung auf Absatz 1 nicht lediglich Satz 1 des Absatzes gemeint ist, sondern auf alle Regelungen des Absatzes 1 verwiesen wurde. Wäre dies nicht gewollt, wäre die Verweisung – wie in Absatz 4a – auf einen bestimmten Satz beschränkt. Der Vorrang der Einwilligung gilt insofern auch in vorliegender Konstellation.[102] Hiervon besteht nur dann ein Dispens, wenn die Einholung unzumutbar ist. Die Zumutbarkeit ist dabei nicht bereits deswegen zu verneinen, weil ein nicht unerheblicher Verwaltungsaufwand erforderlich ist, um die Anforderungen der Vorschrift zu erfüllen.[103]

Eine Einwilligung ist gemäß § 75 Abs. 1 S. 3 SGB X zudem nicht erforderlich, wenn Angaben über den Namen und Vornamen, die Anschrift, die Telefonnummer oder die für die Einleitung eines Vorhabens nach Satz 1 zwingend erforderlichen Strukturmerkmale der betroffenen Person **für Befragungen** betroffen sind.

Keine Anwendbarkeit des § 67c Abs. 5 SGB X

Die Vorgaben des § 67c Abs. 5 SGB X, wonach Daten, die für Zwecke der Planung im Sozialleistungsbereich erhoben und gespeichert wurden, nur für bestimmte Vorhaben verändert oder genutzt werden dürfen, alsbald anonymisiert und bis dahin getrennt gespeichert werden müssen, ist bereits nach dem Wortlaut in der vorliegenden Konstellation nicht einschlägig. § 67c Abs. 5 SGB X lautet:

> *„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. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Planungszweck dies erfordert."*

101 Vgl. *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 29f.
102 Zu den Voraussetzungen der Einwilligung s. Kap. 1.4.3.3.
103 Vgl. *Bieresborn*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 6ff. m.w.N.

Vorliegend geht es um im Rahmen des § 284 Abs. 1 SGB V erhobene und gespeicherte Daten. Sie wurden somit nicht bereits für Zwecke der Planung im Sozialleistungsbereich erhoben und gespeichert. Eine Zweckänderung soll aber derart möglich sein, dass für Zwecke der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich erhobene und gespeicherte Daten für **andere Vorhaben** der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich verwendet werden können.[104]

Missverständlich ist angesichts des klaren Wortlauts die ihr widersprechende Gesetzesbegründung. Demnach soll das geltende Recht zwar beibehalten werden. Dann heißt es aber:

> *„Demnach können die verantwortlichen Datenerheber (Erstverarbeiter) die personenbezogenen Daten, die ursprünglich für einen* ***anderen Zweck erhoben wurden, für Forschungszwecke weiterverarbeiten****. Die in § 35 SGB I genannten Stellen dürfen die Sozialdaten, die sie ursprünglich bei der Erfüllung ihrer gesetzlichen Aufgaben erhoben haben, für Forschungszwecke verändern oder nutzen. Mit der Pflicht zur Anonymisierung von Sozialdaten, sobald dies nach dem Forschungs- oder Planungszweck möglich ist, wird dem informationellen Selbstbestimmungsrecht Rechnung getragen."*[105] *[Hervorhebung nicht im Original]*

Der Wortlaut einer Vorschrift stellt allerdings die Grenze der Auslegung dar. Somit greift Absatz 5 im vorliegenden Fall, in dem die Daten nicht zu Forschungs- und Planungszwecken erhoben werden, nicht ein. Fraglich ist aber angesichts der unmittelbaren Geltung der DSGVO, ob die Vorgaben des Absatzes 5 nicht trotzdem beachtet werden müssen. In Art. 89 DSGVO sind Anforderungen an die Zulässigkeit zweckändernder Nutzung sensibler Daten enthalten. Erforderlich sind demnach Garantien für die Datensicherheit, mit denen sichergestellt ist, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören. Insofern bilden die Anforderungen gemäß § 67c Abs. 5 SGB X – wie laut der Gesetzesbegründung beabsichtigt – die Vorgaben des Art. 89 DSGVO ab. In Satz 2 heißt es insbesondere, dass die Sozialdaten zu anonymisieren sind, sobald dies nach dem Forschungs- oder Planungszweck möglich ist.

Allerdings ist der Rückgriff auf die Regelungen § 67c Abs. 5 SGB X nicht erforderlich. Denn die Vorgaben der DSGVO wurden im Rahmen der hier maßgeblichen Erlaubnisnorm (§ 67c Abs. 2 Nr. 2 SGB X) bereits durch die Verweisung auf die oben dargestellten Regelungen in § 75 Abs. 1. SGB X eingehalten.

104 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 67c Rn. 61.
105 BT-Drs. 18/12611, S. 114.

Keine Anwendbarkeit des § 75 Abs. 2 und Abs. 4a S. 1 SGB X

Ferner verweist § 67c Abs. 2 Nr. 2 SGB X auf die Voraussetzungen des § 75 Abs. 2 *oder* 4a S. 1 SGB X. Durch die Verweisungen auf den Abs. 2 und Abs. 4a S. 1 des § 75 SGB X soll sichergestellt werden, dass die betroffenen Stellen die in § 75 SGB X geregelten neuen Verarbeitungsbefugnisse in Anspruch nehmen können.[106] Neu geschaffen wurden die Möglichkeiten im Bereich der Forschungsfolgefragen (§ 75 Abs. 2 SGB X) und hinsichtlich noch nicht bestimmter Forschungsvorhaben des gleichen Forschungsbereichs (§ 75 Abs. 4a SGB X).

Die Vorschriften betreffen nach ihrem Wortlaut die Nutzung der Daten allein zu Forschungszwecken, Planungszwecke sind hiervon nicht erfasst. Dies ergibt sich hinsichtlich § 75 Abs. 2 SGB X auch aus der Gesetzesbegründung, in der es um Datennutzung durch „Forscher bzw. Forschungseinrichtungen" geht.[107]

Die Gesetzesbegründung zu § 75 Abs. 4a SGB X ist dagegen widersprüchlich, weil sie einerseits auf den „Bereich der Forschung und Planung", andererseits nur auf „Forschungsvorhaben" und nicht auf Planungsvorhaben, abstellt.[108] Es ist davon auszugehen, dass es sich hierbei um ein Redaktionsversehen handelt und – entsprechend dem Wortlaut – nur hinsichtlich der Datennutzung zu Forschungszwecken erweiterte Möglichkeiten vorgesehen werden sollten. Dies ergibt sich insbesondere auch angesichts des Hintergrundes der Neuregelung in Abs. 4a SGB X, mit der die Wertung des Erw.Gr. 33 der DSGVO aufgegriffen werden soll.[109] Dort heißt es:

> *„Oftmals kann zum Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es den 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 die Gelegenheit erhalten, ihre Einwilligung nur für bestimmte Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen."*

Diese Ausführungen können auf den Forschungsbereich übertragen werden, was ausweislich der Ausführungen in der Gesetzesbegründung vom Gesetzgeber auch beabsichtigt war.

Für die vorliegend interessierende Auswertung der Daten durch den Leistungsträger zu Planungszwecken kommt es somit auf die Voraussetzungen des § 75 Abs. 2 und 4a S. 1 SGB X nicht an.

106 BT-Drs. 18/12611, S. 114.
107 Vgl. BT-Drs. 18/12611, S. 118.
108 BT-Drs. 18/12611, S. 119.
109 Vgl. BT-Drs. 18/12611, S. 119.

Diese Verweisungen betreffen jeweils Möglichkeiten und Voraussetzungen der Datennutzung zu Forschungszwecken und sind im Übrigen vorliegend auch für die Datennutzung zu Forschungszwecken wegen der vorrangigen Geltung des § 287 SGB V für die (Eigen-)Auswertung der Daten durch den Leistungsträger nicht einschlägig.

Anforderungen an i.R.d. § 295 Abs. 1b S. 1 SGB V übermittelte Daten (§ 284 Abs. 3 S. 2 SGB V)

Darüber hinaus statuiert § 284 Abs. 3 S. 2 SGB V[110] eine Pflicht zur Löschung des Versichertenbezugs vor der Auswertung der Daten durch den Leistungsträger, wenn es sich bei den zu übermittelnden Daten um solche handelt, die gemäß § 295 Abs. 1b S. 1 SGB V von den Leistungserbringern übermittelt wurden. So können versichertenbezogene Abrechnungsdaten, die die Krankenkasse etwa im Zusammenhang mit einem Vertrag zur integrierten Versorgung ohne Beteiligung der kassenärztlichen Vereinigung von den Leistungserbringern erhalten hat, für außerhalb von § 284 Abs. 1 S. 1 Nr. 4, 8–14 und § 305 Abs. 1 SGB V liegende Zwecke – folglich auch für Zwecke der wissenschaftlichen Forschung, der Planung und der Qualitätssicherung – nicht an Dritte übermittelt werden. Vielmehr ist der Versichertenbezug vor einer Übermittlung zu diesen Zwecken zu löschen. Ob der Gesetzgeber hier bewusst auf den Terminus der Anonymisierung verzichtet hat, ist unsicher. Folglich ist bei der Übermittlung der Sozialdaten zu Forschungs- und Planungszwecken i.R.v. § 75 SGB X zu unterscheiden, ob es sich um Daten i.S.d. § 295 Abs. 1b S. 1 SGB V handelt oder nicht. Ist Ersteres der Fall, sind die Daten gemäß § 284 Abs. 3 S. 2 Hs. 2 SGB V zwingend vom Versichertenbezug zu befreien.

Vereinbarkeit mit der DSGVO

Eine Unvereinbarkeit der Erlaubnisnormen (§ 67b Abs. 1 S. 1, 2 SGB X i.V.m. § 284 Abs. 3 SGB V, § 67c Abs. 2. Nr. 2 SGB X) mit der DSGVO ist nicht ersichtlich. Die Zulässigkeit einer nationalen Norm zur zweckändernden Verarbeitung von Gesundheitsdaten folgt aus Art. 9 Abs. 2 lit. h) bzw. j) DSGVO. Die Zulässigkeit ist daher zum einen an die Bedingungen und Garantien gem. Art. 9 Abs. 3 (lit. h]) sowie an die Anforderungen des Art. 89 DSGVO (lit. j) geknüpft. Vorliegend dürften die Voraussetzungen des Art. 89 DSGVO durch die Verweisung auf die einschränkenden Regelungen aus § 75 SGB X der seinerseits auf § 22 Abs. 2 BDSG verweist, erfüllt werden.

Die Datenverarbeitung zu Planungszwecken im Sinne des § 67c Abs. 2 Nr. 2 SGB X dürfte jedoch (nur) unter die Ausnahmevorschrift in Art. 9 Abs. 2

110 § 284 Abs. 3 S. 2 SGB V lautet: *„Die Daten, die nach § 295 Abs. 1b Satz 1 an die Krankenkasse übermittelt werden, dürfen nur zu Zwecken nach Absatz 1 Satz 1 Nr. 4, 8, 9, 10, 11, 12, 13, 14 und § 305 Abs. 1 versichertenbezogen verarbeitet und genutzt werden und nur, soweit dies für diese Zwecke erforderlich ist; für die Verarbeitung und Nutzung dieser Daten zu anderen Zwecken ist der Versichertenbezug vorher zu löschen."*

lit. h) DSGVO, nicht aber lit. j), fallen. In diesem Fall dürften die Daten gemäß Art. 9 Abs. 3 DSGVO nur verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls einer Geheimhaltungspflicht unterliegt.

Zwischenergebnis

Die Auswertung der Sozialdaten durch den Leistungsträger zu Planungszwecken im Sozialleistungsbereich ist nur unter sehr engen Voraussetzungen zulässig. Vorliegend dürfte die Erlaubnisvorschrift insbesondere deswegen in vielen Fällen greifen, weil die Sozialdaten vor der Auswertung anonymisiert werden sollen und das Personal des Leistungsträgers zur Geheimhaltung verpflichtet ist.

1.4.3.2.4 Nutzung zur Qualitätssicherung (§ 299 SGB V)

Die Auswertung der Sozialdaten zur Qualitätssicherung könnte grundsätzlich auf Grundlage des § 67b Abs. 1, S. 1, 2 SGB X i.V.m. § 284 Abs. 3, § 299 Abs. 1a SGB V zulässig sein. Die Krankenkassen sind gemäß § 299 Abs. 1a SGB V befugt und verpflichtet, nach § 284 Abs. 1 SGB V erhobene und gespeicherte Sozialdaten zu verarbeiten oder zu nutzen, wenn die einzelnen Voraussetzungen der Vorschrift vorliegen.

Neben den in Absatz 1a selbst genannten Voraussetzungen gelten auch die in Absatz 1 Satz 3 bis 7 entsprechend (§ 299 Abs. 1a S. 3). Gemäß § 299 Abs. 1 S. 4 Nr. 2 SGB V muss die Auswertung der Daten von einer unabhängigen Stelle vorgenommen werden, wenn sie nicht die Datenauswertung durch die Kassenärztliche Vereinigung im Rahmen der Qualitätsprüfungen betrifft. Die Vorschrift greift insofern bereits deswegen nicht für die hier interessierende **Selbst**auswertung durch den Leistungsträger.

Dies ergibt sich auch daraus, dass die Auswertung der Daten zu Qualitätssicherungszwecken gemäß § 299 Abs. 1a SGB V in Richtlinien und Beschlüssen des Gemeinsamen Bundesausschusses nach §§ 135b Abs. 2 und 136 Abs. 1 S. 1 SGB V, §§ 136b und 137b Abs. 1 SGB V sowie in Vereinbarungen nach § 137d SGB V vorgesehen sein muss. Dabei müssen in diesen Richtlinien, Beschlüssen und Vereinbarungen gemäß § 299 Abs. 1a S. 3 SGB V u.a. auch die Empfänger der betroffenen Daten festgelegt werden. Ein Empfänger setzt insoweit einen Übermittlungsprozess und keine Selbstauswertung der Daten voraus. In der Gesetzbegründung heißt es hierzu:

> *„In Absatz 1a werden erstmals die Krankenkassen gesetzlich legitimiert und verpflichtet, bestimmte nach § 284 Absatz 1 rechtmäßig erhobene und gespeicherte versicherten- und einrichtungsbezogene Daten für die Zwecke der Qualitätssicherung an den*

*in den Richtlinien **festgelegten Empfänger zu übermitteln**. Damit wird die Möglichkeit geschaffen, im Prozess der Qualitätssicherung auf Versichertenstamm- und Abrechnungsdaten der Krankenkassen zurückzugreifen, soweit diese Rückschlüsse auf die Qualität der Leistungserbringung ermöglichen (z.B. Abrechnungsdaten zu Komplikationen einer Behandlung). Dieser Rückgriff steht allerdings unter der Voraussetzung der Erforderlichkeit für die konkreten Maßnahmen der Qualitätssicherung. Eine entsprechende Richtlinienregelung ist zulässig, wenn sich nach Abwägung der maßgeblichen Aspekte wie Nutzen und Informationsgewinn dieser Daten, Ersparnis gesonderter Datenerhebungen bei weiteren Stellen, Reduzierung von Verwaltungsaufwand und Bestehen weniger eingreifender Alternativen der Informationsbeschaffung sich die konkret vorgesehenen **Datenübermittlungen** der Krankenkassen als vorzugwürdiges Ergebnis erweisen. Entsprechende Erwägungen müssen im Richtlinienbeschluss zum Ausdruck kommen."*[111] *[Hervorhebung nicht im Original]*

Aus den Bestimmungen zur Festlegung des Empfängers und der Gesetzesbegründung ergibt sich letztlich auch, dass es sich bei § 299 Abs. 1a SGB V um eine weitere Erlaubnis- bzw. Verpflichtungsvorschrift hinsichtlich der Übermittlung der Daten durch die Leistungsträger zum Zwecke der Qualitätssicherung an einen Dritten (eine unabhängige Stelle) handelt. Die Selbstauswertung sollte nicht Inhalt der neu geschaffenen Möglichkeiten sein.

Die Selbstauswertung durch den Leistungsträger zum Zwecke der Qualitätssicherung gemäß § 299 Abs. 1a SGB V scheidet insofern aus. Auch anderen Erlaubnisvorschriften sind insoweit nicht ersichtlich.

1.4.3.3 Einwilligung

Neben einer gesetzlichen Ermächtigung kann sich die Zulässigkeit der Verarbeitung aus einer Einwilligung des Betroffenen ergeben (Art. 6 Abs. 1 lit. a] DSGVO, Art. 9 Abs. 2 lit. a] DSGVO), die bei allen hier relevanten Zwecken in Betracht kommt. Während für Einwilligungen nach Art. 6 Abs. 1 lit. a) DSGVO kein Regelungsspielraum der Mitgliedsstaaten verbleibt, da hierfür keine Öffnungsklausel in der DSGVO eingreift, ergibt sich ein solcher für den Bereich der Verarbeitung besonderer Kategorien personenbezogener Daten (im Folgenden auch: sensible Daten) aus der Öffnungsklausel des Art. 9 Abs. 2 lit. a) DSGVO.[112] Diesbezüglich kann sich aus dem Unionsrecht oder dem Recht der Mitgliedsstaaten ergeben, dass das grundsätzliche Verbot der Verarbeitung etwa von Gesundheitsdaten durch eine Einwilligung nicht aufgehoben werden kann. Wenn also eine nationale Vorschrift existiert, die die Einwilligungsmöglichkeit ausschließt, ist die Datenverarbeitung gemäß Art. 9 Abs. 1 DSGVO verboten. Wenn den Mitgliedsstaaten die Regelungsbefugnis zukommt, die Einwilligung vollständig auszuschließen, bedeutet dies allerdings auch, dass

111 BT-Drs. 17/8005, S. 130.
112 Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 316f.

das nationale Recht anstelle eines vollständigen Ausschlusses lediglich engere Voraussetzungen an die Einwilligung, als Minus zum möglichen, vollständigen Ausschluss der Einwilligung, vorgeben kann, als sie in der DSGVO bestimmt sind.[113] Der deutsche Gesetzgeber hat für den hier einschlägigen Bereich zunächst hinsichtlich nicht sensibler Sozialdaten die Einwilligungsmöglichkeit in § 67b Abs. 1 S. 1 SGB X nicht mehr aufgeführt und hinsichtlich der Einwilligung in die Verarbeitung von sensiblen Daten von seiner Regelungskompetenz zum vollständigen Ausschluss der Einwilligung keinen Gebrauch gemacht (vgl. § 67b Abs. 1 S. 2, 3 SGB X).[114] Dementsprechend ist eine Einwilligung grundsätzlich auch für diesen Bereich möglich.

Die grundlegenden Anforderungen an die Einwilligung sind in Art. 4 Nr. 11 und Art. 7 DSGVO festgelegt. Gemäß Art. 4 Nr. 11 DSGVO ist eine Einwilligung

> *„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 versehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."*

Art. 7 DSGVO ergänzt die Anforderungen dahingehend, dass die Einwilligung jederzeit widerruflich (Abs. 3) und der Verantwortliche zum Nachweis der Einwilligungserklärung verpflichtet ist (Abs. 1). Im Bereich sensibler Daten ergeben sich aus Art. 9 Abs. 2 lit. a) DSGVO darüber hinaus noch weitergehende Anforderungen an eine Einwilligung. Auch nationale sozialdatenschutzrechtliche Regelungen enthalten zusätzliche Anforderungen an eine wirksame Einwilligung als Grundlage für die Datenverarbeitung. Im Einzelnen:

1.4.3.3.1 Freiwilligkeit

Bereits nach der Definition der Einwilligung nach Art. 4 Nr. 11 DSGVO ist die Freiwilligkeit der Einwilligung erforderlich. Besonderes Augenmerk ist bei der Einholung einer Einwilligung im Zusammenhang mit der Datenverarbeitung durch Sozialleistungsträger auf die Gestaltung der Einwilligungserklärungen zu legen. Auf Grund des Abhängigkeitsverhältnisses zwischen Betroffenem und Leistungsträger bewegt sich die Freiwilligkeit der Erklärung stets auf einem schmalen Grat. Dies macht insbesondere Erw.Gr. 43 der DSGVO deutlich. Danach

> *„sollte diese [die Einwilligung] in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere*

113 Siehe auch: Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 49f.

114 An dieser Stelle sei darauf hingewiesen, dass mit dem Entwurf zum 2. DSAnpUG-EU bei der Verarbeitung von biometrischen, genetischen oder Gesundheitsdaten formelle Wirksamkeitsvoraussetzungen für Einwilligungserklärungen geschaffen werden sollen, vgl. BT-Drs. 19/4674, S. 153. Hierzu bereits oben in Kap. 1.1.3.2.1.

wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

Dementsprechend ist die Einwilligung derart zu gestalten, dass dem Betroffenen die Wahlmöglichkeit klar vor Augen geführt und betont wird, dass die Nichterteilung keine nachteiligen Folgen für das Versicherungsverhältnis hat und haben wird. Dabei kann die Freiwilligkeit, sofern im Rahmen des konkreten Vorhabens möglich, über ein abgestuftes Einwilligungssystem besonders herausgestellt werden.

Insbesondere ist gemäß Art. 7 Abs. 4 DSGVO zu vermeiden, den Abschluss eines Vertrages an die Abgabe der Einwilligung zu koppeln.

1.4.3.3.2 Informiertheit/Hinweispflicht

Grundvoraussetzung der wirksamen Einwilligung ist die Informiertheit des Einwilligenden. Der Betroffene ist vorab über die wesentlichen Punkte der Datenverarbeitung, wie den Verantwortlichen den Empfänger, die Übermittlungswege und -zwecke sowie das Forschungsprojekt zu informieren.[115] Erw. Gr. 42 der DSGVO konkretisiert die Informationspflichten des Verantwortlichen dahingehend, dass der Betroffene über den Verantwortlichen und die Zwecke der Datenverarbeitung aufzuklären ist und dass er erkennen kann, dass und in welchem Umfang er seine Einwilligung erteilt. Gemäß § 67b Abs. 2 S. 2 SGB X muss die betreffende Person auf den Zweck der vorgesehenen Verarbeitung, auf die Folgen der Verweigerung der Einwilligung sowie auf die jederzeitige Widerrufsmöglichkeit im Rahmen der Einholung der Einwilligung hingewiesen werden. Der deutliche Hinweis auf diese Punkte ist dabei auch von erheblicher Bedeutung für die Freiwilligkeit der Erklärung, denn auf Grund des bestehenden Abhängigkeitsverhältnisses der Betroffenen von den Leistungsträgern kann die Freiwilligkeit der Einwilligung nur bejaht werden, wenn dem Betroffenen klar wird, dass die Erteilung einer Einwilligung für ihn nicht zwingend ist. Hierdurch wird insbesondere auch der Forderung im Erw.Gr. 32 der DSGVO entsprochen, wonach die Einwilligung freiwillig, für den konkreten Fall und in informierter Weise erfolgen soll. Damit die betreffende Person die Einwilligung in Kenntnis der Sachlage abgeben kann, muss sie wiederum wissen, für welche Zwecke ihre Daten verarbeitet werden sollen (vgl. Erw.Gr. 42 DSGVO).

115 Rombach, in: Hauck/Noftz, Stand: 08/2017, SGB X, § 75 Rn. 32.

Mangels einer konkretisierenden Regelung in der DSGVO, welche Informationen der Einwilligende genau erhalten soll, kann der nationale Gesetzgeber entsprechende Vorgaben machen.

1.4.3.3.3 Zweckbindung/Umfang

Bereits aus der Definition in Art. 4 Nr. 11 DSGVO ergibt sich, dass die Einwilligung nur für einen bestimmten Fall abgegeben werden kann. Art. 6 Abs. 1 S. 1 lit. a) DSGVO sowie Art. 9 Abs. 2 lit. a) DSGVO konkretisieren dieses Erfordernis dahingehend, dass sich die Einwilligung auf einen oder mehrere festgelegte Zwecke beziehen muss. Das Maß der Konkretisierung hängt dabei regelmäßig von der geplanten Verwendungssituation ab.[116] Dementsprechend ist das konkrete Vorhaben im Rahmen der Einwilligung zu benennen und soweit möglich zu beschreiben.

Bei der Verarbeitung von Daten zu Forschungszwecken gilt darüber hinaus § 67 Abs. 3 SGB X, wonach die Einwilligung für ein bestimmtes Vorhaben **oder für bestimmte Bereiche der wissenschaftlichen Forschung** erteilt werden kann (Broad Consent). Mit dieser erweiterten Einwilligung soll den Bedürfnissen der Wissenschaft Rechnung getragen werden, wenn etwa zum Zeitpunkt der Erhebung der Sozialdaten noch nicht das konkrete Forschungsvorhaben, jedoch bestimmte Forschungsbereiche angegeben werden können. Durch die Regelung sollte berücksichtigt werden, dass Forschungsfragen teilweise in einer offenen Vorgehensweise sukzessive entwickelt werden[117]. Dies greift den Gedanken des Erw.Gr. 33 DSGVO auf, der das Konzept einer solchen „weiten Einwilligung" für die DSGVO beinhaltet, ohne dass der deutsche Gesetzgeber aber gleichzeitig die Bezugnahme auf die zur Kompensation von Erw.Gr. 33 geforderte „Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung" ausdrücklich aufgreift.[118] Das führt nach hier vertretener Auffassung aber nicht zur Unvereinbarkeit mit der DSGVO, da die Erwägungsgründe zum einen kein verbindlicher Verordnungstext sind und überdies auch Erw.Gr. 33 nicht fordert, dass ein Mitgliedsstaat die Einhaltung ethischer Standards im jeweiligen Datenschutzrecht normiert. Verpflichtungen zur Einhaltung ergeben sich aus diversen Rechtsquellen außerhalb des nationalen Datenschutzrechts.[119]

Um dem Grundsatz der informierten Einwilligung Rechnung zu tragen, sollte der in der Einwilligung zu nennende Bereich der Forschung nicht zu allgemein gefasst sein und ist thematisch möglichst einzugrenzen. Die Teilnehmer wissenschaftlicher Studien sollten zudem über das Vorgehen informiert und darauf hingewiesen werden, dass sich die Forschungsfragen in einem

116 *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO, 2017, Art. 7 Rn. 65.
117 BT-Drs. 18/12611, S. 113.
118 Siehe zum Broad Consent auch: Kap. 3.2.
119 Siehe hierzu Kap. 3.2.6.

abgegrenzten thematischen Feld bewegen, jedoch schrittweise konkretisiert werden.[120]

1.4.3.3.4 Form und Nachweispflicht

Hinsichtlich der **Form** der Einwilligung bestehen weder nach den SGB X noch der DSGVO zwingende Vorschriften. § 67b Abs. 2 S. 1 SGB X regelt, dass die Einwilligung nach Möglichkeit schriftlich oder elektronisch eingeholt werden soll. Diese Soll-Vorschrift dient im Wesentlichen der Sicherstellung der Nachweispflicht (Art. 7 Abs. 1 DSGVO), steht aber einer anderweitigen Form – etwa der mündlich erteilten, protokollierten Einwilligung – im Falle besonderer Umstände nicht entgegen.[121] Dennoch ist es ratsam, die Einwilligungen zu den hier beabsichtigten Zwecken schriftlich oder hilfsweise elektronisch einzuholen. Mit der Möglichkeit einer elektronischen Erklärung soll berücksichtigt werden, dass in Zukunft immer mehr Verwaltungsverfahren elektronisch geführt werden. Zur Vermeidung von Medienbrüchen soll durch die ergänzende Möglichkeit der elektronischen Erklärung diesen Entwicklungen Rechnung getragen werden.[122] Nicht ausreichend ist dagegen Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person. Durch die vorgeschriebene Nachweispflicht wird die Beweislast für das Vorliegen einer wirksamen Einwilligung dem Leistungsträger auferlegt. Letztlich laufen diese Vorgaben auf eine **Dokumentationspflicht** für den gesamten Verarbeitungsvorgang und die Einholung der jeweiligen Einwilligung hinaus.[123]

Sind von der Datenverarbeitung besondere Kategorien personenbezogener Daten umfasst, regelt Art. 9 Abs. 2 lit. a) DSGVO zudem, dass die Einwilligung ausdrücklich erfolgen muss. Eine mutmaßliche Einwilligung kommt ebenso wie eine konkludent durch schlüssiges Verhalten geäußerte nicht in Betracht.[124] Die Ausdrücklichkeit der Einwilligung gemäß Art. 9 Abs. 2 lit. a) DSGVO soll den Betroffenen auf die besondere Sensibilität der Daten aufmerksam machen. Konkret wird gefordert, dass der betroffenen Person unter konkreter Nennung der Datenkategorie verdeutlicht werden muss, dass die entsprechenden Daten von der Einwilligung erfasst sind.[125] Auch unter diesem Gesichtspunkt ist eine schriftliche oder elektronische Einwilligung folglich empfehlenswert.

Es sei an dieser Stelle auf den eingangs erwähnten Gesetzentwurf zum 2. DSAnpUG-EU hingewiesen, wonach strengere Wirksamkeitsvoraussetzungen an die datenschutzrechtliche Einwilligungserklärung bei der Verarbeitung

120 BT-Drs. 18/12611, S. 113.
121 BT-Drs. 18/12611, S. 113.
122 BT-Drs. 18/12611, S. 112f.
123 Vgl. Plath, in: Plath, BDSG/DSGVO, 2. Aufl., 2016, Art. 7 Rn. 3.
124 Frenzel, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 9 Rn. 21; Schiff, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 9 Rn. 28.
125 Plath, in: Plath, BDSG/DSGVO, 2. Aufl., 2016, Art. 9, Rn. 13.

von genetischen, biometrischen und Gesundheitsdaten in einem neuen § 67b Abs. 2 S. 2, Abs. 3 SGB X geplant sind.[126]

1.4.3.3.5 Hervorhebungsgebot

In Art. 7 Abs. 2 DSGVO werden für den Fall, dass die Einwilligung schriftlich erfolgt und noch andere Sachverhalte betrifft, weitere Voraussetzungen vorgegeben. Diese muss dann in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Es gilt somit das sog. Trennungs- und Transparenzprinzip, insbesondere auch zur Verhinderung „versteckter" Einwilligungserklärungen in den Allgemeinen Geschäftsbedingungen.

1.4.3.3.6 Widerrufsmöglichkeit

Gemäß Art. 7 Abs. 3 DSGVO hat die betroffene Person jederzeit das Recht, ihre Einwilligung zu widerrufen. Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein. Hierdurch kann der Betroffene seine Einwilligung ex nunc beseitigen und zukünftige Datenverarbeitung auf Grundlage seiner Einwilligung verhindern.[127]

1.4.3.3.7 Zwischenergebnis

Unter Beachtung der aufgezeigten Anforderungen kommt die Auswertung der Sozialdaten jeweils zu Forschungs-, Planungs- sowie Qualitätssicherungszwecken in Betracht.

Im Bereich der Datenauswertung zu Forschungszwecken gilt insofern eine Erleichterung hinsichtlich der Zweckbindung, als die Nennung bestimmter Bereiche der Forschung zulässig ist, soweit eine weitere Konkretisierung zum Zeitpunkt der Einwilligung noch nicht möglich ist.

1.4.4 Angemessene, spezifische Maßnahmen (§ 22 Abs. 2 BDSG)

Bei der Auswertung der Sozialdaten durch den Leistungsträger handelt es sich auch um die Veränderung oder Nutzung der Sozialdaten im Sinne des § 67b SGB X. Gemäß § 67b Abs. 1 S. 4 SGB X gilt § 22 Abs. 2 BDSG entsprechend und ist auch vorliegend anzuwenden.[128] § 22 Abs. 2 BDSG lautet wie folgt:

> *„In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des*

126 Hierzu bereits eingangs in Kap. 1.1.3.2.1.

127 Vgl. Plath, in: Plath, BDSG/DSGVO, 2. Aufl., 2016, Art. 7, Rn. 10, für den Bereich der Forschung Schaar, ZD 2017, 213 (214, 216).

128 Vgl. BT-Drs. 18/12611, S. 114.

Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. *technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der [DSGVO] erfolgt,*
2. *Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben verändert oder entfernt worden sind,*
3. *Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,*
4. *Benennung einer oder eines Datenschutzbeauftragten,*
5. *Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,*
6. *Pseudonymisierung personenbezogener Daten,*
7. *Verschlüsselung personenbezogener Daten,*
8. *Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,*
9. *zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zu regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder*
10. *spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetztes sowie der [DSGVO] sicherstellen."*

Durch diese Regelung wurde das Erfordernis aus Art. 9 Abs. 2 lit. b), g), i) und j) der DSGVO umgesetzt, geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person bzw. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen.[129]

Die Anforderungen sind in § 22 Abs. 2 BDSG bereits detailliert wiedergegeben. Wie diese in der Praxis im Einzelnen umzusetzen sind, muss im Einzelfall geprüft werden und kann nur anhand eines konkreten Datenschutz-Konzeptes beurteilt werden.

129 BT-Drs. 18/11325, S. 95.

1.4.5 Genehmigungserfordernis und -anforderungen

1.4.5.1 Forschungszwecke

Ein Genehmigungserfordernis besteht bei Auswertung der Daten zu Forschungszwecken ohne Einwilligung der Betroffenen auf Grundlage des § 287 SGB V. Hier muss die Aufsichtsbehörde dem Leistungsträger eine Erlaubnis erteilen. Das Erlaubnisverfahren ist im Gesetz nicht geregelt. Nach dem Gesetzeszweck ist die Erlaubnis vor Beginn der Forschungsvorhaben erforderlich. Hierdurch soll die Einhaltung der Datenschutzvorschriften gewährleistet werden, sodass die Aufsichtsbehörde über die Einzelheiten des geplanten Forschungsvorhabens (vorher) zu unterrichten ist.[130]

1.4.5.2 Planungsvorhaben

Bei der Auswertung der Daten zu Planungszwecken ohne Einwilligung der Betroffenen auf Grundlage des § 67 Abs. 2 Nr. 2 SGB X ist mangels Verweis auf § 75 Abs. 4 SGB X kein Genehmigungsverfahren erforderlich. Dennoch ist aufgrund des Verweises auf § 75 Abs. 1 SGB X der zuständigen Aufsichtsbehörde ein Datenschutzkonzept vorzulegen, vgl. § 75 Abs. 1 S. 4 SGB X. In dem Datenschutzkonzept ist insbesondere darzulegen, dass die technischen und organisatorischen Anforderungen sowie der Grundsatz der Datenminimierung erfüllt sind.[131] Diese kann bei einer Prüfung sodann im Rahmen ihrer aufsichtsrechtlichen Möglichkeiten auf den Leistungsträger einwirken.

1.4.6 Ergebnis

Zu Szenario 1 lassen sich damit folgende Ergebnisse zusammenfassen:

Eine Verarbeitung von Sozialdaten zu Forschungszwecken ist in den Grenzen des § 287 SGB V zulässig. Die Forschungsvorhaben sind dabei nicht auf medizinische Fragestellungen begrenzt. Die Beteiligung einer externen Stelle, die sich darauf beschränkt die Forschungsfrage sowie die Planung des Forschungsvorhabens mitzugestalten, ist unproblematisch. Ebenfalls denkbar wäre eine Einbeziehung einer externen Stelle im Rahmen einer Auftragsverarbeitung. Auswertungen dürfen jedoch nicht von einem Dritten vorgenommen werden. Die Anforderung des § 287 Abs. 2 SGB V, wonach eine Anonymisierung der Daten erforderlich ist, kann nur sinnvoll in der Praxis umgesetzt werden, wenn ein modifiziertes Verständnis des Begriffs der Anonymisierung zugrunde gelegt wird. Hierbei könnte man sich an den Kategorien der sogenannten „formalen Anonymisierung", wie sie in § 16 Abs. 2 S. 1 Bundesstatistikgesetz verwendet wird, orientieren. Eine Unvereinbarkeit des § 287 SGB V mit der DSGVO liegt unseres Erachtens nicht

130 *Didong*, in: jurisPK-SGB V, 3. Aufl., 2016, § 287 Rn. 11 m.w.N.
131 BT-Drs. 18/12611, S. 118.

vor. Ein Rückgriff auf den allgemeineren Tatbestand des § 76c SGB X ist nach vorherrschender Meinung ausgeschlossen. Dem Gesetzgeber stünde es offen, diesen Rückgriff auch unter Beachtung der DSGVO zu ermöglichen.

Eine Nutzung von Sozialdaten durch eine Krankenkasse zu Planungszwecken ist auf Grundlage des gesetzlichen Tatbestandes des § 67c Abs. 2 Nr. 2 SGB X zulässig. Ob eine Anwendung von § 75 Abs. 2 und Absatz 4 S. 1 SGB X in Betracht kommt, ist allerdings fraglich. Die besseren Argumente sprechen dafür, dass die sich aus dem Wortlaut ergebende Begrenzung auf Forschungsvorhaben eine Anwendung für Planungsvorhaben nicht zulässt.

Hinsichtlich einer Nutzung zu Qualitätssicherungszwecken ist eine Auswertung durch die Krankenkasse nach den Vorgaben des § 299 SGB V nicht zulässig.

Alternativ zu einer gesetzlichen Ermächtigungsnorm kann sowohl ein Forschungsvorhaben, ein Planungsvorhaben als auch ein Qualitätssicherungsvorhaben auf eine Einwilligung gestützt werden. Da der Gesetzgeber von seiner Regelungskompetenz zum vollständigen Ausschluss der Einwilligung im Bereich der Verarbeitung von besonderen Kategorien personenbezogener Daten keinen Gebrauch gemacht hat, ist eine Einwilligung unter Rückgriff auf die DSGVO stets zulässig. Im Rahmen einer denkbaren Anpassung des SGB V an die DSGVO könnte der deutsche Gesetzgeber jedoch die Möglichkeit der Einholung einer Einwilligungserklärung für besondere Kategorien personenbezogener Daten ausschließen oder nur unter erhöhten Anforderungen zulassen.

Bei allen Verarbeitungen sind angemessene, spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen, wie sie sich aus der DSGVO bzw. dem nationalen Datenschutzrecht ergeben. Ein Genehmigungserfordernis besteht ausschließlich bei einer Verarbeitung von Sozialdaten zu Forschungszwecken.

1.5 Beurteilung von Szenario 2

1.5.1 Darstellung des Szenarios

Ein Leistungsträger der gesetzlichen Krankenversicherung und eine externe Einrichtung kooperieren. Die Sozialdaten werden für ein bestimmtes Vorhaben an die externe Einrichtung übermittelt, die diese im Sinne des Vorhabens verarbeitet und auswertet.

1.5.2 Rechtfertigungsbedürftige Datenverarbeitungsvorgänge

Bereits vorab wurde klargestellt, dass die Verarbeitung anonymisierter Daten aus datenschutzrechtlicher Sicht nicht relevant ist, sodass auch eine Weitergabe anonymisierter Sozialdaten für ein bestimmtes Vorhaben an eine externe Einrichtung sowie die Verarbeitung und Auswertung durch diese zulässig ist.

Für pseudonymisierte Sozialdaten gilt Gleiches, wenn nach dem maßgeblichen Verständnis eines relativen Personenbezugs die pseudonymisierten Daten aus Sicht des Empfängers faktisch anonym sind. Dies wäre dann nicht anzunehmen, wenn ein rechtlich zulässiges Mittel bestünde, das eine De-Pseudonymisierung und damit eine Re-Identifikation durch die externe Einrichtung ermöglichte. Ein solches Mittel ist im Forschungs- oder Planungskontext nicht ersichtlich.

Vorliegend kommen daher folgende rechtfertigungsbedürftige Verarbeitungsvorgänge in Betracht: Abhängig von der rechtlichen Ausgestaltung ist zunächst eine Übermittlung (s. Kap. 1.4.3.2) an die externe Stelle zu untersuchen, die diese Daten dann im Sinne einer Auswertung nutzen würde (s. Kap. 1.5.4).

Soll die externe Stelle hingegen als Auftragsverarbeiter tätig werden, stellen sich die Weitergabe der Daten an den Auftragsverarbeiter und die Auswertung durch diesen für den Auftraggeber jeweils als Nutzung durch den verantwortlichen Auftraggeber dar (s. Kap. 1.5.4.4).

1.5.3 Zulässigkeit der Weitergabe von Sozialdaten durch den Leistungsträger (hinsichtlich der jeweiligen Zwecke) an eine externe Einrichtung

Sollen personenbezogene Abrechnungsdaten von Versicherten zum Zweck der Verarbeitung für ein bestimmtes Projekt im Bereich der wissenschaftlichen Forschung, Planung im Sozialleistungsbereich oder der Qualitätssicherung an eine externe Einrichtung übertragen werden, bedarf es entsprechend dem generellen Verbot mit Zulässigkeitsvorbehalt einer Ermächtigungsgrundlage. Neben den gesetzlichen Erlaubnistatbeständen (s. Kap. 1.5.3.2) kommt dabei auch die Einwilligung des Betroffenen (s. Kap. 1.5.3.3) in Betracht. Verzichtbar kann eine solche Ermächtigungsgrundlage gegebenenfalls sein, wenn die Daten nicht an einen eigenständigen Dritten, sondern einen weisungsgebundenen Auftragsverarbeiter weitergegeben werden (s. Kap. 1.5.3.4).

1.5.3.1 Prüfungsmaßstab/Identifikation des einschlägigen Datenschutzregimes

Hinsichtlich der Verarbeitungen durch die Krankenkasse bleibt es bei den in Kapitel 1.4.3.1 beschriebenen Rahmenbedingungen.

1.5.3.2 Gesetzliche Ermächtigung

Aufgrund des Vorrangs der bereichsspezifischen Datenschutzregelungen des Sozialgesetzbuchs[132] bedarf es einer entsprechenden Ermächtigungsgrundlage im SGB. § 67b Abs. 1 SGB X bestimmt, dass die Übermittlung von Sozialdaten, inklusive der besonderen Kategorien personenbezogener Daten, durch die Leistungsträger zulässig ist, sofern die Folgevorschriften des SGB X oder eine

132 Vgl. dazu oben Kap. 1.4.3.1.

andere Rechtsvorschrift des Sozialgesetzbuchs dies erlaubt oder anordnet. Dabei ist zunächst auf die bereichsspezifischen Vorschriften des SGB V abzustellen, bevor eine Ermächtigungsgrundlage des allgemeinen Sozialrechts nach dem SGB X herangezogen wird.

Die §§ 284ff. SGB V regeln bereichsspezifisch die zulässige Verarbeitung von Sozialdaten insbesondere auch durch die Krankenkassen. Dabei gibt § 284 Abs. 1 S. 1 SGB V abschließend vor, zu welchen Zwecken die Krankenkassen Sozialdaten erheben und speichern dürfen. Für die Verarbeitung (und Nutzung) dieser Daten regelt § 284 Abs. 3 S. 1 Hs. 1 SGB V, dass die so erhobenen Sozialdaten grundsätzlich nur für die in Absatz 1 genannten Zwecke verarbeitet werden dürfen. Eine Verarbeitung (und Nutzung) dieser Daten für andere Zwecke, ist gemäß § 284 Abs. 3 S. 1 Hs. 2 SGB V – in Übereinstimmung mit § 67b Abs. 1 SGB X – nur zulässig, sofern eine andere Rechtsvorschrift des Sozialgesetzbuchs dies anordnet oder erlaubt. Folglich bedarf die Übermittlung von Daten durch die Leistungserbringer zu Zwecken der wissenschaftlichen Forschung, Planung im Sozialleistungsbereich oder der Qualitätssicherung einer gesonderten Ermächtigungsgrundlage im Sozialgesetzbuch. Wie bereits unter Teil 2 A.III.1.b) (s. Kap. 1.4.3.1.2) dargelegt, geht dabei keine Sperrwirkung von den bereichsspezifischen Erlaubnistatbeständen des SGB V gegenüber dem SGB X aus. Vielmehr enthält das SGB V lediglich spezifischere Vorschriften, die im Einzelfall vorrangig anzuwenden sind, die jedoch darüber hinaus einen Rückgriff auf die allgemeinen Vorschriften nicht gänzlich verwehren.

1.5.3.2.1 Nutzung zu Forschungszwecken (§ 287 SGB V)

In Betracht käme zunächst die bereichsspezifische Regelung des § 287 SGB V. Nach dieser dürfen Krankenkassen mit Erlaubnis der Aufsichtsbehörde die Datenbestände leistungserbringer- oder fallbeziehbar für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben auswerten und aufbewahren. § 287 SGB V ist jedoch ausschließlich auf die krankenkasseninterne Auswertung von leistungserbringer- oder fallbeziehbaren Daten zugeschnitten.[133] Die Ermächtigung umfasst weder die interne Verarbeitung von versichertenbeziehbaren Daten[134] noch die Übermittlung der Daten an externe Stellen zur Verarbeitung der Daten zu den beabsichtigten Zwecken. § 287 SGB V stellt folglich keine geeignete Ermächtigungsgrundlage dar.

1.5.3.2.2 Nutzung zur Qualitätssicherung (§ 299 SGB V)

Gemäß § 299 Abs. 1a SGB V sind Krankenkassen befugt und verpflichtet, die im Rahmen ihrer Aufgabenerfüllung nach § 284 Abs. 1 SGB V erhobenen Sozialdaten für Zwecke der Qualitätssicherung zu verarbeiten und zu nutzen.

133 Vgl. Ausführungen zu Szenario 1 Kap. 1.4.3.2.1, Abschnitt „Interne Fragestellungen“ und Kap. 1.4.3.2.2.
134 Vgl. Didong, in: Schlegel/Voelzke, jurisPK-SGB V, 3. Aufl., 2016, § 287 Rn. 8.

Der Gemeinsame Bundesausschuss nach § 91 SGB V (G-BA) regelt in Beschlüssen und Richtlinien, welche konkreten Daten für die Verarbeitung und Nutzung zugelassen sind und legt die Empfänger fest. Die von der Krankenkasse zu übermittelnden Sozialdaten sind in Anlage II Teil b) der Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung (Quesü-RL)[135] festgeschrieben. Dazu gehören beispielsweise die Stammdaten der Versicherten. Gemäß § 9 Abs. 1 Satz 9, Teil 1 Quesü-RL haben die Krankenkassen die Daten an die vom G-BA nach § 4 Abs. 5 Satz 1, Teil 1 Quesü-RL beauftragte Datenannahmestelle (DAS-KK) zu übermitteln. Eine darüber hinaus gehende Übermittlung anderer Daten an andere Stellen ist nicht über § 299 SGB V zu legitimieren. Vielmehr bedarf es in diesen Fällen einer gesonderten Rechtsgrundlage.

Erfolgt eine Übermittlung von Sozialdaten i.R.v. § 299 Abs. 1a SGB V, sind die versichertenbezogenen Daten grundsätzlich zu pseudonymisieren (§ 299 Abs. 1a S. 3 i.V.m. Abs. 1 S. 4 Nr. 1 SGB V). Dies erfolgt entweder bei den Leistungserbringern selbst (§ 299 Abs. 2 S. 3 SGB V), bei einer vom G-BA beauftragten eigenständigen Stelle (§ 299 Abs. 2 S. 3 SGB V) oder nach einer Vollerhebung über die ebenfalls vom G-BA beauftragte Vertrauensstelle (§ 11 Teil 1 Quesü-RL). Nur in den Richtlinien und Beschlüssen des G-BA geregelten Ausnahmefällen ist eine Pseudonymisierung entbehrlich. Darüber hinaus sieht das Gesetz grundsätzlich nur eine stichprobenweise Datenerhebung vor, sodass eine Vollerhebung ebenfalls nur im Rahmen der in den Richtlinien und Beschlüssen des G-BA geregelten Ausnahmefällen möglich ist (§ 299 Abs. 1a S. 3 i.V.m. Abs. 1 S. 4 Nr. 1 SGB V).

1.5.3.2.3 Nutzung im Rahmen der Datentransparenz (§ 303a ff. SGB V)

Die §§ 303a ff. SGB V schaffen eine Ermächtigungsgrundlage zur Übermittlung der im Rahmen des Risikostrukturausgleichs vom Bundesversicherungsamt erhobenen Daten in pseudonymisierter Form an das DIMDI in seiner Funktion als Datenaufbereitungs- und Vertrauensstelle. Mit Ausnahme des § 303b Abs. 2 SGB V, der die Ermächtigungsgrundlage für die Übermittlung verschlüsselter Regionalkennzeichen durch die Krankenkassen an das Bundesversicherungsamt enthält, schaffen die §§ 303a ff. SGB V ausschließlich eine Rechtsgrundlage für die Übermittlung von Daten des Risikostrukturausgleichs durch das Bundesversicherungsamt, nicht jedoch für Übermittlung von Abrechnungsdaten durch die Krankenkassen. Folglich bilden auch die §§ 303a ff. SGB V keine geeignete Ermächtigungsgrundlage.

1.5.3.2.4 Übermittlung zu Zwecken der Forschung und Planung (§ 75 SGB X)

Gemäß § 75 Abs. 1 SGB X ist die Übermittlung von Sozialdaten zulässig, sofern sie für ein **bestimmtes Vorhaben** der wissenschaftlichen Forschung im

135 In der Fassung vom 20.04.2017.

Sozialleistungsbereich, der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben **erforderlich** ist, **schutzwürdige Interessen** des Betroffenen nicht beeinträchtigt oder vom öffentlichen Interesse an der Forschung/Planung erheblich überwogen werden und die zuständige oberste Bundes- oder Landesbehörde die Übermittlung zuvor genehmigt hat (§ 75 Abs. 4 SGB X).

Die bisher vergleichsweise streng gefassten Anforderungen an ein im Vorhinein bestimmtes Forschungsvorhaben hat der Gesetzgeber unter Berücksichtigung der „Bedeutung der Forschung für die gesamtgesellschaftliche Entwicklung“[136] teilweise gelockert. Mit den neuen Regelungen verfolgt der Gesetzgeber das Ziel, sozialdatenbasierter Forschung weitere rechtliche Möglichkeiten zu eröffnen, die die Effektivität und Langfristigkeit der Forschungsergebnisse fördern, wobei ein „angemessener Ausgleich zwischen den Erfordernissen der Forschung auf der einen Seite und dem berechtigten Interesse der einzelnen betroffenen Personen an dem Schutz ihrer persönlichen Daten auf der anderen Seite“ hergestellt werden soll.[137]

Der hierzu eingefügte § 75 Abs. 4a SGB X lautet:

> *„Ergänzend zur Übermittlung von Sozialdaten zu einem bestimmten Forschungsvorhaben nach Absatz 1 Satz 1 kann die Verwendung 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.“*

Somit soll der große Aufwand der Beantragung von Folgeforschungsvorhaben reduziert werden, wobei die in Erwägungsgrund 33 der DSGVO „getroffene Wertung, dass oftmals der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung

136 BR-Drs. 430/18, S. 180.
137 BR-Drs. 430/18, S. 180.

der personenbezogenen Daten nicht vollständig angegeben werden kann", umgesetzt werden soll.[138] Die Privilegierung ist dabei auf inhaltlich zusammenhängende Forschungsvorhaben des gleichen Forschungsbereichs begrenzt, wobei „einzelne Elemente der Forschungsfrage unterschiedlich" sein können.[139] Gleichzeitig soll durch eine hinreichende Bestimmtheit, und weitere Kontrollrechte eine Absenkung des Schutzniveaus verhindert werden.[140] Zur weiteren Vereinfachung enthält Satz 5 eine Genehmigungsfiktion, sofern nicht vor Ablauf einer Frist von acht Wochen nach Eingang der vollständigen Unterlagen die Genehmigungsbehörde ein gesondertes Genehmigungsverfahren für erforderlich erklärt. Insbesondere letztere Regelung kann zu besserer Planungssicherheit und einer Beschleunigung der Verfahren führen. Gleichzeitig besteht hierbei das Risiko, dass ohne entsprechende Prüfung Sozialdaten verarbeitet werden und somit das Ziel der Verhinderung der Absenkung des Schutzniveaus konterkariert werden könnte. Der zurückhaltend formulierte Wortlaut spricht jedoch lediglich davon, dass mit dem Forschungsvorhaben „bereits begonnen" werden darf. Ein nachträgliches behördliches Einschreiten bliebe möglich; vor dem Hintergrund der achtwöchigen Frist erscheint dieses Risiko jedoch angemessen.

Im Einzelnen stellt sich die Anwendung des § 75 SGB X wie folgt dar:

Bestimmtes Vorhaben

§ 75 Abs. 1 S. 1 SGB X kann eine Datenübermittlung grundsätzlich nur legitimieren, wenn diese **für ein bestimmtes Vorhaben** erfolgt. Die Beschränkung auf ein bestimmtes Vorhaben schließt die Übermittlung für generelle, nicht näher bestimmte Forschungs- und Planungszwecke zunächst aus.[141] Darüber hinaus erweitern § 75 Abs. 2 und 4a SGB X[142] die zulässige Übermittlung im Einzelfall. Sofern eine entsprechende Genehmigung vorliegt, können zum einen weitere Sozialdaten für die Bearbeitung von mit dem Ausgangsvorhaben inhaltlich zusammenhängenden Forschungsfolgefragen bzw. die ursprünglich übermittelten Sozialdaten auch für inhaltlich mit dem Ausgangsvorhaben in Zusammenhang stehende Forschungsvorhaben des gleichen Forschungsbereichs übermittelt werden.

138 BT-Drs. 18/12611, S. 110.
139 BT-Drs. 18/12611, S. 110.
140 BT-Drs. 18/12611, S. 111.
141 Zur wortgleichen Fassung des § 75 Abs. 1 S. 1 SGB X a.F. Diering/Seidel, in: Diering/Timme, SGB X, 4. Aufl. 2016, § 75 Rn. 4; BT-Drs. 12/5187, S. 40.
142 § 75 Abs. 2 SGB X lautet: *„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."*

Vorhaben im Bereich der wissenschaftlichen Forschung im Sozialleistungsbereich, der wissenschaftlichen Arbeitsmarkt- und Berufsforschung oder der Planung im Sozialleistungsbereich

§ 75 Abs. 1 S. 1 SGB X kann zudem nur als Ermächtigungsgrundlage herangezogen werden, wenn das Vorhaben im Bereich der wissenschaftlichen Forschung im Sozialleistungsbereich, der wissenschaftlichen Arbeitsmarkt-, sowie Berufsforschung (Nr. 1) oder der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben (Nr. 2) angesiedelt ist.

Bereich der wissenschaftlichen Forschung im Sozialleistungsbereich

Für die Subsumtion eines Vorhabens unter den Bereich der **wissenschaftlichen Forschung im Sozialleistungsbereich** ist es nicht erforderlich, dass sich das Forschungsvorhaben auf das Gebiet des Leistungsrechts beschränkt oder konzentriert.[143] Vielmehr können auch Forschungsvorhaben mit volkswirtschaftlichem, soziologischem oder medizinischem Schwerpunkt darunter fallen, sofern etwaige Erkenntnisse mit gewisser Wahrscheinlichkeit auch im Sozialleistungsbereich von Bedeutung sein können.[144] Demzufolge kann über § 75 Abs. 1 SGB X die Übermittlung von personenbezogenen Sozialdaten für eine Vielzahl von (bestimmten) Forschungsvorhaben legitimiert werden, sofern die zu erwartenden Erkenntnisse für den Sozialleistungsbereich von Bedeutung sein können. Dieser zu erwartende Nutzen muss im Genehmigungsantrag (§ 75 Abs. 4 SGB X) im Einzelfall konkret dargelegt werden. Je weiter der eigentliche Forschungszweck dabei vom Sozialleistungsbereich entfernt ist, desto umfassender sind die Anforderungen an die Darlegung dieses Nutzens für den Sozialleistungsbereich.[145]

§ 75 Abs. 1 Nr. 2 SGB X

Des Weiteren können Sozialdaten gemäß § 75 Abs. 1 Nr. 2 SGB X auch zum Zweck der **Planung im Sozialleistungsbereich** übermittelt werden. Der Begriff der Planung im Sozialleistungsbereich umfasst dabei im Wesentlichen die Bedarfs-, Bereitstellungs- und Finanzplanung.[146]

Empfangende Stelle

Für die in § 75 Abs. 1 S. 1 Nr. 1 SGB X genannten Zwecke der wissenschaftlichen Forschung im Sozialleistungsbereich kann die Übermittlung sowohl an eine

143 Krause, in: Schlegel/Voelzke, jurisPK-SGB X, 3. Aufl., 2013, § 75 Rn. 28.
144 Rombach, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 14; Krause, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 75 Rn. 28.
145 Rombach, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 14
146 Krause, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 75 Rn. 28; vgl. dazu weitergehend Kap. 1.4.3.2.3.

öffentliche als auch an eine nicht-öffentliche Stelle erfolgen. Wesentliches Kriterium soll in diesem Zusammenhang allein die Seriosität der empfangenden Stelle und deren Unabhängigkeit, sprich Freiheit von rein kommerziellen Forschungsinteressen, sein.[147] Die empfangende Stelle muss bei der Verarbeitung besonderer Kategorien personenbezogenen Daten – Gesundheitsdaten – angemessene Sicherungsmaßnahmen nach § 22 Abs. 2 BDSG vorsehen. Ist der Empfänger der Daten eine nicht-öffentliche Stelle muss sich diese zudem gemäß § 75 Abs. 4 S. 3 SGB X gegenüber der Genehmigungsbehörde vorab verpflichten, die Daten ausschließlich im Rahmen der vorgesehenen Zwecke zu verarbeiten. Zudem kann die genehmigende Behörde einer nicht-öffentlichen Stelle Auflagen erteilen, um die Einhaltung der gesetzlichen Vorgaben des § 75 SGB X sicherzustellen (§ 75 Abs. 5 SGB X). Aufsichtsbehörde für nicht-öffentliche Stellen ist gemäß § 75 Abs. 6 SGB X i.V.m. § 40 Abs. 1 BDSG die nach dem jeweiligen Landesrecht, der die nicht-öffentliche Stelle unterfällt, zuständige Behörde. Das sind regelmäßig die Landesbeauftragten für den Datenschutz.

Werden die Daten gemäß § 75 Abs. 1 S. 1 Nr. 2 SGB X zu Zwecken der Planung im Sozialleistungsbereich übermittelt, ist der Kreis der Empfänger auf öffentliche Stellen beschränkt, für die die Planung im entsprechenden Bereich im Rahmen ihrer Aufgaben liegt. Eine Übermittlung der Daten an eine nicht-öffentliche Stelle ist hier nicht zulässig.

Zu übermittelnde Daten

Gemäß des allgemeinen Erforderlichkeits- und Datenminimierungsprinzips (Art. 5 Abs. 1 lit. c] DSGVO) schreibt auch § 75 Abs. 1 S. 1 SGB X vor, dass eine Übermittlung von Sozialdaten nur zulässig ist, soweit sie für das jeweilige Vorhaben erforderlich ist. Demnach wird die Übermittlung auf die für das konkrete Forschungs- oder Planungsvorhaben erforderlichen Daten begrenzt. Gleiches gilt auch, sofern die Übermittlung weiterer Sozialdaten nach § 75 Abs. 2 SGB X genehmigt wurde.

§ 67d Abs. 2 SGB X erweitert die Übermittlungsbefugnis auf für das konkrete Vorhaben nicht erforderliche Daten, wenn diese mit den Sozialdaten, für die eine Übermittlungsbefugnis besteht, derart verbunden sind, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand verbunden ist und schutzwürdige Interessen des Betroffenen oder eines Dritten nicht überwiegen. Ein unvertretbarer Aufwand ist dabei nur zu bejahen, wenn die Daten derart physisch miteinander verbunden sind, dass die Trennung einen erheblichen Zeit-, Personal- und/oder Kostenaufwand bedeuten würde.[148] Dies ist nicht der Fall, wenn die Daten noch getrennt vorliegen oder mit technischen Hilfsmitteln

147 Rombach, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 16.
148 *Diering/Seidel*, in: Diering/Timme, SGB X, 4. Aufl., 2106, § 67d Rn. 4.

ohne größere Mühe herauskopiert werden können.[149] Hinsichtlich der Abwägung der mit den ggf. bestehenden schutzwürdigen Interessen der Betroffenen, bedarf es einer Einzelfallbetrachtung, bei der die Art der Daten und die Folgen für den Betroffenen von erheblicher Bedeutung sind. Gemäß § 67d Abs. 2 Hs. 2 SGB X dürfen die überschießenden Daten ausschließlich mit übermittelt, darüber hinaus aber nicht verändert oder genutzt werden. § 67d Abs. 2 Hs. 2 SGB X statuiert insoweit ein absolutes Verwertungsverbot für die überschießenden Daten[150].

Keine Beeinträchtigung schutzwürdiger Interessen des Betroffenen oder überwiegendes öffentliches Interesse

Die Übermittlung darf schutzwürdige Interessen der betroffenen Person nicht beeinträchtigen (§ 75 Abs. 1 S. 1 SGB X). Die Bestimmung schutzwürdiger Interessen erfolgt unter Berücksichtigung objektiver und subjektiver Gesichtspunkte mit Blick auf den Grad der Sensibilität der Daten und die möglichen Folgen einer Übermittlung.[151] Beachtlich sind in diesem Zusammenhang nicht nur die Interessen des Einzelnen, sondern auch aller Betroffenen zusammen.[152] Da vorliegend regelmäßig besondere Kategorien personenbezogener Daten betroffen sind, sind aufgrund der besonderen Schutzwürdigkeit der Daten jedoch keine allzu hohen Anforderungen an ein schutzwürdiges Interesse zu stellen. Liegt ein schutzwürdiges Interesse vor, ist eine Beeinträchtigung der Schutzwürdigkeit gegeben, sofern die Übermittlung aus objektiver Sicht zu Nachteilen für den Betroffenen führen kann oder der Betroffene der Übermittlung bereits widersprochen hat.[153] Eine pauschale Aussage, wann eine Beeinträchtigung eines schutzwürdigen Interesses gegeben ist, ist folglich nicht möglich. Vielmehr bedarf es einer genauen Betrachtung des Einzelfalls.

Werden die schutzwürdigen Belange des Einzelnen beeinträchtigt, kann eine Übermittlung dennoch stattfinden, sofern das öffentliche Interesse an der Übermittlung und dem dahinterstehenden Vorhaben die Interessen des Betroffenen erheblich überwiegt. Dabei sind aufseiten des öffentlichen Interesses der Nutzen und die Bedeutung des Vorhabens maßgeblich zu berücksichtigen. Ein überwiegendes Interesse liegt etwa vor, wenn das Vorhaben für die weitere Aufgabenerfüllung der übermittelnden Stelle erforderlich ist und das Vorhaben ohne die Übermittlung unmöglich würde.[154] Denkbar ist die Annahme eines überwiegenden öffentlichen Interesses jedoch auch, wenn über die Ergebnisse ein erheblicher Nutzen für die Allgemeinheit zu erwarten ist.

149 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 67d Rn. 107.
150 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 67d Rn. 110.
151 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 27f.
152 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 25.
153 *Krause*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 75 Rn. 44.
154 *Krause*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 75 Rn. 47.

Anonymisierung

§ 75 Abs. 1 S. 1 SGB X legitimiert eine Übermittlung personenbezogener Sozialdaten nur, sofern dies für den jeweiligen Zweck erforderlich ist. Über die ausdrückliche Erwähnung des Erforderlichkeitsgebots hebt diese Vorschrift den Vorrang der Übermittlung anonymisierter Daten hervor.[155] Als für den Betroffenen mildere Form der Verarbeitung hat die Anonymisierung der Sozialdaten auch für den Bereich der Forschungs- und Planungszwecke Priorität.[156] Eine Verarbeitung personenbezogener Sozialdaten kann nur erforderlich sein, wenn eine Anonymisierung nicht in Betracht kommt. Für besondere Kategorien personenbezogener Daten, wie die im Rahmen der Abrechnungsdaten regelmäßig betroffenen Gesundheitsdaten, regelt § 75 Abs. 3 S. 2 SGB X darüber hinaus, dass die Daten im Rahmen der Verarbeitung durch den Empfänger zu anonymisieren sind, sobald dies nach dem Forschungszweck möglich ist. Dies entspricht der Forderung des Art. 89 Abs. 1 Satz 4 DSGVO. Darüber hinaus statuiert § 284 Abs. 3 S. 2 SGB V eine Pflicht zur Löschung des Versichertenbezugs, wenn es sich bei den zu übermittelnden Daten um Daten handelt, die gemäß § 295 Abs. 1b S. 1 SGB V von den Leistungserbringern an die Krankenkassen übermittelt wurden.[157]

Einwilligung

§ 75 Abs. 1 S. 2 SGB X regelt die Priorität der Einwilligung, wonach auch im Bereich der in § 75 Abs. 1 S. 1 SGB X genannten Vorhaben eine Übermittlung grundsätzlich nur mit der vorherigen Einwilligung des Betroffenen zulässig ist, es sei denn, dies ist dem Verantwortlichen unzumutbar oder es handelt sich ausschließlich um explizit genannte Daten, die ausschließlich zu Befragungszwecken eingesetzt werden sollen (§ 75 Abs. 1 S. 3 SGB X).[158] Dabei müssen auch hier die oben genannten, grundlegenden Anforderungen an die Einwilligung erfüllt sein, wobei ein besonderes Augenmerk auf die Gestaltung der Einwilligung im Hinblick auf die Freiwilligkeit zu richten ist.[159] Im Hinblick auf die Zweckbestimmung ist das konkrete Vorhaben im Rahmen der Einwilligung zu benennen und soweit möglich zu beschreiben. Für Einwilligungen in die Übermittlung zu Forschungszwecken besteht gemäß § 67b Abs. 3 SGB X daneben jedoch auch die Möglichkeit eines Broad Consent.[160]

155 Vgl. *Bieresborn*, in: von Wulffen/Schütze, SGB X, 8. Aufl. 2014, § 75 Rn. 6.
156 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 40; *Bieresborn*, in: von Wulffen/Schütze, SGB X, 8. Aufl. 2014, § 75 Rn. 6.
157 Vgl. hierzu oben Kap. 1.4.3.2.3, Abschnitt „Anforderungen an i.R.d. § 295 Abs. 1b S. 1 SGB V übermittelte Daten".
158 Vgl. oben Kap. 1.4.3.2.3, Abschnitt: „Vorrang der Einwilligung (§ 75 Abs. 1 S. 2 SGB X)".
159 Vgl. oben Kap. 1.4.3.3.
160 Hierzu sogleich Kap. 3.2.

Entbehrlichkeit

Gemäß § 75 Abs. 1 S. 3 SGB X ist die Einwilligung des Betroffenen immer dann entbehrlich, wenn lediglich Angaben zum Namen, Vornamen, Anschrift, Telefonnummer sowie zu für die Einleitung des Forschungsvorhabens zwingend erforderlichen Strukturmerkmalen der Person – hierzu gehören allgemeine Merkmale wie Alter, Herkunft, Berufsstatus[161] – ausschließlich für Befragungen übermittelt werden. Mit dieser Ausnahmeregelung für Kontaktdaten zum Zweck der Befragung soll einer frühzeitigen, nicht mehr korrigierbaren Selektion und Verzerrung der Forschungsergebnisse begegnet werden.[162] Sollen die Daten jedoch über die bloße Befragung hinaus verarbeitet werden, bedarf die Übermittlung einer gesonderten Ermächtigungsgrundlage.

Darüber hinaus ist die Einwilligung entbehrlich, sofern die Einholung für die übermittelnde Stelle unzumutbar ist.[163] Die Darlegungslast für die Unzumutbarkeit der Einholung der Einwilligungen obliegt der übermittelnden Stelle.[164] Diese muss im Rahmen des Genehmigungsverfahrens die Gründe für die Unzumutbarkeit im Einzelnen darlegen.

Einwilligungserfordernis nach § 76 SGB X (Schweigepflichtverlängerung)

Trotz einer möglichen Entbehrlichkeit der datenschutzrechtlichen Einwilligung nach § 75 Abs. 1 SGB X, besteht ein Erfordernis nach einer Schweigepflichtentbindung (strafrechtlichen Einwilligungserklärung), sofern bei der Übermittlung solche Sozialdaten an einen Dritten übertragen werden, die die Krankenkassen originär von einem Arzt oder einer sonst nach § 203 Abs. 1 StGB geheimnisverpflichteten Person erhalten haben. So heißt es in § 76 Abs. 1 SGB X:

> *„Die Übermittlung von Sozialdaten, die einer in § 35 des Ersten Buches genannten Stelle von einem Arzt oder einer Ärztin oder einer anderen in § 203 Absatz 1 und 3 des Strafgesetzbuches genannten Person zugänglich gemacht worden sind, ist nur unter den Voraussetzungen zulässig, unter denen diese Person selbst übermittlungsbefugt wäre."*

Für die von Ärzten übermittelten Abrechnungsdaten ist höchstrichterlich entschieden, dass diese Daten dem Schutzbereich des § 203 StGB unterfallen.[165] Folglich darf der Sozialleistungsträger die Daten, die ihm beispielsweise von einem Arzt aufgrund der §§ 284ff. SGB V übermittelt worden sind, nur an Dritte

161 *Krause*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 75 Rn. 50.1; *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 40b.
162 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 40b.
163 Siehe dazu im Detail Kapitel 1.4.3.2.3, Abschnitt „Vorrang der Einwilligung".
164 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 33.
165 BGH, Urteil vom 10.07.1991, VIII ZR 296/90.

übermitteln, wenn der Arzt vor dem Hintergrund des § 203 StGB selbst befugt wäre, diese Daten zu den entsprechenden Zwecken an den Dritten zu offenbaren. Eine Befugnis zur Offenbarung i.S.d. § 203 StGB kann etwa anzunehmen sein, wenn der Betroffene eine Schweigepflichtentbindung hinsichtlich der Weitergabe der Daten erteilt hat oder eine gesetzliche Offenbarungspflicht oder -befugnis besteht. Letzteres ist für Ärzte regelmäßig nicht gegeben. Für Ärzte selbst existieren keine gesetzlichen Ermächtigungsgrundlagen, die eine Weitergabe personenbezogener Daten zu Forschungszwecken erlauben. Im Einzelfall kann eine datenschutzrechtliche Norm zwar eine Befugnis zur strafrechtlichen Offenbarung enthalten, wenn sich dies aus dem Wortlaut der betreffenden Norm klar ergibt. Das Bundesverfassungsgericht sieht § 203 StGB wegen des Merkmals „unbefugt" als sog. Blankettnorm an[166], sodass auch landesrechtliche Gesetze und gegebenenfalls auf einer ausreichenden Ermächtigung beruhende Verordnungen eine Befugnis einräumen können.[167] Selbst die in einigen Landeskrankenhausgesetzen enthaltenen Forschungsklauseln betreffen im Regelfall nur die krankenhausinterne Forschung und nicht die Weitergabe der Daten zu Forschungszwecken an externe Dritte. Diese Frage ist je nach einschlägigem Landesrecht im Einzelfall zu prüfen. Regelmäßig bedarf es einer Schweigepflichtentbindungserklärung des Betroffenen, um den Arzt von seiner Schweigepflicht zu entbinden und die Übermittlung zu legitimieren.

Zwar wird nicht verlangt, dass die Rechtfertigungsgründe von Erstübermittlung und Zweitübermittlung identisch sind, sodass der an § 76 SGB X gebundene Zweitübermittler auch andere Rechtfertigungsgründe heranziehen kann, auf die sich der originär an § 203 StGB gebundene Erstübermittler hätte stützen können.[168] Ein Sozialleistungsträger wird aufgrund der verlängerten ärztlichen Schweigepflicht aber in der Regel einer Schweigepflichtentbindung des Betroffenen benötigen, um die personenbezogenen Abrechnungsdaten der Ärzte zu Forschungszwecken an einen Dritten übermitteln zu können. Die Ausnahmetatbestände des § 75 Abs. 1 S. 2 und 3 SGB X helfen hier nicht weiter. Vielmehr besteht dieses aus der strafrechtlich verankerten Geheimhaltungspflicht herrührende Zustimmungserfordernis neben dem datenschutzrechtlichen Einwilligungserfordernis (§ 35 Abs. 2a SGB I). Ist die Einwilligung aus datenschutzrechtlicher Sicht entbehrlich, bedarf es bei Abrechnungsdaten dennoch einer Schweigepflichtentbindung. Die Schweigepflichtentbindung muss sich im Falle der Entbehrlichkeit der datenschutzrechtlichen Einwilligung jedoch nicht an den datenschutzrechtlichen Anforderungen messen lassen. Vielmehr kommt auf dieser Ebene auch eine formlose, gar konkludente Erklärung in Betracht. Da dem Sozialleistungsträger aber auch hier im Streitfall die Beweislast obliegt, ist eine schriftliche oder elektronische Einwilligung

166 BVerfGE 55, 274 (324f.).
167 *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 112 m.w.N.
168 *Bieresborn*, in: v. Wulffen/Schütze, 8. Aufl. 2014, SGB X § 76 Rn. 4–17a.

empfehlenswert. Inhaltlich muss die Erklärung lediglich die Entbindung von der Schweigepflicht in Bezug auf die zu benennenden Daten/Geheimnisse umfassen.

Es sei an dieser Stelle nochmals darauf hingewiesen,[169] dass eine Weitergabe von pseudonymisierten Daten hingegen in aller Regel ohne Schweigepflichtentbindung zulässig sein wird, da es insofern an einer Offenbarung im Sinne des § 203 StGB fehlen wird. Eine solche liegt nämlich dann nicht vor, wenn für den Empfänger eines Geheimnisses die Kenntnis der betreffenden Person nicht möglich ist. Auch hier gilt also, dass eine Pseudonymisierung für den Empfänger eines Datensatzes mit einer Anonymisierung gleichzusetzen sein kann und eine persönlichkeitsrechtliche Relevanz daher nicht mehr fortbesteht.

Maßnahmen nach § 22 BDSG

Sofern wie bei der Übermittlung von Abrechnungsdaten besondere Kategorien personenbezogener Daten – Gesundheitsdaten – an Dritte übermittelt werden, fordert § 67b Abs. 1 S. 4 SGB X, dass neben dem Erfordernis einer entsprechenden Ermächtigungsgrundlage die Gewährleistung der in § 22 Abs. 2 BDSG beschriebenen besonderen Schutzmaßnahmen durch den Dritten sichergestellt sind (siehe hierzu bereits Kap. 1.4.4).

Behördliche Genehmigung

Gemäß § 75 Abs. 4 SGB X bedarf die Übermittlung von Sozialdaten zu den in Absatz 1 und 2 genannten Forschungs- und Planungszwecken für bestimmte Vorhaben der behördlichen Genehmigung. Zuständige Genehmigungsbehörde ist die jeweilige oberste Bundes- oder Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist, mithin das im Einzelfall zuständige Bundes- oder Landesministerium (§ 75 Abs. 4 S. 1 SGB X). Entsprechend der Ermächtigung in § 75 Abs. 4 S. 2 SGB X hat das Gesundheitsministerium diese Aufgabe für Anträge der GKV Anfang 2012 auf das Bundesversicherungsamt übertragen,[170] sodass entsprechende Genehmigungen seither beim Bundesversicherungsamt zu beantragen sind.

Genehmigungsantrag

Der Genehmigungsantrag ist durch die empfangende Stelle zu stellen.[171] Er muss Ausführungen zu den wesentlichen Punkten des Vorhabens und den benötigten Daten enthalten. Dementsprechend ist zunächst das bestimmte Vorhaben und der betroffene Forschungs-/Planungsbereich i.S.d. § 75 Abs. 1 S. 1

169 Vergleiche bereits einleitend unter Kap. 1.4.2.
170 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 41a.
171 BT-Drs. 12/5187, S. 40.

SGB X möglichst genau darzustellen. Soweit es sich um ein Forschungsvorhaben im Sozialleistungsbereich handelt, welches aufgrund des Forschungsgegenstands nicht eindeutig dem Sozialleistungsbereich zugeordnet werden kann, weil der Forschungsschwerpunkt in einem anderen Bereich liegt, ist zudem darzulegen, dass die zu erwartenden Ergebnisse auch für den Sozialleistungsbereich von Relevanz sein können.[172] Darüber hinaus ist darzulegen, welche Sozialdaten benötigt werden, in welchen Phasen des Vorhabens diese relevant werden, welcher Personenkreis betroffen sein wird und für welchen Zeitraum die Daten zu dem entsprechenden Zweck verarbeitet werden sollen.[173] Des Weiteren sind im Antrag Ausführungen dazu zu machen, dass die Betroffeneninteressen nicht beeinträchtigt werden oder inwiefern das öffentliche Interesse an dem Vorhaben diese überwiegt. Sofern die Übermittlung ohne Einwilligung und Anonymisierung erfolgen soll, sind die Gründe für die Unzumutbarkeit der Einholung der Einwilligungen sowie die einer Anonymisierung entgegenstehenden Gründe darzulegen.[174]

Wird der Antrag entsprechend § 75 Abs. 2 SGB X auf die Genehmigung der Übermittlung weiterer Sozialdaten für die Bearbeitung von Forschungsfolgefragen erstreckt, muss der inhaltliche Zusammenhang mit dem Ausgangsvorhaben dargelegt werden. Da der von § 75 Abs. 2 SGB X geforderte inhaltliche Zusammenhang dabei eher eng auszulegen ist, sind im Einzelfall detaillierte Angaben notwendig. Die Gesetzesbegründung nennt in diesem Zusammenhang beispielhaft die Änderung oder Erweiterung einzelner Elemente des Forschungsvorhabens, die den Charakter des Vorhabens als solchen nicht verändern.[175]

Werden, wie dies bei Abrechnungsdaten der Fall ist, besondere Kategorien personenbezogener Daten übermittelt, muss der Datenempfänger Angaben zu dem von ihm vorgehaltenen angemessenen und spezifischen Maßnahmen zur Wahrung der Interessen der Betroffenen i.S.d. § 22 BDSG machen. Bei der Übermittlung der Daten an eine nicht-öffentliche Stelle hat der Empfänger zudem eine Verpflichtungserklärung dahingehend abzugeben, dass dieser die Daten entsprechend § 78 Abs. 1 S. 1 SGB X nur zu dem beantragten Zweck verarbeiten wird.

Zudem ist gemäß § 75 Abs. 1 S. 4 SGB X ein Datenschutzkonzept vorzulegen.

Genehmigungsbescheid

Liegt ein ordnungsgemäßer Antrag nach § 75 Abs. 4 SGB X vor und sind alle Voraussetzungen des § 75 Abs. 1 SGB X – sowie bei der erweiterten Genehmigung

172 Vgl. Kap. 1.5.3.2.4, Abschnitt: „Bereich der wissenschaftlichen Forschung im Sozialleistungsbereich".
173 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 45.
174 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 45.
175 BT-Drs. 18/12611, S. 118.

der Absätze 2 bzw. 4a – erfüllt, hat die Behörde die Genehmigung ohne einen Ermessensspielraum gegenüber dem Empfänger zu erteilen.[176] Die Entscheidung ergeht in Form eines Verwaltungsakts und ist dem Leistungsträger ebenfalls bekanntzugeben.[177] Gemäß § 75 Abs. 4 S. 5 SGB X muss die Genehmigung den Dritten, an den die Daten übermittelt werden, die Art der zu übermittelnden Sozialdaten und den betroffenen Personenkreis sowie die wissenschaftliche Forschung oder die Planung, zu der die übermittelten Sozialdaten verwendet werden dürfen genau bezeichnen. Darüber hinaus muss aus der Genehmigung der Tag hervorgehen, bis zu dem die übermittelten Sozialdaten verarbeitet werden dürfen. Zudem kann die Behörde unmittelbar mit dem Erlass des Bescheides oder auch nachträglich Auflagen erteilen, ergänzen oder ändern. Ist der Empfänger eine nicht-öffentliche Stelle, hat die Behörde die Einhaltung der Vorgaben des § 75 SGB X über eben solche Auflagen sicherzustellen.

Neben dem Antrag ist der Genehmigungsbehörde zudem ein Datenschutzkonzept vorzulegen, aus dem hervorgeht, dass der Empfänger die technischen und organisatorischen Anforderungen des Datenschutzes i.S.d. Art. 32 DSGVO sowie den Grundsatz der Datenminimierung erfüllt.[178]

Löschung

Grundsätzlich sind personenbezogene Daten zu löschen, sobald sie für den jeweiligen Zweck nicht mehr erforderlich sind (§ 304 Abs. 3 SGB V i.V.m. § 84 Abs. 2 SGB X a.F.; vgl. Art. 17 Abs. 1 lit. a) DSGVO)[179]. Demzufolge müssten die Daten nach Abschluss des Forschungsvorhabens bzw. nach Ablauf des im Genehmigungsbescheid genannten Zeitpunkts unmittelbar gelöscht werden. Um eine Nachprüfung der Forschungsergebnisse auf der Grundlage der aufbereiteten Daten sowie die Verarbeitung der Daten für weitere Forschungsvorhaben gemäß Abs. 2 zu ermöglichen, bestimmt § 75 Abs. 4 S. 6 SGB X jedoch, dass die Daten nach Ablauf des von der Genehmigungsbehörde für die Verarbeitung bestimmten Vorhabens bis zu zehn Jahre aufbewahrt werden können. Dabei obliegt es der Genehmigungsbehörde durch Auflagen zu bestimmen, wie lang und bei welcher Stelle (übermittelnde oder empfangende Stelle) die Daten gespeichert werden können.[180] Zudem kann sie weitere Auflagen für die verlängerte Speicherung erteilen.

176 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 47.
177 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 75 Rn. 47.
178 BT-Drs. 18/12611, S. 118.
179 § 304 SGB V ist anpassungsbedürftig, da infolge der unmittelbaren Geltung des Art. 17 DS-GVO auch § 84 SGB X angepasst wurde und der Löschbefehl nicht mehr in § 84 SGB X normiert ist, sodass die Verweisung fehlerhaft ist. An dieser Stelle sei darauf hingewiesen, dass der Entwurf zum 2. DSAnpUG-EU die Streichung des Verweises auf § 84 Abs. 2 SGB X entsprechend vorsieht, vgl. BT-Drs. 19/4674, S. 143.
180 BT-Drs. 18/12611, S. 119.

Möglichkeiten der Verweigerung der Herausgabe der Daten an eine externe Einrichtung trotz Vorliegens einer Einwilligung

§ 75 SGB X erklärt die Datenübermittlung bei Vorliegen aller genannten Voraussetzungen für zulässig. Damit ist der Leistungsträger im Einzelfall befugt, die Daten zu übermitteln. Eine Verpflichtung lässt sich aus dem Wortlaut des § 75 SGB X nicht herleiten.[181] Auch die Einwilligung des Betroffenen verpflichtet den Verantwortlichen nicht, die Daten tatsächlich zu den genannten Zwecken zu übertragen. Vielmehr stellt die Einwilligung lediglich eine Befugnis dar.

Fraglich ist jedoch, ob sich aus der behördlichen Genehmigung zumindest mittelbar eine Pflicht zur vollumfänglichen Übertragung der in der Genehmigung benannten Daten ergibt. Zwar stellt auch die Genehmigung zunächst lediglich eine Übermittlungsbefugnis und keine -verpflichtung dar. Jedoch kann sich die Genehmigung entsprechend dem Sinn und Zweck des gegenständlichen Vorhabens zu einer Verpflichtung verdichten. So kann die Verweigerung der Herausgabe einzelner Daten im Rahmen eines genehmigten Vorhabens die Gefahr einer selektiven Informations-/Forschungs-/Planungsgrundlage bergen und so zu einer Verzerrung der Forschungsergebnisse führen. Dies entspräche dann jedoch nicht mehr dem behördlich genehmigten Vorhaben. Sofern die Genehmigung folglich bestimmte Datensätze bestimmter Personenkreise für ein Vorhaben umfasst, sind diese auch in Gänze zu übermitteln. Nur sofern eine solche Gefahr der Selektivität und der Ergebnisverzerrung im Einzelfall plausibel ausgeschlossen werden kann, ließe sich entsprechend der obigen Ausführungen gegen eine Übermittlungspflicht argumentieren. Darüber hinaus kann sich eine Übermittlungspflicht auch aus den konkreten vertraglichen Regelungen zwischen der übermittelnden und der empfangenden Stelle ergeben.

Zwischenergebnis

Zu Zwecken der wissenschaftlichen Forschung und Planung im Sozialleistungsbereich kommt eine Übermittlung von Sozialdaten gemäß § 75 SGB X in Betracht, soweit die Genehmigung der zuständigen Genehmigungsbehörde vorliegt (§ 75 Abs. 4 SGB X). Diese Genehmigung ist zu erteilen, wenn die Voraussetzungen des § 75 Abs. 1 SGB X, sowie bei der erweiterten Genehmigung der Absätze 2 und 4a vorliegen. Dabei muss der Schwerpunkt des Vorhabens im Bereich der Forschung nicht zwingend auf dem Sozialleistungsbereich liegen. Ausreichend ist, dass die Forschungsergebnisse dem Sozialleistungsbereich mit gewisser Wahrscheinlichkeit dienlich sind.

Gemäß § 75 Abs. 1, § 76 SGB X ist für die Übermittlung von Sozialdaten in diesen Bereichen grundsätzlich die Einwilligung der Betroffenen erforderlich.

181 Hase, DuD 2011, 875 (876).

Zwar sieht § 75 Abs. 1 SGB X auf datenschutzrechtlicher Ebene eine Ausnahme von diesem Erfordernis vor, sofern die Einholung unzumutbar ist. Aufgrund der Ausdehnung der Voraussetzungen der Geheimhaltungspflicht nach § 203 StGB in § 76 SGB X bedarf es jedoch – entsprechend den Anforderungen, die etwa ein Arzt einhalten müsste – auch in diesen Fällen grundsätzlich einer Einwilligung in Form einer Schweigepflichtentbindung.

Entsprechend dem Grundsatz der Datenminimierung dürfen Sozialdaten nur in einem Umfang übermittelt werden, der für die Zweckerreichung im jeweiligen Vorhaben auch erforderlich ist. Eine unbegründete, wahllose Datenübermittlung dürfte daher regelmäßig im Genehmigungsverfahren scheitern. Zudem sind die Daten auch hier zu anonymisieren, soweit es der Forschungszweck zulässt. Darüber hinaus darf die Übermittlung keine schutzwürdigen Interessen der Betroffenen beeinträchtigen, es sei denn, das öffentliche Interesse an dem Vorhaben überwiegt diese erheblich.

Der Empfänger muss über technische und organisatorische Maßnahmen sicherstellen, dass die Rechte und Interessen der Betroffenen hinreichend geschützt werden und hat diese Maßnahmen im Genehmigungsverfahren über ein Datenschutzkonzept und entsprechende Nachweise zu belegen. Dabei ist es für den Bereich der wissenschaftlichen Forschung unerheblich, ob die empfangende Stelle eine öffentliche oder eine nicht-öffentliche Stelle ist. Letztere haben im Rahmen des Genehmigungsverfahrens lediglich zusätzliche Verpflichtungserklärungen zur zweckgebundenen Verarbeitung abzugeben. Für den Bereich der Planung kommen als Empfänger hingegen nur öffentliche Stellen in Betracht, da § 75 Abs. 1 S. 1 Nr. 2 SGB X fordert, dass die Planung zum Aufgabenbereich der jeweiligen Stelle gehört.

In jedem Fall unterliegt auch die externe Stelle mit Erhalt der Sozialdaten dem Sozialgeheimnis nach § 35 SGB I und hat dafür Sorge zu tragen, alle mit den Daten befassten Mitarbeiter entsprechend zu verpflichten.

1.5.3.3 Einwilligung

Die Übermittlung der Daten an eine externe Einrichtung zu Zwecken der wissenschaftlichen Forschung, der Planung im Sozialleistungsbereich oder der Qualitätssicherung kann alternativ auf Grundlage einer Einwilligung des Betroffenen erfolgen. Dabei sind die oben genannten allgemeinen und speziellen/sozialrechtlichen Anforderungen an die Einwilligung zu beachten[182]. Wie bereits oben unter A.III.3.a) (s. Kap. 1.4.3.3.1) ausgeführt, ist aufgrund des bestehenden Abhängigkeitsverhältnisses zwischen Leistungsträger und Betroffenem besonderes Augenmerk auf die Gestaltung der Einwilligung im Hinblick auf die Freiwilligkeit der Erklärung zu richten.

182 Vgl. oben Kap. 1.4.3.3.

1.5.3.4 Auftragsverarbeitung

Neben der Übermittlung der Daten an eine eigenständige externe Stelle ist es zudem denkbar, dass sich der Leistungsträger eines Auftragsverarbeiters bedient, um die personenbezogenen Abrechnungs-/Sozialdaten zu Zwecken der Forschung, Planung oder Qualitätssicherung zu verarbeiten. Eine externe Stelle ist immer dann als Auftragsverarbeiter einzuordnen, wenn sie die Daten im Interesse und auf Weisungen des Verantwortlichen verarbeitet und keine wesentlichen Entscheidungen über Zweck und Mittel der Datenverarbeitung trifft.[183]

Art. 28 DSGVO enthält spezifische Regeln zur Ausgestaltung und Zulässigkeit der Auftragsverarbeitung. Darüber hinaus enthält § 80 SGB X speziell für den Bereich des Sozialdatenschutzes weitere Vorgaben zur Auftragsverarbeitung. Da Art. 28 DSGVO keine Öffnungsklauseln in Bezug auf die Auftragsverarbeitung enthält, ist fraglich, inwiefern diese bereichsspezifische nationale Norm mit der DSGVO in Einklang steht. Da die Auftragsverarbeitung jedoch als (ausgelagerter) Verarbeitungsvorgang des Verantwortlichen zu verstehen ist, können weitergehende Regelungen durch die Mitgliedsstaaten getroffen werden, sofern innerhalb der DSGVO (Art. 6–10 DSGVO) Öffnungsklauseln für den konkreten Bereich der Datenverarbeitung existieren.[184] Die Regelung des § 80 SGB X ist folglich über die Öffnungsklauseln der Art. 6. Abs. 1 lit. e), Abs. 2, Abs. 3 S, 3, Art. 9 Abs. 2 lit. b), h), j) DSGVO europarechtskonform.

1.5.3.4.1 Ermächtigungsgrundlage

Fraglich ist zunächst, ob die Weitergabe der Sozialdaten an einen Auftragsverarbeiter ebenso wie die Weitergabe der Daten an einen Dritten einer gesonderten gesetzlichen Ermächtigungsgrundlage bedarf.

Datenschutzrechtliche Ermächtigung

Nach dem BDSG a.F. kam der Auftragsverarbeitung eine Privilegierung in der Form zu, dass eine Weitergabe der Daten an den Auftragsverarbeiter nicht als Übermittlung, sondern vielmehr als interne Nutzung der Daten verstanden wurde, die einer gesonderten Ermächtigungsgrundlage nicht bedurfte. Eine Weitergabe an den Auftragsverarbeiter war immer dann zulässig, wenn die Verarbeitung durch den Verantwortlichen selbst rechtmäßig war. Begründet wurde dies mit den Definitionen der §§ 3 Abs. 4 Nr. 3, 3 Abs. 8 S. 2 und 3 BDSG a.F., nach denen eine Übermittlung nur bei der Weitergabe der Daten an einen Dritten vorliegt, der Auftragsverarbeiter aber gerade kein Dritter ist.

183 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 4 Nr. 8 Rn. 7.
184 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 113.

Die DSGVO greift diese Definition der Übermittlung nicht auf, sondern erfasst diese als Unterfall der Verarbeitung in Form der Offenlegung (Art. 4 Nr. 2 DSGVO). Dabei liegt eine Offenlegung nach der DSGVO in jeder Weitergabe der Daten unabhängig von der Einordnung der empfangenden Stelle als Dritter oder Auftragsverarbeiter.[185] Dennoch wird in der Literatur das Fortbestehen der Privilegierung der Auftragsverarbeitung mit Verweis auf die historische Entwicklung und systematische Stellung der Auftragsverarbeitung sowie der Bedeutung der Auftragsverarbeitung auch im Rahmen der DSGVO befürwortet.[186] Insbesondere die Tatsachen, dass die DSGVO die Regelungen zur Auftragsverarbeitung im Wesentlichen aus der Datenschutz-Richtlinie, in deren Rahmen eine Privilegierung der Auftragsverarbeitung angelegt war[187], übernommen hat und dass der Auftragsverarbeiter streng an die Weisungen des Verantwortlichen gebunden ist und Art. 28 DSGVO detaillierte Anforderungen an die Auftragsverarbeitung stellt, sprechen dafür, dass die Weitergabe von Daten auch nach der DSGVO keines gesonderten Erlaubnistatbestands bedarf.[188] Ohne eine Privilegierung der Auftragsverarbeitung würden die zahlreichen besonderen Regelungen zur Auftragsverarbeitung in der DSGVO keinen Sinn ergeben. Folglich ist die Weitergabe der Abrechnungsdaten zu Zwecken der wissenschaftlichen Forschung, Planung im Sozialleistungsbereich sowie der Qualitätssicherung an einen Auftragsverarbeiter aus datenschutzrechtlicher Sicht zulässig, sofern der Verantwortliche selbst zu einer Datenverarbeitung zu den entsprechenden Zwecken legitimiert ist.[189] Einer gesonderten Ermächtigungsgrundlage oder Einwilligung für die Weitergabe der Daten an den Auftragsverarbeiter bedarf es aus datenschutzrechtlicher Sicht daher nicht.[190]

Strafrechtliche Befugnis

Fraglich ist jedoch, inwiefern die Weitergabebefugnis aufgrund von § 76 SGB X durch den Geheimnisschutz nach § 203 StGB begrenzt wird. § 76 SGB X bestimmt, dass die Übermittlung von Sozialdaten, die der Leistungsträger von einer in § 203 Abs. 1 und 3 StGB genannten, zur Geheimhaltung verpflichteten Stelle erhalten hat, nur zulässig ist, wenn die nach § 203 Abs. 1 und 3 StGB verpflichtete Person selbst zur Übermittlung befugt wäre. Verlangt wird dabei

185 *Herbst*, in: Kühling/Buchner, DS-GVO, 2017, Art. 4 Nr. 2 Rn. 30f.

186 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 13ff.; *Schmitz/von Dall'Armi*, ZD 2016, 427 (429, 432); *Schmidt/Freund*, ZD 2017, 14; ebenso BayLDA, Auftragsverarbeitung nach der DS-GVO, Kurz-Papier vom 26.10.2016, 1. Nach anderer Ansicht ist die Zulässigkeit der Verarbeitung auch beim Auftragsverarbeiter zu prüfen, vgl. etwa Dovas, ZD 2016, 512 (516); eine solche dürfte in der Regel jedoch gerechtfertigt sein.

187 *Schmidt/Freund*, ZD 2017, 14 (15).

188 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 13ff.; Schmidt/Freund, ZD 2017, 14 (15f.).

189 Zur rechtmäßigen Verarbeitung von Sozialdaten durch den Leistungserbringer vgl. Ausführungen zu Szenario 1, s. Kap. 1.4.3.1.1.

190 Ebenso *Unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK*), Kurzpapier Nr. 13, Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.02.2018, S. 2.

nicht die Identität der Rechtfertigungsgründe von Erstübermittlung und Zweitübermittlung; der an § 76 SGB X gebundene Zweitübermittler kann also auch andere Rechtfertigungsgründe heranziehen, auf die sich der originär an § 203 StGB gebundene Erstübermittler hätte stützen können.[191]

Ob davon aber nur die Weitergabe der Daten an einen Dritten oder auch die Weitergabe an einen Auftragsverarbeiter erfasst ist, ist bisher nicht geklärt.

Jegliche Offenbarung i.S.d. § 203 StGB erfasst

Der Begriff der Übermittlung stellt nach der DSGVO nicht mehr auf die Weitergabe der Daten an einen Dritten ab. Vielmehr ist nunmehr jegliche Übermittlung an einen Empfänger eine Form der Verarbeitung im Sinne der Offenlegung. Dementsprechend ließe sich auch die Weitergabe der Daten an einen Auftragsverarbeiter unter den Begriff der Datenübermittlung subsumieren. Zudem besagt § 35 Abs. 2a SGB I, dass die Berufsgeheimnisse sowie die gesetzlichen Geheimhaltungspflichten unberührt bleiben und folglich umfassend neben den datenschutzrechtlichen Regelungen fortgelten sollen. Daraus ließe sich folgern, dass die gesetzliche Geheimhaltungspflicht des § 203 StGB auch bei einer Verlängerung umfassend neben den datenschutzrechtlichen Pflichten gelten soll. Ist dies der Fall, wäre dem Leistungsträger jedoch jegliche Offenbarung gegenüber einem nicht gemäß § 203 StGB zum Mitwissen Befugten und somit auch gegenüber dem Auftragsverarbeiter ohne die Einwilligung/Schweigepflichtentbindungserklärung des Betroffenen unzulässig.

Nur die Weitergabe an Dritte erfasst

§ 76 SGB X beschränkt nach seinem Wortlaut – wie bereits bisher § 76 Abs. 1 SGB X a.F. – lediglich die Befugnis zur Übermittlung von besonders schutzwürdigen Sozialdaten. Entsprechend der Definition des Übermittlungsbegriffs in § 3 Abs. 4 Nr. 3 BDSG a.F., nach der eine Übermittlung nur an Dritte, nicht aber an Auftragsverarbeiter erfolgen kann, wäre die Verlängerung des § 203 StGB nicht auf die Weitergabe der Daten an den Auftragsverarbeiter zu übertragen. Für diese Auffassung spricht, dass mit dem 2. SGBÄndG der Wortlaut der Norm von „Offenbarung", die jegliche Preisgabe von Daten an andere erfasst, auf Übermittlung umgestellt wurde und damit vermeintlich bewusst ein engerer Kreis gezogen wurde.[192] Dass der Gesetzgeber im Rahmen des § 76 SGB X keine Ausführungen zu einem veränderten Geltungsbereich des § 76 SGB X gemacht hat, spricht dafür, dass ihm die Problematik nicht bewusst und keine Änderung gewollt war. Zudem ist zwar die Eigenschaft des Empfängers, Dritter zu sein, für eine Übermittlung nach der DSGVO nicht mehr

191 *Bieresborn*, in: v. Wulffen/Schütze, 8. Aufl. 2014, SGB X § 76 Rn. 4–17a.

192 So im Ergebnis bei einem Vergleich zu § 39 BDSG a.F. zur aktuellen Fassung Rombach, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 76 Rn. 9.

maßgeblich. Jedoch ist dies für eine Weitergabe der Daten an den Auftragsverarbeiter auch nicht relevant, da dieser Vorgang lediglich einen Teil der internen Verarbeitung durch den Verantwortlichen darstellt, der zulässig ist, wenn die Verarbeitung durch den Verantwortlichen ihrerseits zulässig ist und die gesetzlichen Vorgaben der Auftragsverarbeitung eingehalten werden. Die Weitergabe der Daten an einen Auftragsverarbeiter wäre folglich auch mit Blick auf § 203 StGB ohne Einwilligung des Betroffenen zulässig.

Exkurs: Übermittlungsbefugnis des Geheimnisträgers nach § 203 StGB

Ginge man von der erstgenannten Ansicht (s. Kap. 1.5.3.4.1 Abschnitt „Jegliche Offenbarung i.S.d. § 203 StGB erfasst") aus, wäre auch die Weitergabe der Daten durch den Leistungserbringer an den Auftragsverarbeiter nur zulässig, wenn der nach § 203 StGB unmittelbar Geheimnisverpflichtete – beispielsweise der Arzt – selbst zur Weitergabe berechtigt wäre. Dies war nach § 203 StGB a.F. nur der Fall, wenn der Arzt sich auf eine entsprechende gesetzliche Ermächtigungsgrundlage, die Einwilligung des Patienten oder einen sonstigen strafrechtlichen Rechtfertigungsgrund stützen könnte. Dies ist bei der Übermittlung zu Forschungs- und Planungszwecken jedoch regelmäßig nicht der Fall.[193]

Diese Problematik löst sich auch nach Inkrafttreten des nunmehr geltenden § 203 StGB nicht vollständig. Zwar wird durch § 203 Abs. 3 StGB der Kreis der zum Mitwissen Befugten auf sonstige Personen, die an der beruflichen oder dienstlichen Tätigkeit des Geheimnisverpflichteten mitwirken, also etwa bestimmte Auftragsverarbeiter, erweitert. Diese Erweiterung erstreckt sich jedoch nur auf Auftragsverarbeiter, die an der beruflichen oder dienstlichen Tätigkeit des Geheimnisverpflichteten mitwirken. Stellt man hier auf den Arzt und die für ihn geltenden Rechtsgrundlagen ab, erweist sich die Übertragung des Geheimnisschutzes nach § 203 StGB als problematisch. Denn für einen Vertragsarzt gehört die Forschung oder Planung im Sozialleistungsbereich wohl nicht zu seiner beruflichen Tätigkeit, sodass ein Mitwirken nach dem nunmehr geltenden § 203 Abs. 3 StGB abzulehnen ist und eine zulässige Offenbarung ausscheidet. Für den Arzt einer Uniklinik gehört die Forschung hingegen zumeist zum Bereich seiner dienstlichen Tätigkeit, sodass ein Mitwirken an dieser i.S.d. § 203 StGB möglich und eine Weitergabe der Daten an einen Auftragsverarbeiter zulässig ist. Eine solche Differenzierung dürfte in der Praxis kaum zu handhaben sein. Auch dies spricht letztendlich gegen eine Übertragung der Geheimnisverpflichtung bei der Weitergabe der Daten an einen Auftragsverarbeiter.

193 Hierzu siehe oben Kap. 1.5.3.2.4, Abschnitt „Einwilligungserfordernis nach § 76 SGB X (Schweigepflichtverlängerung)".

Zwischenergebnis

Wie die Prüfüberlegung (s. Kap. 1.5.3.4.1, Abschnitt „Exkurs: Übermittlungsbefugnis des Geheimnisträgers nach § 203 StGB“) zeigt, würde die Ausweitung des Geltungsbereichs des § 76 SGB X auf Auftragsverarbeiter im Einzelfall zu erheblichen Subsumtionsproblemen führen, sodass auch dies dafür spricht, die Weitergabe der Daten an den Auftragsverarbeiter vom Anwendungsbereich des § 76 SGB X auszunehmen.

1.5.3.4.2 Anforderungen nach § 80 SGB X

Bedient sich der Leistungsträger eines Auftragsverarbeiters, sind die zusätzlichen Anforderungen des § 80 SGB X sowie des Art. 28 DSGVO zu beachten.

Gemäß § 80 Abs. 1 SGB X hat der Verantwortliche die Einschaltung eines Auftragsverarbeiters der für ihn zuständigen Fach- oder Rechtsaufsicht (Bundesversicherungsamt oder Sozialministerien der Länder) schriftlich oder elektronisch anzuzeigen. Die Anzeige muss dabei Angaben

- zum Auftragsverarbeiter,
- zu dessen technischen und organisatorischen Maßnahmen sowie
- zu den erteilten ergänzenden Weisungen,
- der Art der betroffenen Daten und Personenkreise
- der Aufgabe, deren Erfüllung die Einschaltung dient sowie
- zum Abschluss etwaiger Unterauftragsverhältnisse

enthalten. Sofern der Auftragsverarbeiter seinerseits eine öffentliche Stelle ist, hat dieser seine Rechts- oder Fachaufsicht gleichermaßen rechtzeitig von der Beauftragung zu unterrichten. Die Rechtzeitigkeit der Anzeige soll der Aufsichtsbehörde die Möglichkeit der Stellungnahme oder Beratung vor Abschluss des Auftrages ermöglichen und ist entsprechend der Umstände im Einzelfall zu berechnen. In jedem Fall hat sie vor Auftragserteilung zu erfolgen.

Eine Auftragserteilung an eine nicht-öffentliche Stelle ist gemäß § 80 Abs. 3 SGB X nur zulässig, wenn bei dem Verantwortlichen selbst Störungen im Betriebsablauf zu befürchten wären oder die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.[194] Insbesondere im Bereich der Forschung sind durchaus Vorhaben denkbar, bei denen der Aufwand Störungen im Betriebsablauf der Leistungsträger begründen oder die bei nicht-öffentlichen Stellen mit entsprechender Ausrüstung/Ausstattung

194 Nach dem Entwurf für das 2. DSAnpUG-EU soll dies nicht gelten, wenn Dienstleister in der Informationstechnik, deren absolute Mehrheit der Anteile oder deren absolute Mehrheit der Stimmen dem Bund oder den Ländern zusteht, mit vorheriger Genehmigung der obersten Dienstbehörde des Verantwortlichen beauftragt werden; BT-Drs. 19/4674, S. 154. Die Regelung soll insbesondere der Förderung der Umsetzung der vom Bundeskabinett beschlossenen Vorhaben zur IT-Konsolidierung in der Bundesverwaltung dienen; BT-Drs. 19/4674, S. 402.

kostengünstiger durchgeführt werden können. Dabei ist im Rahmen der Anzeige an die Behörde der Fach- oder Rechtsaufsicht eine nachvollziehbare Darlegung im Einzelfall erforderlich. Allgemein ist es aufgrund der erheblichen Restriktionen durchaus von Vorteil, öffentliche Stellen als Auftragsverarbeiter einzubinden. Ausgenommen von dieser Beschränkung sind lediglich Auftragsverhältnisse über die Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, bei denen ein Zugriff auf Sozialdaten nicht gänzlich ausgeschlossen werden kann (§ 80 Abs. 5 SGB X).

Abschließend unterwirft § 80 Abs. 4 SGB X den Auftragsverarbeiter der Aufsicht und den Befugnissen des Bundes- oder Landesdatenschutzbeauftragten für den Datenschutz und die Informationsfreiheit bzw. der nach Landesrecht zuständigen Aufsichtsbehörde sowie den Straf- und Bußgeldvorschriften der §§ 85 und 85a SGB X.

Darüber hinaus regelt § 80 Abs. 2 SGB X, dass eine Auftragserteilung nur zulässig ist, wenn die Datenverarbeitung im Inland, in einem Mitgliedsstaat der EU oder des EWR, der Schweiz oder einem Staat, der die Kommission ein angemessenes Schutzniveau per Beschluss nach Art. 45 DSGVO bescheinigt hat, verarbeitet werden. Mit dieser Beschränkung soll sichergestellt werden, dass sensible Sozialdaten nicht in einen unsicheren Drittstaat gelangen und dort einem geringeren Schutz und weitergehenden Verarbeitungsmöglichkeiten unterliegen.[195]

1.5.3.4.3 Anforderungen nach Art. 28 DSGVO

Die DSGVO enthält in Art. 28 umfangreiche Vorgaben für die Umsetzung einer wirksamen Auftragsverarbeitung.

Zunächst muss die Auftragsverarbeitung auf einen zwischen den Parteien geschlossenen schriftlichen oder elektronischen Vertrag basieren. Diese Verträge können individuell gestaltet sein oder auf (noch zu erstellenden) Standardvertragsklauseln der Kommission oder der Aufsichtsbehörden beruhen. Notwendige Inhalte des Vertrages sind:

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen sowie
- die Pflichten und Rechte des Verantwortlichen und
- die Pflichten des Auftragsverarbeiters,

wobei Letztere in Art. 28 Abs. 3 S. 2 DSGVO näher bestimmt sind (z.B. Weisungsgebundenheit, Verschwiegenheitsverpflichtung der Mitarbeiter, Unterstützung des Verantwortlichen). Die Beschreibung der Verarbeitung (Gegenstand,

195 BT-Drs. 18/12611, S. 124.

Art, Zweck, betroffene Daten und Personen) sind „angemessen ausführlich" zu beschreiben.[196] Es ist darauf zu achten, dass die Zweckbestimmung eindeutig beschrieben und erkennbar dem Verantwortlichen zugeordnet werden kann.[197] Aus der Beschreibung heraus muss ein Dritter wie etwa eine Datenschutzbehörde die Verarbeitungstätigkeit hinreichend klar einsehen können. Bei Pflichten und Rechten des Verantwortlichen ist an das Recht, über Löschung und Berichtigung der Daten und Auskünfte an Betroffene zu entscheiden, die Prüfung der generellen Zulässigkeit und Rechtmäßigkeit einer Datenverarbeitung wahrzunehmen und ausreichend Weisungen zu erteilen, zu denken.[198] Darüber hinaus steht es den Parteien frei, weitere Regelungen zu treffen.[199]

Daneben ist eine grundlegende Voraussetzung, dass die ausgewählten Auftragsverarbeiter hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen vorgehalten und eingesetzt werden, sodass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Dabei erfordert der Begriff der „Garantie" zumindest ausreichende (vertragliche) Verpflichtungen sowie Nachweise des Auftragsverarbeiters, die eine sorgfältige und gewissenhafte Erbringung der Tätigkeit unter Einhaltung der Vorgaben der DSGVO wahrscheinlich machen.[200] Künftig kann der Nachweis hinreichender Garantien zudem unter Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DSGVO nachgewiesen werden. Der Verantwortliche bleibt dabei auch nach Erteilung des Auftrags zur Begleitung und Kontrolle der Auftragsverarbeitung verpflichtet.[201] Eine Zusammenarbeit mit Auftragsverarbeitern ist ab dem Zeitpunkt nicht mehr gestattet, ab dem entsprechende Garantien nicht mehr gewährleistet sind.[202]

Des Weiteren enthält Art. 28 DSGVO die ausdrückliche Verpflichtung des Auftragsverarbeiters, Daten nur auf dokumentierte Weisung des Verantwortlichen oder einer gesetzlichen Pflicht zu verarbeiten (Art. 28 Abs. 3 S. 2 lit. a] DSGVO) und Unterauftragsverhältnisse nur mit Einwilligung des Verantwortlichen und bei Abschluss von Art. 28 Abs. 3 DSGVO entsprechenden Verträgen zu erteilen.

196 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 65 unter Verweis auf Art.-29-Datenschutzgruppe Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 32.
197 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 65.
198 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 66.
199 Vgl. hierzu Hartung, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 80.
200 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 56.
201 *Hartung*, in: Kühling/Buchner, DS-GVO, 2017, Art. 28 Rn. 60.
202 *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 28 Rn. 21.

1.5.3.4.4 Zwischenergebnis

Die Weitergabe von Sozialdaten an einen Auftragsverarbeiter im Rahmen der Durchführung eines bestimmten Vorhabens im Bereich der wissenschaftlichen Forschung oder der Planung im Sozialleistungsbereich ist ohne eine gesonderte Ermächtigungsgrundlage zulässig, sofern der Verantwortliche selbst zur Verarbeitung im entsprechenden Umfang befugt ist und die Voraussetzungen des § 80 SGB X sowie des Art. 28 DSGVO erfüllt sind. Dementsprechend ist ein Vertrag über die Auftragsverarbeitung mit den dort genannten Mindestangaben zu erstellen und die Beauftragung der jeweiligen Aufsichtsbehörde anzuzeigen. Dabei ergibt sich hinsichtlich der Auswahl des Auftragsverarbeiters eine Einschränkung dahingehend, dass nicht-öffentliche Stellen nur unter engen Voraussetzungen (bei dem Verantwortlichen sind ohne die Beauftragung Störungen im Betriebsablauf zu befürchten oder die Beauftragung ermöglicht eine erheblich kostengünstigere Bearbeitung) beauftragt werden können. Eine Ausnahme von dieser Restriktion besteht nach § 80 Abs. 5 SGB X lediglich für Auftragsverhältnisse zur Prüfung und Wartung automatisierter Verfahren der Datenverarbeitungsanlagen, auch wenn in diesem Rahmen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

1.5.3.5 Ergebnis

Die Weitergabe von Sozialdaten an eigenverantwortlich handelnde externe Einrichtungen ist in den Bereichen der wissenschaftlichen Forschung, der Planung im Sozialleistungsbereich sowie der Qualitätssicherung in unterschiedlichem Umfang möglich.

Für die Qualitätssicherung ergibt sich die Befugnis zur Übermittlung allein aus der spezialgesetzlichen Norm des § 299 SGB V, die eine Übermittlung ausschließlich nach den Vorgaben der Beschlüsse und Richtlinien des G-BA legitimiert.

Für den Bereich der wissenschaftlichen Forschung ist die Übermittlung an externe Stellen vornehmlich auf Grundlage von §§ 75, 76 SGB X möglich. Dabei stellen die §§ 75, 76 SGB X jedoch detaillierte Regelungen auf, deren Einhaltung im Rahmen eines obligatorischen Genehmigungsverfahrens überprüft wird. So stellen die vorzuhaltenden technischen und organisatorischen Maßnahmen, der Erforderlichkeitsgrundsatz und das grundsätzliche Einwilligungserfordernis, welches aufgrund der Ausweitung des strafrechtlichen Geheimnisschutzes (§ 203 StGB) auf die Übermittlung der von Ärzten stammenden Abrechnungsdaten nach § 76 SGB X – auch nicht unter den in § 75 SGB X genannten Voraussetzungen – entbehrlich ist, die wesentlichen Anforderungen an die Zulässigkeit des Vorhabens dar. Festzuhalten bleibt abschließend, dass die Übermittlung von Sozialdaten zum Zweck der wissenschaftlichen Forschung einem strengen Genehmigungsvorbehalt unterliegt und in jedem Fall der Einwilligung der Betroffenen (in Form einer Schweigepflichtentbindung) bedarf.

Für die Planung im Sozialleistungsbereich gestaltet sich die Übermittlung an eigenverantwortlich handelnde, externe Stellen ebenso wie im Bereich der Forschung. Einschränkend kommt hier hinzu, dass die externe Stelle nur eine öffentliche Stelle sein kann, bei der die Planung zum zugewiesenen Aufgabenbereich gehört.

Soll die externe Stelle als Auftragsverarbeiter eingebunden werden, bedarf dies nach hier vertretener Auffassung grundsätzlich keiner gesonderten Ermächtigungsgrundlage. Vielmehr ist die Einbindung als Teil der Verarbeitungstätigkeit des Verantwortlichen zulässig, wenn dieser zu der geplanten Form der Verarbeitung legitimiert ist und die zusätzlichen Anforderungen des Art. 28 DSGVO sowie des § 80 SGB X eingehalten werden. Neben dem Erfordernis eines Auftragsverarbeitungsvertrages ergibt sich aus § 80 Abs. 3 SGB X eine Einschränkung für die Beauftragung von nicht-öffentlichen Stellen, die nur unter den beschriebenen, sehr engen Voraussetzungen einbezogen werden können.

1.5.4 Zulässigkeit der Datenumgänge durch die externe Einrichtung (hinsichtlich der jeweiligen Zwecke)

1.5.4.1 Prüfungsmaßstab/Identifikation des einschlägigen Datenschutzregimes

Agiert die externe Stelle als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO, stellt sich die Frage nach dem einschlägigen Datenschutzregime erneut.

1.5.4.1.1 Rechtsnatur

Allgemein richtet sich die Anwendbarkeit – abgesehen vom umfassenden Geltungsanspruch der DSGVO – im deutschen Datenschutzrecht nach der Rechtsnatur des Verantwortlichen. Für öffentliche Stellen des Bundes sowie für nicht-öffentliche Stellen gilt im Grundsatz das BDSG gemäß § 1 Abs. 1 S. 1 Nr. 1 und S. 2 BDSG. Auf öffentliche Stellen der Länder ist im Grundsatz das jeweilige Landesdatenschutzgesetz anwendbar[203], nur in den Fällen des § 1 Abs. 1 S. 1 Nr. 2 BDSG findet auch das BDSG auf diese Anwendung.

1.5.4.1.2 Sonderfall Sozialdatenschutzrecht

Gemäß § 1 Abs. 2 S. 1 BDSG gehen andere Rechtsvorschriften des Bundes über den Datenschutz dem BDSG vor. Während dies in den meisten Fällen lediglich punktuell regelnde Normen des bereichsspezifischen Datenschutzrechts betrifft, bei dem das BDSG außerhalb einer Tatbestandskongruenz als Auffangnorm weiter Anwendung findet, ist das Sozialdatenschutzrecht nach § 35 SGB I i.V.m. §§ 67 ff. SGB X als Vollregelung konzipiert und regelt daher – mit

203 Auf eine Anpassung an die DS-GVO kommt es nicht an. Auch ohne Anpassung kommen die mit der DS-GVO vereinbaren landesdatenschutzrechtlichen Vorschriften zur Anwendung.

Ausnahme der DSGVO – die Verarbeitung von Sozialdaten abschließend (§ 35 Abs. 2 S. 1 SGB X). Ein Rückgriff auf das BDSG ist ausgeschlossen (vgl. § 1 Abs. 2 S. 2 BDSG).

Gleichzeitig knüpft das Sozialdatenschutzrecht nicht an der Rechtsnatur der verantwortlichen Stelle an, sondern nennt zunächst – wie auch nach bisherigem Recht – in § 35 Abs. 1 SGB I die sozialdatenschutzverpflichteten Stellen. Während die Aufzählung im bisherigen § 35 SGB I a.F. abschließend und nicht analogiefähig ist,[204] enthält nunmehr § 35 Abs. 6 SGB I eine Ausweitung der Sozialdatenschutzverpflichteten. Demnach sollen die Absätze 1 bis 5 des § 35 SGB I „neben den in Absatz 1 genannten Stellen" auch Anwendung auf solche Verantwortliche oder deren Auftragsverarbeiter finden, die Sozialdaten im Inland (nicht im Rahmen einer Niederlassung in einem anderen EU- oder EWR-Staat) oder im Rahmen der Tätigkeiten einer inländischen Niederlassung verarbeiten.

Diese Regelung ist problematisch. Die Anwendbarkeit eines bestimmten Datenschutzregimes wird nämlich nunmehr nicht mehr von der Anknüpfung an der Rechtsnatur oder einer festgelegten Anzahl an Stellen aus definiert, sondern knüpft am Charakter des Datums als Sozialdatum an. Der Begriff der Sozialdaten wird, wie oben bereits dargelegt, in § 67 Abs. 2 S. 1 SGB X definiert und nimmt hierbei insbesondere Bezug auf eine Verarbeitung durch eine „in § 35 des Ersten Buches genannten Stelle". Damit ergibt sich ein teilweiser Zirkelschluss, der das Potenzial einer ausufernden Anwendbarkeit des Sozialdatenschutzrechts, das unbestimmbar zu werden droht, birgt. Nach hier vertretener Ansicht ist eine restriktive Auslegung erforderlich, deren Bestimmung angesichts einer unpassenden Äußerung in den Gesetzgebungsmaterialien erschwert wird. Dort heißt es:

> *„Stellen, die nicht in Absatz 1 genannt und denen Sozialdaten übermittelt worden sind, sind gemäß § 78 Absatz 1 Satz 2 SGB X verpflichtet, die Daten in demselben Umfang geheim zu halten, wie eine in Absatz 1 genannte Stelle."*[205]

Diese Begründung setzt also – anders als der Normtext – voraus, dass zunächst eine Übermittlung durch eine Stelle nach § 35 Abs. 1 SGB I vorliegt, die den Anknüpfungspunkt für das initiale Vorliegen von Sozialdaten liefert. Im Übrigen ist die Begründung allerdings ihrerseits widersinnig. Zum einen käme § 78 SGB X – eo ipso – ohnehin zur Anwendung und bedürfte keiner Ausweitung des Anwendungsbereichs des Sozialgeheimnisses insgesamt. Zum anderen beinhaltet der Wortlaut des § 78 Abs. 1 S. 3 SGB X bei strenger Lesart auch nur eine **Geheimhaltung**spflicht, die im Sozialgeheimnis (s.o.) gerade nicht zu sehen ist. Im Sinne einer, auch von § 35 Abs. 2a SGB I ausdrücklich anerkannten, Unterscheidung von Geheimhaltungspflicht und Datenschutzrecht, ist

204 *Steinbach*, in: Hauck/Noftz/Becker, SGB I, Stand 07/2014, § 35 Rn. 22.

205 BT-Drs. 18/12611, S. 105; gemeint war hier aber wohl § 78 Abs. 1 S. 2 SGB X a.F., der in der neuen Fassung § 78 Abs. 1 S. 3 SGB X entspricht.

es zunächst konsequent, wenn gefordert wird, dass ein Empfänger die Sozialdaten wie ein Sozialleistungsträger „hüten" muss. So wird unter anderem gefordert, dass Empfänger, die keine originären Normadressaten des Sozialgeheimnisses sind, gem. § 2 Abs. 2 Nr. 2 Verpflichtungsgesetz auf das Sozialgeheimnis zu verpflichten sind.[206]

Allerdings wurde bisher auch ein weitergehendes Verständnis vertreten, wonach der Datenempfänger im Sinne des § 78 Abs. 1 S. 2 SGB X a.F. in „dieselbe Schutzpflichtposition eingewiesen wird" wie der „Datenabsender" und dadurch zum „abgeleiteten (derivativen) Normadressaten des § 35 SGB I" werde.[207] Das bedeute aber, dass diese Stelle die Daten auch wie ein Sozialleistungsträger unter den Voraussetzungen der §§ 68–76 SGB X a.F. verwenden dürfte.[208] Diese Beschränkung wird sowohl aus § 78 Abs. 1 S. 3 SGB X a.F. gefolgert, der ansonsten überflüssig wäre[209], als auch aus § 78 Abs. 1 S. 1 SGB X, da ansonsten die dort verortete „absolute Zweckbindung" umgangen werden könnte.[210]

Eben jene Argumentation könnte bei uneingeschränkter Anwendung des § 35 Abs. 6 SGB I aber beeinträchtigt werden, da dieser ausdrücklich auf die Absätze 1 bis 5 des § 35 SGB I verweist und somit – vermittels § 35 Abs. 2 SGB I – auch auf die §§ 67ff. SGB X.

Im Ergebnis ist daher eine dem Wortlaut prima facie zu entnehmende Ausdehnung des Anwendungsbereichs über § 35 Abs. 6 SGB I abzulehnen.

Dennoch führt dies nicht dazu, dass hinsichtlich der Verarbeitungsvorgänge, die durch den Empfänger durchgeführt werden, wiederum auf das für ihn allgemein geltende Datenschutzrecht (z.B. das BDSG) zurückgegriffen werden müsste oder könnte. Vielmehr folgt auch die Verarbeitungsbefugnis zu dem konkreten Zweck, zu dem die Daten übermittelt wurden, unmittelbar aus § 78 Abs. 1 S. 1 SGB X („dürfen").[211] Die Geheimhaltungspflicht des § 78 Abs. 1 S. 3 SGB X umfasst im Übrigen auch die Einhaltung der weiteren Anforderungen an die Verarbeitung, wie etwa Anforderungen an technische und organisatorische Maßnahmen, entsprechend den Vorgaben des für Stellen nach § 35 Abs. 1 SGB I geltenden Sozialdatenschutzes.[212]

1.5.4.2 Gesetzliche Ermächtigung

Somit gibt § 78 SGB X für die nach § 75 SGB X übermittelten Daten vor, in welchem Umfang und auf welche Art und Weise die Verarbeitung durch den

206 *Kunkel*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 78 SGB X, Rn. 20.
207 *Kunkel*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 78 SGB X, Rn. 19.
208 *Kunkel*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 78 SGB X, Rn. 19.
209 *Kunkel*, in: Schlegel/Voelzke, jurisPK-SGB X, 2013, § 78 SGB X, Rn. 19.
210 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 78 Rn. 25.
211 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 78 Rn. 13ff.
212 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 78 Rn. 11.

Empfänger der Daten erfolgen darf. Gemäß § 78 Abs. 1 S. 1 SGB X dürfen Empfänger, die nicht in § 35 SGB I genannt sind, die Daten ausschließlich zu den Zwecken speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, zu denen sie ihnen befugtermaßen übermittelt wurden (absolute Zweckbindung[213]). Dabei ist es unerheblich, ob die Stelle eine öffentliche oder nicht-öffentliche Stelle ist. Auch eine Weiterübermittlung durch die externe Einrichtung ist nur zulässig, wenn diese vom Zweck, der der Übermittlung durch den Sozialleistungsträger zugrunde liegt, umfasst sind.[214]

Sofern im Rahmen von § 78 SGB X a.F. noch darauf abgestellt wird, dass diese Befugnis nur für die konkrete Zweckbestimmung des einzelnen Vorhabens zu sehen ist und nicht auf die abstrakte Zweckbestimmung der Ermächtigungsgrundlage (hier § 75 SGB X) abgestellt werden darf[215], darf dies im Rahmen der wissenschaftlichen Forschung nicht dahingehend missverstanden werden, dass die Verarbeitung durch den Empfänger nunmehr doch von einer konkreten Zweckbestimmung abhängt und der Broad Consent ausgeschlossen ist. Es darf lediglich nicht auf den allgemeinen Zweck der wissenschaftlichen Forschung (oder Planung) abgestellt werden, sondern auf die jeweilige Zweckbestimmung im Einzelnen. Ist der Broad Consent oder eine erweiterte Genehmigung nach § 75 Abs. 4a SGB X Rechtsgrundlage für die Übermittlung, muss auch die Verarbeitung durch den Empfänger in der jeweiligen Breite zulässig sein.

Neben der strengen Zweckbindung schreibt § 78 Abs. 1 S. 3 SGB X vor, dass der Empfänger der Daten die Daten in gleicher Weise wie der Verantwortliche nach § 35 Abs. 1 SGB X geheim zu halten hat. Dies sichert zusätzlich zu der strengen Zweckbindung ab, dass die Daten in einem dem Sozialgeheimnis unterliegenden Bereich verbleiben und nicht unkontrolliert verbreitet werden.

Für nicht-öffentliche Stellen fordert § 78 Abs. 1 S. 2 SGB X, dass diese sich zuvor zu einer ebensolch zweckgebundenen Verarbeitung verpflichtet haben.[216] Zudem muss die nicht-öffentliche Stelle sicherstellen, dass die dort beschäftigten Personen, die die Sozialdaten entsprechend verarbeiten, auf ihre Pflichten nach Absatz 1, sprich die Pflicht zur Geheimhaltung und die strenge Zweckbindung der Verarbeitung, hingewiesen wurden (§ 78 Abs. 2 SGB X).

1.5.4.3 Einwilligung

Grundsätzlich kann die Einwilligung auf Grundlage von Art. 6 Abs. 1 lit. a) DSGVO und Art. 9 Abs. 2 lit. a) DSGVO – mangels Beschränkung der Einwilli-

213 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 78 Rn. 17ff.
214 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 78 Rn. 21.
215 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 78 Rn. 17.
216 An dieser Stelle sei darauf hingewiesen, dass diese Verpflichtung nach dem Entwurf zum 2. DSAnpUG-EU nur dann erforderlich sein soll, wenn die nicht-öffentliche Stelle um die Übermittlung ersucht hat, vgl. BT-Drs. 19/4674, S. 154.

gungsmöglichkeit durch den nationalen Gesetzgeber – auch im Sozialrecht nicht generell ausgeschlossen werden. Eine solche lässt sich auch nicht ohne Weiteres aus § 78 SGB X ablesen. Versteht man den § 78 SGB X jedoch in seiner strengen Zweckbindung eng, schließt dieser die Verwendung der übermittelten Sozialdaten zu Zwecken der Einholung einer Einwilligung aus, wenn dies nicht ausnahmsweise von der Ermächtigungsgrundlage, die der Übermittlung der Daten durch den Leistungsträger zugrunde lag – etwa bei der Einwilligung in Form des Broad Consent – erfasst ist. § 78 SGB X soll eine strenge Zweckbindung des Empfängers herbeiführen und ihn auf die Verarbeitung zu den sich aus der Befugnis der übermittelnden Stelle ergebenden Zwecken ermöglichen. Darüber hinaus soll dem Empfänger eine Verarbeitung nicht möglich sein. Dementsprechend sperrt § 78 SGB X für den Empfänger die Möglichkeit, eine Einwilligung für eine anderweitige Verarbeitung einzuholen. Dies ergibt sich daraus, dass der Empfänger die Daten nicht dazu verwenden darf, mit dem Betroffenen Kontakt aufzunehmen, um eine Einwilligung einzuholen. Dies ist vom Zweck, der die Übermittlung durch den Leistungsträger legitimierte, nicht mehr gedeckt.

1.5.4.4 Auftragsverarbeitung

Ist die externe Stelle selbst Auftragsverarbeiter, ist § 78 SGB X nicht relevant. Die Verarbeitungsbefugnisse richten sich in diesem Zusammenhang streng nach den Weisungen des Verantwortlichen und nach der für diesen bestehenden Verarbeitungsbefugnis. Eine darüberhinausgehende Verarbeitung durch den Auftragsverarbeiter ist weder für eigene noch für fremde Zwecke gestattet. Im Falle einer Unterbeauftragung durch eine als Auftragsverarbeiter agierenden externen Stelle perpetuiert sich die Verantwortlichkeit des ursprünglichen Auftraggebers.

Fraglich ist aber, ob die eigenverantwortliche, externe Stelle selbst befugt ist, einen Auftragsverarbeiter hinzuzuziehen und nach welchen Vorschriften sich die Auftragsverarbeitung dann richtet. Der Empfänger der Daten ist zu einer Verarbeitung entsprechend der Übermittlung der Daten an ihn zugrundeliegenden Zweckbestimmung berechtigt. Da die Weitergabe der Daten an einen Auftragsverarbeiter keinen eigenständigen Verarbeitungsvorgang darstellt, der einer gesonderten Ermächtigungsgrundlage bedarf, sondern vielmehr als Verarbeitung des Verantwortlichen im Rahmen seiner Befugnisse zu verstehen ist, kann eine Weitergabe der Daten an einen Auftragsverarbeiter erfolgen, sofern die Vorgaben des Art. 28 DSGVO sowie des § 80 SGB X eingehalten werden. Letzterer ist vorliegend anwendbar, da der Auftraggeber nach § 78 SGB X verpflichtet ist und damit allen Beschränkungen, die das Sozialgeheimnis mit sich bringt, unterliegt. Dementsprechend richtet sich eine Auftragsverarbeitung, bei der die externe Stelle Auftraggeber ist, ebenfalls nach § 80 SGB X.

1.5.4.5 Anforderungen an „technische und organisatorische Maßnahmen"

Gemäß § 67b Abs. 1 S. 4 SGB X gilt § 22 Abs. 2 BDSG entsprechend. Hierzu kann auf die vorangehenden Ausführungen verwiesen werden.[217]

1.5.4.6 Genehmigungserfordernis und -anforderungen

Im Rahmen von § 75 SGB X besteht ein Genehmigungserfordernis bereits für die Übermittlung an die externe Einrichtung. Die Verarbeitung durch diese bedarf darüber hinaus grundsätzlich keiner gesonderten Genehmigung. Eine Ausnahme kann im Fall der erweiterten Genehmigung nach § 75 Abs. 4a SGB X bestehen, bei der die Daten für einen bestimmten Bereich wissenschaftlicher Forschung genutzt werden sollen. Hier ist der Empfänger der Sozialdaten verpflichtet, die konkreten Vorhaben, zu denen die Daten verarbeitet werden sollen, vor dem Beginn des Vorhabens bei der Behörde, die die Genehmigung erteilt hat, anzuzeigen. Kommt diese Behörde zu dem Schluss, dass die Voraussetzungen nicht erfüllt sind, etwa weil der inhaltliche Zusammenhang fehlt, kann ein erneutes Genehmigungsverfahren nach § 75 Abs. 4 SGB X erforderlich werden.

Hinsichtlich der Auftragsverarbeitung erfordert § 80 Abs. 1 SGB X vorab eine Anzeige gegenüber der zuständigen Rechts- oder Fachaufsichtsbehörde.[218]

1.5.4.7 Ergebnis

Aus § 78 SGB X folgt sowohl die streng verstandene Zweckbindung hinsichtlich einer Verarbeitung der Sozialdaten durch den Empfänger, der wie eine in § 35 SGB I genannte Stelle an das Sozialgeheimnis gebunden ist, als auch die Befugnis zur Verarbeitung zu diesem Zweck. Auf sonstige Erlaubnistatbestände – insbesondere solche des allgemeinen Datenschutzrechts – kann nicht zur Weiterverarbeitung zurückgegriffen werden. Alternativ wäre es zwar möglich, eine Einwilligung nach den Vorgaben der DSGVO einzuholen, allerdings kann die externe Stelle als durch § 78 Abs. 1 SGB X gebundener Empfänger die erhaltenen Daten nicht zum Zweck der Einholung einer solchen Einwilligung verwenden, sodass praktisch kaum ein Anwendungsfall bestehen dürfte.

Eine Auftragsverarbeitung richtet sich in jedem Fall nach den Vorgaben des § 80 SGB X, in dessen Rahmen sie auch zulässig ist.

Die Verarbeitung nach einer Übermittlung ist von der Genehmigung nach § 75 Abs. 4 SGB X umfasst. Im Falle der Auftragsverarbeitung ist eine Anzeige gegenüber der Rechts- oder Fachaufsicht erforderlich.

217 Hierzu siehe Kap. 1.4.4.

218 Siehe hierzu bereits Kap. 1.5.3.4.2; vgl. Rombach, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 80 SGB X Rn. 69.

1.6 Beurteilung von Szenario 3

1.6.1 Darstellung des Szenarios

In diesem Szenario werden Sozialdaten von einer oder mehreren Einrichtungen der gesetzlichen Krankenversicherung zu übergeordneten Zwecken (z.B. medizinische Forschung oder übergeordnete Qualitätssicherungsaspekte) an eine externe Einrichtung (Datenplattform) übermittelt. Die externe Einrichtung wiederum stellt diese Sozialdaten für bestimmte Vorhaben Dritten zur Verfügung, entweder in Form einer weiteren Übermittlung oder indem anonyme Auswertungsergebnisse zu konkreten Fragestellungen herausgegeben werden.

Das Szenario 3 lässt sich somit in zwei Unterszenarios (3A und 3B) unterteilen:

1.6.1.1 Szenario 3A

In der Variante 3A erhält die externe Plattform Sozialdaten von unterschiedlichen Krankenkassen, führt diese zusammen und wertet sie selbst aus. Im Anschluss werden nur die anonymisierten Ergebnisse weitergegeben.

1.6.1.2 Szenario 3B

In Variante 3B erhält die externe Plattform Sozialdaten von den unterschiedlichen Krankenkassen, um diese nicht selbst auszuwerten, sondern mit den Daten der anderen Krankenkassen ggf. zusammenzuführen und zu Auswertungszwecken an eine abermals dritte Stelle zu übermitteln.

1.6.2 Rechtfertigungsbedürftige Datenverarbeitungsvorgänge

Wie auch in den vorangehenden Szenarien weisen wir daraufhin, dass lediglich die Übermittlung und weitere Verarbeitung personenbezogener Daten rechtfertigungsbedürftig ist. Liegen (faktisch) anonyme Daten, jedenfalls aus Sicht der empfangenden und weiterverarbeitenden externen Plattform sowie weiterer Empfänger vor, so sind diese ohne datenschutzrechtliche Restriktionen zulässig.

Vorliegend kommen im Übrigen bei jedem Unterszenario mehrere rechtfertigungsbedürftige Verarbeitungsschritte in Betracht.

1.6.2.1 Szenario 3A

Wie auch bei Szenario 2 ist hier jeweils eine Weitergabe der Daten durch die Krankenkasse an die Plattform erforderlich (s. Kap. 1.6.3.1). Anschließend werden die Daten zum Zweck der Auswertung durch die Plattform genutzt (s. Kap. 1.6.3.2).

1.6.2.2 Szenario 3B

Wie auch in Szenario 3A müssen Sozialdaten von Krankenkassen an die externe Plattform übermittelt werden, nun aber zum Zweck der Weiterübermittlung (s. Kap. 1.6.4.1). Die weitere Verarbeitung erfolgt als Weiterübermittlung der Sozialdaten an abermals Dritte (s. Kap. 1.6.4.2).

1.6.3 Szenario 3A (Weitergabe an und Auswertung durch die externe Plattform)

1.6.3.1 Zulässigkeit der Weitergabe durch den Leistungsträger (hinsichtlich der jeweiligen Zwecke) an die externe Plattform

1.6.3.1.1 Prüfungsmaßstab/Identifikation des einschlägigen Datenschutzregimes

Hinsichtlich der Verarbeitungen durch die Krankenkassen bleibt es bei den in Kapitel 1.4.3.1 beschriebenen Rahmenbedingungen.

1.6.3.1.2 Medizinische Forschung

Gesetzliche Ermächtigung

Hinsichtlich einer Übermittlung von Sozialdaten zu Forschungszwecken, insbesondere zu medizinischen Forschungszwecken, kann im Wesentlichen auf die Ausführungen in Kapitel 1.5.3.2.4 verwiesen werden. Die Tatsache, dass die Daten verschiedener Krankenkassen bei der externen Plattform zusammengeführt werden, ist dann unproblematisch, wenn dieses Vorgehen vom jeweiligen Forschungsvorhaben und somit von der konkreten Zweckbestimmung im Einzelfall umfasst ist und folglich für die Durchführung des Forschungsvorhabens erforderlich ist.

Soll hingegen die externe Plattform Daten auf Vorrat speichern, die später ggf. zu Forschungszwecken verwendet werden könnten, so ist für eine Übermittlung keine Ermächtigungsgrundlage ersichtlich.

Einwilligung

Eine Übermittlung ist auf Grundlage einer Einwilligung zulässig. Hierzu kann auf die Ausführungen in Kapitel 1.5.3.3 verwiesen werden.

Auftragsverarbeitung

Eine Auftragsverarbeitung käme nur unter den in Kapitel 1.5.3.4 beschriebenen Voraussetzungen in Betracht. Zusätzlich ist darauf hinzuweisen, dass über eine Auftragsverarbeitung kein Datenumgang ermöglicht werden kann, der Daten anderer Krankenkassen betrifft. In einem solchen Fall würde der Auftragsverarbeiter, der dem Verantwortlichen zugerechnet werden muss, Daten

über Versicherte anderer Leistungsträger (auch) für den Auftraggeber ggf. erheben, jedenfalls aber speichern. Diese Speicherung wäre nach § 284 Abs. 1 SGB V unzulässig, da sie über die dort konkreten Daten hinausgehen würde. Weiterhin müsste die Weisungsbefugnis der Auftraggeber auch bei kollidierenden Weisungen der unterschiedlichen Auftraggeber wirksam werden können. Beide Anforderungen dürften bei der Arbeit mit Datenbeständen mehrerer Leistungsträger in jeweiliger Weisungsabhängigkeit praktisch nicht durchführbar sein, zumal der notwendige Konkretisierungsgrad der erforderlichen Verarbeitungsschritte regelmäßig nicht erreicht werden dürfte. Bestünden eigene Entscheidungsspielräume der externen Stelle hinsichtlich der Verarbeitungen, so wäre dies als Auftragsverarbeitung ohnehin nicht abbildbar.

1.6.3.1.3 Weitere Zwecke

Für die Übermittlung zu anderen Zwecken sind gemäß § 67b Abs. 1 SGB X entsprechende Übermittlungstatbestände im SGB zu identifizieren. Für die hier beispielhaft genannten übergeordneten Qualitätssicherungsaspekte ist eine solche Norm nicht ersichtlich. Alternativ kommt die Einholung einer Einwilligung nach den Vorgaben der DSGVO in Betracht (s. Kap. 1.4.3.3).

1.6.3.2 Zulässigkeit der Auswertung durch die externe Plattform

Die Auswertungsbefugnisse entsprechen den Darstellungen in Kapitel 1.5.4.

1.6.4 Szenario 3B (Weitergabe an und Weiterübermittlung durch die externe Plattform)

1.6.4.1 Zulässigkeit der Übermittlung durch den Leistungsträger (hinsichtlich der jeweiligen Zwecke)

1.6.4.1.1 Prüfungsmaßstab/Identifikation des einschlägigen Datenschutzregimes

Für eine Weiterübermittlung gilt das für die Verarbeitung durch eine externe Stelle anwendbare Datenschutzrecht, wie in Kapitel 1.5.4.1 dargestellt.

1.6.4.1.2 Medizinische Forschung

Gesetzliche Ermächtigung

Hinsichtlich einer Übermittlung von Sozialdaten zu Forschungszwecken, insbesondere zu medizinischen Forschungszwecken, kann auf die Ausführungen in Kapitel 1.6.3.1.2 verwiesen werden. Die Tatsache, dass die Daten verschiedener Krankenkassen bei der externen Plattform ggf. zusammengeführt werden, und anschließend weiterübermittelt werden sollen, ist dann unproblematisch, wenn dieses Vorgehen vom jeweiligen Forschungsvorhaben und somit von der konkreten Zweckbestimmung im Einzelfall umfasst ist und folglich für die Durchführung des Forschungsvorhabens erforderlich ist.

Auftragsverarbeitung

Entsprechend § 67d Abs. 3 SGB X ist auch eine Übermittlung von Sozialdaten über Vermittlungsstellen im Rahmen einer Auftragsverarbeitung zulässig. Hierbei würde im Ergebnis eine Übermittlung von der Krankenkasse an die weitere dritte Stelle vorliegen, die nur durch die Plattform als Auftragsverarbeiter durchgeführt würde.

Einwilligung

Eine Übermittlung ist auf Grundlage einer Einwilligung zulässig. Hierzu kann auf die Ausführungen in Kapitel 1.5.3.3 verwiesen werden. Die Einwilligung muss sich auch auf die Weiterübermittlung beziehen.

1.6.4.2 Zulässigkeit der Zusammenführung und Weitergabe durch die externe Plattform (hinsichtlich der jeweiligen Zwecke)

Hinsichtlich einer Zusammenführung und Weiterübermittlung kommen dieselben Grundsätze, wie bei der Auswertung zum Tragen, da auch hier die absolute Zweckbindung nach § 78 Abs. 1 SGB X eingreift (s. Kap. 1.5.4). Wenn die vorherige Übermittlung also die Zwecke der Weiterübermittlung umfasst, ergibt sich für den Empfänger auch eine entsprechende Befugnis aus § 78 Abs. 1 S. 1 SGB X. Die Wirkung des § 78 SGB X perpetuiert sich anschließend auch gegenüber der weiteren Dritten.

1.6.5 Anforderungen an „technische und organisatorische Maßnahmen"

Die Anforderungen an technische und organisatorische Maßnahmen entsprechen denen der übermittelnden Stellen nach § 35 Abs. 1 SGB I.

1.6.6 Genehmigungserfordernis und -anforderungen

Hinsichtlich der Genehmigungsanforderungen ergeben sich keine abweichenden Besonderheiten zu den in Kapitel 1.5.4.6 dargestellten Grundsätzen.

1.7 Sozialrechtliche Zulässigkeit der Zusammenführung von Sozialdaten mit weiteren Patientendaten

1.7.1 Ohne Einbindung eines Treuhänders oder einer Vertrauensstelle

Bei der Frage, ob Krankenkassen Sozialdaten mit weiteren Patientendaten zusammenführen dürfen, ist der streng zu verstehende § 284 Abs. 1 SGB V zu beachten. Dieser bestimmt abschließend, zu welchen Zwecken Krankenkassen

Sozialdaten erheben und speichern dürfen. Eine Erhebung zu Forschungszwecken ist hiervon nicht umfasst.

Denkbar wäre allenfalls die Legitimation über die Einholung einer Einwilligung nach der DSGVO. Hinsichtlich – hier maßgeblich in Rede stehender – Gesundheitsdaten besteht nach Art. 9 Abs. 2 lit. a) DSGVO aber die Möglichkeit der Mitgliedsstaaten, die Einwilligung auszuschließen. Es wäre daher möglich, § 284 Abs. 1 SGB V derart zu interpretieren, dass eine abweichende Zweckbestimmung auch durch eine Einwilligung nicht möglich sein soll.

1.7.2 Mit Einbindung eines Treuhänders oder einer Vertrauensstelle

Ohne eine eigenständige rechtliche Grundlage, die die Einbindung weiterer Stellen in der Funktion eines Datentreuhänders oder einer Vertrauensstelle ermöglicht, führt die Einbindung einer solchen Stelle nicht zu einer abweichenden Bewertung. Zwar wäre es sowohl aus grundrechtlicher Perspektive vertretbar, wie auch aus Gründen der Praktikabilität wünschenswert, eine gesonderte Stelle zu involvieren, die in einheitlichen, validierten Verfahren Anonymisierungsprozesse vornimmt und überwacht, sowie die Speicherung der Daten unter besonders hohen Anforderungen der Datensicherheit sicherstellen kann. Allerdings müsste eben diese Stelle – wie auch jede andere Stelle – zur Verarbeitung personenbezogener Daten befugt sein.

1.7.3 Erstreckung der sozialrechtlich begründeten Genehmigung auf die Rechtmäßigkeit der Verwendung weiterer Gesundheitsdaten

Existiert eine sozialrechtliche Genehmigung für die Verarbeitung personenbezogener Daten, etwa nach § 75 Abs. 4 SGB X für die Verarbeitung, umfasst diese grundsätzlich Verarbeitungsvorgänge bezüglich der in der Genehmigung benannten (Sozial-)Daten. Sollen auch andere Gesundheitsdaten – etwa von medizinischen Leistungserbringern (z.B. Ärzte, Krankenhäuser) – verarbeitet werden, richtet sich die Zulässigkeit der Verarbeitung dieser Daten nach den jeweils geltenden Normen und Erlaubnistatbeständen. Die sozialrechtliche Genehmigung kann diese nicht ohne Weiteres erfassen, auch wenn der Sinn und Zweck des Vorhabens eine solche Verarbeitung weiterer Daten voraussetzt. Dafür wäre eine gesonderte gesetzliche Anordnung erforderlich, die eine solche Erstreckungswirkung im Einzelfall vorsieht. Dies geht bereits aus § 67d Abs. 2 SGB X hervor, der regelt, dass überschießende, also für das konkrete Vorhaben nicht benötigte Daten zwar übermittelt, nicht jedoch verarbeitet werden dürfen. Wenn eine solche Beschränkung bereits für Sozialdaten des gleichen Leistungsträgers gilt, kann eine Erstreckung auf andere Bereiche nicht ohne Weiteres möglich sein.

1.8 Löschverpflichtungen in den jeweiligen Szenarien

1.8.1 Verlängerte Aufbewahrung zum Zweck der Nachvollziehbarkeit der Auswertungen

Nach dem Grundsatz der Datenminimierung (Art. 5 lit. c) DSGVO) gilt, dass personenbezogene Daten zu löschen sind, wenn sie nicht mehr für den Zweck, für den sie erhoben oder sonst verarbeitet wurden, benötigt werden. Diesen Grundsatz greift Art. 17 Abs. 1 lit. a) DSGVO auf und statuiert eine entsprechende Löschverpflichtung des Verantwortlichen. Demnach wären die zu Forschungs- und Planungszwecken übermittelten Sozialdaten mit Abschluss des Forschungsvorhabens grundsätzlich zu löschen. Art. 17 Abs. 3 lit. b), c) und d) DSGVO regeln jedoch Ausnahmen von diesem Grundsatz, sofern die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung der öffentlichen Gewalt (lit. b), aus Gründen des öffentlichen Interesses im Bereich der Gesundheit (lit. c) oder für im öffentlichen Interesse liegende Forschungszwecke erforderlich ist. Mit diesen Ausnahmeregelungen korrespondieren die Öffnungsklauseln der Art. 6 Abs. 1 lit. c), e) sowie Art. 9 Abs. 2 lit. h) und i) DSGVO, wodurch die nationalen Gesetzgeber die Möglichkeit erhalten, konkretisierende Vorschriften zu erlassen.[219]

Für den Bereich des nationalen Sozialdatenschutzes bestimmt § 304 Abs. 1 S. 1 SGB V unter Verweis auf § 84 Abs. 2 SGB X a.F., dass Sozialdaten, die bei den Krankenkassen, Kassenärztlichen Vereinigungen und Geschäftsstellen der Prüfungsausschüsse gespeichert sind, zu löschen sind, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die rechtmäßige Erfüllung der Aufgaben der verantwortlichen Stelle nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Darüber hinaus legt § 304 Abs. 1 SGB V Höchstfristen fest, nach denen die genannten Daten in jedem Fall zu löschen sind, sofern sie im Einzelfall mit entsprechender Rechtsgrundlage über den nach § 84 Abs. 2 SGB X bestimmten Zeitraum gespeichert werden. Vor dem Hintergrund der unmittelbaren Regelung durch Art. 17 DSGVO und des daran angepassten § 84 SGB X ergibt sich Änderungsbedarf für § 304 SGB V, dessen Inbezugnahme des § 84 Abs. 2 SGB X a.F. ab dem 25.05.2018 obsolet sein wird.

Für den Bereich der wissenschaftlichen Forschung und Planung enthält § 75 SGB X eine Sondervorschrift für die Aufbewahrung der zu Forschungs- und Planungszwecken i.S.d. § 75 Abs. 1 SGB X an eine externe Einrichtung übermittelten Daten. So besagt § 75 Abs. 4 S. 6 SGB X, dass die zu Forschungs- und Planungszwecken i.S.d. § 75 Abs. 1 SGB X übermittelten und verarbeiteten Daten bis zu 10 Jahre über den Zeitpunkt, den die Genehmigungsbehörde für die zulässige Verarbeitung nach § 75 Abs. 4 S. 5 Nr. 4 SGB X festgelegt hat, hi-

219 *Herbst*, in: Kühling/Buchner, DS-GVO, 2017, Art. 17 Rn. 74, 79.

naus gespeichert werden dürfen, um eine Nachprüfung der Forschungsergebnisse sowie eine weitere Verarbeitung für Forschungsfolgefragen nach § 75 Abs. 2 SGB X zu ermöglichen.

Es obliegt der Genehmigungsbehörde, durch Auflagen zu bestimmen, wie lang und bei welcher Stelle (übermittelnde oder empfangende Stelle) die Daten gespeichert werden können.[220] Zudem kann sie weitere Auflagen für die verlängerte Speicherung erteilen. Eine längere Verarbeitung im Sinne der bloßen Aufbewahrung ist hierüber gerechtfertigt. Die Verarbeitung im Rahmen der konkreten Nachprüfung oder weiteren Forschungsfrage wird sich in aller Regel auf dieselben Rechtmäßigkeitstatbestände stützen können wie das ursprüngliche Forschungsvorhaben und bedürfte ggf. einer eigenen Genehmigung. Kommt es nicht zu einer Nachprüfung oder Forschungsfolgefrage, wären die Daten zu löschen. Werden sie hingegen zu weiteren Forschungsfragen herangezogen, spricht viel dafür, die Daten auch zur Nachprüfung der dadurch erreichten Forschungsergebnisse erneut 10 Jahre aufbewahren zu können.

Ohne eine entsprechende Genehmigung oder nach Ablauf der in der Genehmigung festgelegten Frist, sind die zu Forschungszwecken übermittelten Daten zu löschen, sofern sie für das konkrete Forschungsvorhaben oder eine bereits bestehende Folgefrage nach § 75 Abs. 2 SGB X nicht mehr erforderlich sind.

§ 84 SGB X regelt zudem Einschränkungen der Löschverpflichtungen. Gemäß § 84 Abs. 1 SGB X kann bei einer nicht-automatisierten Verarbeitung von einer Löschung abgesehen werden, wenn die Löschung auf Grund der Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich, das Interesse des Betroffenen an der Löschung gering ist und die Verarbeitung rechtmäßig war. Stattdessen ist die Verarbeitung dieser Daten gemäß Art. 18 DSGVO einzuschränken und somit die Daten für eine weitere Verarbeitung zu sperren. Eine Sperrung der Daten ist nach § 84 Abs. 4 SGB X auch erforderlich, sofern der Löschung nach dem Wegfall des Zwecks satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

Somit bleibt für **Szenario 1** festzuhalten, dass die Krankenkassen die bei ihnen gespeicherten Sozialdaten (bisher) gemäß § 304 Abs. 1 SGB V a.F. bzw. (zukünftig) gemäß Art. 17 DSGVO i.V.m. § 84 SGB X (ggf. i.V.m. einem neuen § 304 SGB V) unverzüglich zu löschen haben, wenn diese Daten nicht mehr für die Erfüllung der ihnen übertragenen Aufgaben erforderlich sind. Dürfen die Daten auf Grund einer Rechtsvorschrift länger aufbewahrt werden, sind die Daten spätestens mit Ablauf der Höchstfrist zu löschen. Es spräche im Fall des unveränderten Fortbestehens des geltenden § 304 SGB V viel dafür, dem jüngeren Recht **des es neuen § 75 SGB V** Vorrang zu gewähren und im Falle der Verarbeitung von Sozialdaten zu Forschungszwecken die Höchstfristen des § 304 SGB V nicht anzuwenden.

220 BT-Drs. 18/12611, S. 119.

Für die **Szenarien 2 und 3** bestimmt § 75 Abs. 4 S. 6 SGB X darüber hinaus, dass die zu Forschungs- und Planungszwecken entsprechend der Festlegungen der Genehmigungsbehörde über den für das Forschungsvorhaben selbst festgelegten Zeitpunkt hinaus 10 Jahre aufbewahrt werden können, um zum Zwecke der Nachprüfung der Forschungsergebnisse sowie der Bearbeitung von Forschungsfolgefragen verarbeitet werden zu können.

1.8.2 Anwendbarkeit des § 304 SGB V auf eine externe Einrichtung

Auch die externe Einrichtung hat die Daten gemäß Art. 17 DSGVO grundsätzlich zu löschen, sobald deren Verarbeitung für den jeweiligen Zweck nicht mehr erforderlich ist. Sofern die externe Stelle die Daten gemäß § 75 SGB X von einem Leistungsträger erhalten hat, kommt eine weitergehende Aufbewahrung der Daten zum Zwecke der Nachprüfung der Forschungsergebnisse sowie der Bearbeitung von Forschungsfolgefragen in Betracht, soweit und solange die gemäß § 75 Abs. 4 SGB X zuständige Behörde die Aufbewahrung durch die externe Stelle genehmigt hat.

Eine Übertragung der allgemeinen Aufbewahrungsfristen nach § 304 SGB V ergibt sich in diesem Zusammenhang jedoch nicht. Zwar ist die externe Stelle gemäß § 78 Abs. 1 S. 3 SGB X gleichermaßen zur Geheimhaltung nach § 35 SGB I wie der verantwortliche Leistungsträger verpflichtet. Daraus folgt jedoch nicht, dass alle für diese geltenden Regelungen gleichermaßen auf die externe Stelle zu übertragen sind. § 304 SGB V sichert die begrenzte Speicherung von Sozialdaten durch die Krankenkassen ab. Die Kassen sollen lediglich die Daten aufbewahren dürfen, die sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen. Alle anderen Daten sind nach der Zweckerreichung zu löschen. In diesem Sinn ist es nicht erforderlich, auch eine externe Stelle den Vorgaben des § 304 SGB V zu unterwerfen. Vielmehr ist die externe Stelle gemäß Art. 17 Abs. 1 DSGVO i.V.m. § 84 SGB X verpflichtet, die ihr übermittelten Daten nach der Erreichung des Zwecks zu löschen, sofern nicht eine gesetzliche Vorschrift – etwa § 75 Abs. 4 S. 6 SGB X – eine längere Aufbewahrung für zulässig erklärt.

1.8.3 Erfüllung der Löschverpflichtung durch Anonymisierung

Das deutsche Datenschutzrecht definierte bisher das Löschen als das „Unkenntlichmachen gespeicherter personenbezogener Daten“ (vgl. § 3 Abs. 4 Nr. 5 BDSG a.F., § 67 Abs. 4 S. 2 Nr. 5 SGB X a.F.). Hierzu war anerkannt, dass eine Löschung durch eine physische Vernichtung oder auch durch sicheres Überschreiben erfolgen kann.[221] Mit der Löschung der Daten entfällt die Anwendbarkeit des Datenschutzrechts. Die gleiche Wirkung kann mit einer An-

221 BeckOK DatenSR/*Brink*, 20. Ed. 1.2.2017, BDSG § 35 Rn. 26, beck-online.

onymisierung erreicht werden.[222] Es stellt sich daher die Frage, ob ein Löschanspruch gleichermaßen mit einer Anonymisierung von Daten erfüllt werden kann. Die Anonymisierung hätte den großen Vorteil für den Verantwortlichen, dass die nach erfolgreicher Anonymisierung verbleibenden (nicht mehr personenbezogenen) Einzelangaben, beispielsweise zum Zweck statistischer Auswertungen, weiterverwendet werden könnten. Ihnen kommt somit unter Umständen weiterhin ein erheblicher Wert zu, der bei einer vollständigen Löschung verloren gehen würde. Gleichzeitig endet aber auch die Betroffenheit der informationellen Selbstbestimmung mit Entfall des Personenbezugs.

Bereits nach alter Rechtslage war daher wohl anerkannt, dass auch die Anonymisierung von Daten eine Form der Löschung darstellen kann.[223] Dies ergibt sich nicht unmittelbar aus dem Wortlaut des Gesetzes, doch Sinn und Zweck der Vorschrift sprechen dafür, da eine Anonymisierung die vollständige Aufhebung des Personenbezugs darstellt.[224] Die herrschende Meinung ging davon aus, dass der Betroffene nach § 35 BDSG a.F. statt der Löschung erst recht eine Anonymisierung oder Pseudonymisierung verlangen konnte.[225] Technisch muss insgesamt ein Datenbestand geschaffen werden, der die personenbezogenen Daten nicht mehr enthält.[226] Eine getrennte Speicherung reicht nicht aus.[227]

Die DSGVO enthält keine Legaldefinition der Löschung. Neben dem Begriff der Löschung nennt die DSGVO aber auch den der Vernichtung als Unterfall der Verarbeitung der ebenfalls in Art. 4 Nr. 2 DSGVO. Aus dieser Unterscheidung lässt sich ableiten, dass eine Löschung nicht zwingend eine Vernichtung voraussetzt.[228] Es sind jedoch keine Anhaltspunkte ersichtlich, aus denen sich eine von vom bisherigen Verständnis abweichende Definition ergeben könnte. Hinsichtlich der Mittel und Verfahren der Löschung steht dem verantwortlichen ein Auswahlermessen zu.[229] Die Wirkung der Anonymisierung, wird, wie oben dargestellt, unverändert auch unter DSGVO gelten. Daher kann sie nach hier vertretener Ansicht auch zukünftig ein geeignetes Mittel sein, um einen Löschanspruch zu erfüllen. Art. 17 Abs. 2 DSGVO enthält im Rahmen des „Rechts auf Vergessenwerden" den Hinweis, dass alle „Kopien oder Replikationen" von einem Löschungsersuchen umfasst sind. Daher gilt auch weiterhin, dass alle Kopien zu löschen oder zu anonymisieren sind. Das folgt auch unmittelbar aus den Erwägungen zur Wirksamkeit der Anonymisierung.[230]

222 Siehe hierzu die Ausführungen im Gutachtenteil von Roßnagel im vorliegenden Band.
223 BeckOK DatenSR/*Brink*, 20. Ed. 1.2.2017, BDSG § 35 Rn. 26, beck-online; Dix, in: Simitis, BDSG, 8. Aufl., 2014, § 35 Rn. 45, *Plath/Schreiber*, in: Plath, BDSG/DSGVO, 2. Aufl., 2016, § 3 BDSG Rn. 52.
224 *Dix*, in: Simitis, BDSG, 8. Aufl., 2014, § 35 Rn. 45.
225 *Meents/Hinzpeter*, in: Taeger/Gabel, BDSG, 2. Aufl., 2013, § 35 Rn. 17; Dix, in: Simitis, BDSG, 8. Aufl., 2014, § 35 Rn. 45.
226 BeckOK DatenSR/*Schild* BDSG, 20. Ed. 1.5.2017, § 3 Rn. 98, beck-online.
227 *Greve*, in: Auerhammer, DSGVO/BDSG, 5. Aufl., 2017, § 40 BDSG Rn. 14.
228 *Kamann/Braun*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 17 Rn. 32 (m.w.N.).
229 *Kamann/Braun*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 17 Rn. 36.
230 Vgl. *Klabunde*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 4 Rn. 16.

Aus der deutschen Anpassungsgesetzgebung ergibt sich keine abweichende Erwägung.

Nach hier vertretender Auffassung kommt eine Anonymisierung, bei der alle Kopien der Datensätze ebenfalls anonymisiert werden, daher einer Löschung gleich.

1.9 Verpflichtung externer Einrichtungen zur Übermittlung von Sozialdaten an weitere Sozialleistungsträger (§§ 18–29 SGB I)

Sofern die Übermittlung von Sozialdaten an eine externe Stelle nach den oben dargelegten Grundsätzen zulässig ist, ist die Verarbeitung dieser Daten durch die externe Stelle durch den Zweckbindungsgrundsatz streng limitiert (vgl. § 78 Abs. 1 SGB X). Eine Datenverarbeitung der externen Stelle, zu der auch die Datenübermittlung gehört, darf nur erfolgen, sofern sie von dem Zweck gedeckt ist, zu dem ihr die Daten übermittelt wurden. Eine Übermittlung an andere Sozialleistungsträger ist mithin nur zulässig, wenn sich die Übermittlung im Rahmen des Zweckes bewegt, zu dem die Daten der externen Stelle übertragen wurden oder wenn eine anderweitige gesetzliche Ermächtigungsgrundlage für die Übermittlung existiert. Eine grundsätzliche Verpflichtung, erhaltene Sozialdaten an andere Sozialleistungsträger zu übermitteln, auch wenn diese die Daten für die ihnen zugewiesenen Zwecke verarbeiten, existiert nicht.

Sofern für die übermittelnde Stelle eine Verpflichtung besteht, Sozialdaten an bestimmte andere Leistungsträger zu übermitteln, gehen diese Übermittlungspflichten des Leistungserbringers nicht ohne Weiteres mit der Datenübermittlung auf die externe Stelle über. Vielmehr verbleibt die Pflicht beim Leistungsträger. Begehrt ein anderer Sozialleistungsträger personenbezogene Sozialdaten, muss er sich, sofern er nicht ohnehin zur Erhebung der Daten beim Betroffenen selbst verpflichtet ist (§ 67a Abs. 2 S. 1 SGB X), an den Leistungsträger wenden, der entsprechend der gesetzlichen Vorschriften zur Übermittlung der begehrten Daten verpflichtet ist. Nur sofern im Einzelfall eine gesetzliche Vorschrift existiert, die – neben dem Übergang des Sozialgeheimnisses (z.B. § 78 Abs. 1 S. 3 SGB X) – den Übergang der Übermittlungspflichten anordnet, kann der Empfänger zur Übermittlung der erhaltenen Sozialdaten verpflichtet sein.

Auch § 69 SGB X statuiert keine Übermittlungsverpflichtung für die externen Stellen. § 69 SGB X berechtigt lediglich die in § 35 Abs. 1 SGB I genannten sowie die ihnen nach § 69 Abs. 2 SGB X gleichgestellten Stellen zur Übermittlung von Sozialdaten. Diese Übermittlungsbefugnis kann sich allenfalls zu einer Übermittlungspflicht verdichten, wenn diese Stelle zur Amtshilfe verpflichtet ist oder die Übermittlung selbst zu ihren gesetzlichen Aufgaben gehört.[231] Exter-

231 *Rombach*, in: Hauck/Noftz, SGB X, Stand: 08/2017, § 69 Rn. 79.

ne Stellen, die keine in § 35 Abs. 1 SGB I genannte oder dieser gleichgestellten Stelle sind, können folglich keiner Übermittlungspflicht nach § 69 SGB X unterliegen. Handelt es sich bei der empfangenden Stelle um eine in § 35 Abs. 1 SGB I genannte oder diesen gleichgestellte Stelle, ist zu bedenken, dass der andere Sozialleistungsträger grundsätzlich verpflichtet ist, die Daten bei der Stelle anzufragen, die die Daten ursprünglich an die externe Stelle übermittelt hat (Direkterhebung gemäß § 67a Abs. 2 S. 1 SGB X). Nur soweit der Übergang einer solchen Verpflichtung auf den Empfänger der Sozialdaten vom Gesetz ausdrücklich angeordnet wird oder die Daten vom Verantwortlichen nicht mehr übermittelt werden können, kommt eine Pflicht zur Übermittlung durch die externe Stelle in Betracht.

Handelt es sich bei der externen Stelle um einen Auftragsverarbeiter ist die Verarbeitungsbefugnis durch den Auftrag und die Weisungen des Verantwortlichen sowie dessen Verarbeitungsbefugnisse begrenzt. Dementsprechend kann sich für die externe Stelle eine Übermittlungspflicht ergeben, sofern der Verantwortliche selbst zur Übermittlung verpflichtet ist und der Auftrag etwa die Speicherung und Übermittlung dieser Daten umfasst. Betrifft der Auftrag jedoch andere Tätigkeiten, schließt dies die Übermittlung durch den Auftragsverarbeiter jedoch aus. Zudem unterliegt der Auftragsverarbeiter den Weisungen des Verantwortlichen. Folglich ist eine eigenmächtige Übermittlung der Daten durch den Auftragsverarbeiter in jedem Fall unzulässig. Vielmehr bedarf es einer entsprechenden Weisung durch den Auftraggeber.

1.10 Auskunftsrechte der Versicherten

Das Auskunftsrecht des Betroffenen ist in Art. 15 DSGVO geregelt. § 34 BDSG und § 83 SGB X erhalten dazu ergänzende Regelungen, die den Anspruch im Wesentlichen einschränken und weitere Voraussetzungen formulieren.[232] Da es sich bei den von der Krankenkasse erhobenen Daten um Sozialdaten im Sinne des § 67 Abs. 2 SGB X handelt, werden gemäß § 35 Abs. 2 SGB I die allgemeinen datenschutzrechtlichen Anforderungen des § 34 BDSG von den spezielleren sozialrechtlichen Bestimmungen des § 83 SGB X verdrängt.

Ob dies auch im Falle der Übermittlung der Daten an die externe Stelle gilt (insbesondere in **Szenario 3**), ergibt sich nicht eindeutig aus dem Gesetz. Es spricht aber viel dafür, dass sich der Auskunftsanspruch gegenüber einer externen Stelle, gegenüber der sich das Sozialgeheimnis nach § 78 Abs. 1 SGB X verlängert, nach den gleichen Anforderungen richtet, wie dies gegenüber einer Stelle nach § 35 Abs. 1 SGB X der Fall wäre. Dies ergäbe sich im Übrigen auch aus § 35 Abs. 6 S. 1 Nr. 1 SGB I, sofern man diese Regelung nicht unter Berücksichtigung des § 78 Abs. 1 SGB X restriktiv auslegen würde.

232 Vgl. bisher: § 34 BDSG a.F. und § 83 SGB X a.F.

1.10.1 Auskunftsanspruch gegen die gesetzliche Krankenkasse

Der Auskunftsanspruch besteht gegenüber dem Verantwortlichen. Dies ist gemäß Art. 4 Nr. 7 DSGVO diejenige natürliche oder juristische Person, die die Entscheidungsgewalt über die personenbezogenen Daten hat. In allen drei Szenarien handelt es sich dabei um die gesetzliche Krankenkasse. Diese erhebt die Sozialdaten beim Betroffenen und übermittelt sie ggf. an eine externe Stelle.

1.10.1.1 Voraussetzungen des Auskunftsanspruchs

Art. 15 DSGVO enthält keine besonderen Anforderungen für die Geltendmachung des Auskunftsanspruchs. Der Versicherte kann seinen Antrag daher formlos, ggf. sogar mündlich stellen. Er hat jedoch seine Identität nachzuweisen, vgl. Art. 12 Abs. 1 und 2 DSGVO. Bei Zweifeln hinsichtlich der Identität kann die verantwortliche Stelle zusätzliche Informationen verlangen (Art. 12 Abs. 6 DSGVO). Gemäß § 83 Abs. 2 S. 1 SGB X soll der Betroffene in seinem Antrag die Art der Sozialdaten, über die er Auskunft begehrt, näher bezeichnen. Pauschale Auskunftsersuchen können daher von der Krankenkasse mit der Bitte um Spezifizierung zurückgewiesen werden.

1.10.1.2 Umfang des Auskunftsanspruchs

Gemäß Art. 15 DSGVO hat der Betroffene gegenüber dem Verantwortlichen Anspruch auf Auskunft darüber, ob und in welchem Umfang personenbezogene Daten von ihm verarbeitet werden. Aus Erw.Gr. 63 der Verordnung ergibt sich, dass sich der Auskunftsanspruch auch auf eigene gesundheitsbezogene Daten (beispielsweise Daten in Patientenakten, Untersuchungsergebnisse oder Befunde) bezieht.

Er kann im Einzelnen Auskunft verlangen über (vgl. Art. 15 Abs. 1, Abs. 2 DSGVO):

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten, die verarbeitet werden
- 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
- 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[233]
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde[234]

233 Vgl. Art. 16 und 17 DS-GVO.
234 Vgl. § 81 Abs. 1 SGB X.

- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden[235], alle verfügbaren Informationen über die Herkunft der Daten
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich des Profilings gemäß Artikel 22 Absätze 1 und 4 DSGVO 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
- die geeigneten Garantien gemäß Artikel 46 DSGVO im Falle der Übermittlung der Daten an ein Drittland oder an eine internationale Organisation.
- 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.
  Gemäß § 83 Abs. 1 Nr. 1 i.V.m. § 82a Abs. 4 i.V.m. § 82 Abs. 1 SGB X sind hier nur diejenigen Empfänger zu nennen, an die eine Weiterleitung aus Sicht des Betroffenen nicht zu erwarten ist, die nicht zu den in § 35 SGB I genannten Personen oder Stellen gehören oder eng mit diesen zusammenarbeiten.
  Zu nennen sind dagegen in **Szenario 2 und 3** die externe Stelle, in **Szenario 3** ggf. weitere Dritte. Die Drittempfänger sollten dabei soweit wie möglich präzisiert werden. Bei der Benennung von Empfängerkategorien reichen die üblichen Branchenbezeichnungen aus.[236]

1.10.1.3 Verfahren und Form

Art. 12 DSGVO enthält verschiedene Anforderungen an die Auskunftserteilung. Sie muss in präziser, transparenter und leicht zugänglicher Form erteilt und in klarer und einfacher Sprache verfasst werden (Art. 12 Abs. 1 DSGVO). In der Regel ist die Auskunft schriftlich oder elektronisch zu übermitteln, kann aber auf Verlangen des Versicherten auch mündlich erfolgen. Einzelheiten zum Verfahren, insbesondere zur Form der Auskunft, kann die Krankenkasse bestimmen (§ 83 Abs. 2 S. 3 SGB X). Soweit die Daten Angaben zu gesundheitlichen Verhältnissen des Betroffenen enthalten, kann sie die Auskunft gemäß § 83 Abs. 2 S. 4 i.V.m. § 25 Abs. 2 SGB X durch einen Arzt erteilen lassen.

Art. 12 Abs. 3 DSGVO sieht für die Erteilung der Auskunft eine Frist von einem Monat vor. Diese Frist kann um maximal zwei Monate verlängert werden. Auch darüber – sowie über die Gründe einer solchen Fristverlängerung – ist der Betroffene in Kenntnis zu setzen.

235 Z.B. bei einer Übermittlung durch Krankenhäuser gemäß § 301 SGB V.
236 Zu § 34 BDSG a.F.: *Kamlah*, in: Plath, BDSG/DSGVO, 2013, § 34 Rn. 24.

Gemäß Art. 15 Abs. 3 DSGVO muss die Krankenkasse dem Betroffenen eine Kopie der verarbeiteten personenbezogenen Daten zur Verfügung stellen (im Falle der elektronischen Übermittlung kann dies z.B. im PDF-Format erfolgen). Diese Kopie sowie die Auskunftserteilung selbst erfolgt unentgeltlich. Nur für weitere Kopien kann die Krankenkasse ein angemessenes Entgelt verlangen.

1.10.1.4 Ausschluss des Anspruchs

Gemäß § 83 Abs. 1 Nr. 1 SGB X besteht kein Auskunftsanspruch, wenn der Betroffene gemäß § 82a SGB X nicht zu informieren ist, die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische oder organisatorische Maßnahmen ausgeschlossen ist. Dies ist gemäß § 82a Abs. 1 SGB X insbesondere dann der Fall, wenn die ordnungsgemäße Erfüllung der Aufgaben des Verantwortlichen oder die öffentliche Sicherheit und Ordnung gefährdet wäre oder wenn die Daten ihrem Wesen nach oder aufgrund einer gesetzlichen Regelung geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Erteilung der Auskunft zurücktreten muss. Damit werden die Bestimmungen des bisherigen § 83 Abs. 2 und Abs. 4 SGB X a.F. beibehalten.[237] Die Beschränkung des Auskunftsanspruchs soll die verantwortliche Stelle insbesondere vor einer übermäßigen Inanspruchnahme schützen.[238] Ein vollständiger Ausschluss des Auskunftsanspruchs dürfte jedoch nur im Ausnahmefall möglich sein. Das Auskunftsersuchen kann beispielsweise nicht bei bloßer Arbeitsüberlastung abgelehnt werden.[239] Stattdessen kann der Verantwortliche verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.[240]

Die Auskunft kann ferner verweigert werden, wenn die Sozialdaten nur noch gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen (§ 83 Abs. 1 Nr. 2 lit. a SGB X) oder wenn sie nur der Datensicherung oder -kontrolle dienen (§ 83 Abs. 1 Nr. 2 lit. b SGB X), und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische oder organisatorische Maßnahmen ausgeschlossen ist. Bei den archivierten[241] oder zu Kontroll- und Sicherheitszwecken gespeicherten[242] Daten ist dabei zu beachten, dass der Verantwortliche ggf. technische Maßnahmen ergreifen muss, um die Daten verfügbar zu machen.[243]

237 BT-Drucks. 18/12611, S. 129.
238 BT-Drucks. 18/12611, S. 130.
239 *Diering/Seidel*, in: Diering/Timme, SGB X, 4. Aufl., 2016, § 83 Rn. 7.
240 Vgl. Erw.Gr. Nr. 63 S. 7, siehe auch § 83 Abs. 2 S. 1 SGB X.
241 Vgl. § 84 Abs. 3 SGB X.
242 Vgl. § 67c Abs. 4 SGB X.
243 BT-Drucks. 18/12611, S. 130.

Bei nicht automatisiert oder in nicht automatisierten Dateisystemen gespeicherten Daten muss die Auskunft gemäß § 83 Abs. 2 S. 2 SGB X ferner nur dann erteilt werden, wenn der Betroffene Angaben macht, die ein Auffinden der Daten ermöglichen und die Erteilung der Auskunft keinen unverhältnismäßigen Aufwand erfordert.[244] Hierfür reicht die Mitteilung des jeweiligen Aktenzeichens aus.[245]

Abgesehen davon kann die verantwortliche Stelle gemäß Art. 12 Abs. 5 DSGVO die Auskunft verweigern, wenn entsprechende Anträge offenkundig unbegründet sind oder exzessiv gestellt werden. Der Antrag ist „offenkundig unbegründet", wenn seine Voraussetzungen offensichtlich nicht erfüllt sind, z.B. wenn der Anspruch nicht von dem Betroffenen selbst geltend gemacht wird.[246] Eine „exzessive" Antragstellung dürfte nur selten vorliegen. Dem Erw. Gr. 63 S. 1 lässt sich entnehmen, dass der Auskunftsanspruch in „angemessenen Abständen" geltend gemacht werden kann. Wann eine exzessive Antragstellung vorliegt, ist eine Frage des Einzelfalls. Es sollte dem Betroffenen jedoch möglich sein, das Auskunftsrecht mehrmals pro Jahr geltend zu machen.

Von den genannten Verweigerungsrechten kann die Krankenkasse sowohl bei Datenerhebungen aufgrund einer gesetzlichen Ermächtigung als auch bei solchen auf Grundlage von Einwilligungen Gebrauch machen. Gemäß § 83 Abs. 3 S. 1 SGB X hat sie die Gründe für die Auskunftsverweigerung zu dokumentieren, es sei denn, der mit der Auskunftsverweigerung verfolgte Zweck würde dadurch gefährdet werden (z.B. wenn die Dokumentation in Rechte Dritter eingreifen würde).

1.10.2 Auskunftsanspruch gegen die externe Stelle

1.10.2.1 Auftragsverarbeiter

Ist die externe Stelle nur „Auftragsverarbeiter" im Sinne des Art. 4 Nr. 8 DSGVO, haben die Versicherten ihr gegenüber keinen Auskunftsanspruch aus Art. 15 DSGVO. Gemäß Art. 28 Abs. 3 lit. d) DSGVO ist der Auftragsverarbeiter jedoch verpflichtet, den Verantwortlichen bei der Erteilung der Auskunft zu unterstützen. Adressiert der Betroffene beispielsweise seinen Antrag versehentlich an die externe Stelle, so sollte ihn diese an die zuständige Krankenkasse weiterleiten.

1.10.2.2 Externe Stelle als Verantwortlicher

Erhält die externe Stelle die Sozialdaten im Rahmen einer Übermittlung dergestalt, dass sie eigenständig Verantwortlicher ist, besteht hier zusätzlich zu

244 Vgl. § 83 Abs. 1 S. 3 SGB X a.F.
245 *Diering/Seidel*, in: Diering/Timme, SGB X, 4. Aufl., 2016, § 83 Rn. 4.
246 *Heckmann/Paschke*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 12 Rn. 43.

dem Auskunftsanspruch gegenüber der gesetzlichen Krankenkasse auch ein Anspruch gegenüber der externen Stelle.

Für diesen Auskunftsanspruch gilt – sofern man, wie oben ausgeführt, von einer Anwendbarkeit der § 67ff. SGB X ausgeht – dasselbe wie für den Auskunftsanspruch gegenüber der gesetzlichen Krankenkasse. Insofern kann vollumfänglich auf die obigen Ausführungen verwiesen werden.

Geht man hingegen davon aus, dass für den Auskunftsanspruch gegenüber der externen Stelle nur die allgemeinen datenschutzrechtlichen Anforderungen gelten, ergibt sich Folgendes:

- Die Einschränkung der § 83 Abs. 2 S. 1 entfällt. Die externe Stelle kann das Auskunftsersuchen daher nicht allein deswegen zurückweisen, weil es zu pauschal formuliert wurde. Die Auskunft kann jedoch gemäß § 34 Abs. 4 BDSG – entsprechend § 83 Abs. 2 S. 2 SGB X – verweigert werden, wenn Angaben, die ein Auffinden der Daten ermöglichen, fehlen.
- Die Ausschlussgründe des § 83 Abs. 1 SGB X entfallen, jedoch ergeben sich aus § 34 Abs. 1 BDSG entsprechende Verweigerungsrechte.
- Werden personenbezogene Daten ohne Einwilligung des Betroffenen für Forschungszwecke oder statistische Zwecke gemäß § 27 Abs. 1 BDSG erhoben, kann der Auskunftsanspruch zudem gemäß § 27 Abs. 2 BDSG ausgeschlossen oder beschränkt werden. Dies ist der Fall, wenn andernfalls die Verwirklichung von Statistik- und Forschungszwecken unmöglich gemacht oder ernsthaft beeinträchtigt werden würde und der Ausschluss für die Erfüllung dieser Zwecke erforderlich ist. Die Verwirklichung des Forschungszwecks ist z.B. ernsthaft beeinträchtigt, wenn die zuständige Ethikkommission zum Schutz der betroffenen Person eine Durchführung des Projekts untersagen würde.[247]
- Der Auskunftsanspruch kann darüber hinaus ausgeschlossen werden, wenn die Daten für wissenschaftliche Forschungszwecke erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Dies kommt bereits dann in Betracht, wenn ein Forschungsvorhaben mit besonders großen Datenmengen arbeitet.[248] Allerdings wird ein vollständiger Ausschluss des Auskunftsanspruchs auch hier wohl nur ausnahmsweise möglich sein. Analog zu den obigen Ausführungen kann der Aufwand der Auskunftserteilung beispielsweise dadurch verringert werden, dass der Betroffene sein Auskunftsersuchen auf bestimmte Informationen oder Verarbeitungsvorgänge beschränkt.[249]
- Außerdem kann die externe Stelle gemäß Art. 12 Abs. 5 DSGVO die Erteilung der Auskunft wegen offenkundiger Unbegründetheit oder exzessiver Antragsstellung verweigern.

247 BT-Drucks. 18/11325, S. 99.
248 BT-Drucks. 18/11325, S. 99f.
249 Vgl. Erw.Gr. Nr. 63 S. 7.

- Die Gründe für die Auskunftsverweigerung sind auch hier zu dokumentieren und dem Betroffenen mitzuteilen (§ 34 Abs. 2 BDSG).
- Ansonsten ergeben sich für den Auskunftsanspruch des Versicherten nach allgemeinem Datenschutzrecht keine Besonderheiten. Es gelten die obigen Ausführungen.

2 Vergleich zur bisherigen Rechtslage

Eine umfassende Erläuterung des bisher geltenden Rechts ist wegen der gewählten Darstellungsform, bereits in Kapitel I die wesentlichen Änderungen mitunter vergleichend zu beschreiben, nicht mehr angezeigt, geschweige denn in Anbetracht der zwischenzeitlich geänderten Rechtslage von besonderer Relevanz. Nichtsdestotrotz soll an dieser Stelle auf einige Unterschiede hingewiesen werden. Diese Unterschiede fallen jedoch überaus gering aus, was insbesondere daran liegt, dass die fachspezifischen Normen des SGB V bei dem hier zugrunde zu legenden Gesetzgebungsstand noch nicht an die DSGVO angepasst wurden.

2.1 Allgemeines

Hinsichtlich der allgemeinen Regelungsstrukturen wurde bereits in Kapitel I auf die Systematik der alten Rechtslage hingewiesen. Sie unterscheidet sich insoweit, als keine unmittelbare Geltung des EU-Sekundärrechts zu beachten war. Allgemeines Datenschutzgesetz auf Bundesebene war das BDSG a.F., dem das Sozialdatenschutzrecht nach SGB I a.F. und SGB X a.F. i.V.m. SGB V gemäß § 1 Abs. 3 S. 1 BDSG a.F. vorging. Wegen des abschließenden Charakters des Sozialdatenschutzrechts war ein Rückgriff auf allgemeines Datenschutzrecht des Bundes nicht angezeigt. Das Sozialgeheimnis galt nur für Stellen nach § 35 SGB I. Allerdings enthielt bereits das bisher geltende Recht die strenge

Zweckbindung des § 78 Abs. 1 SGB X a.F. und die Pflicht zur Geheimhaltung wie eine Stelle nach § 35 SGB I a.F. gemäß § 78 Abs. 1 S. 2 SGB X a.F. Gleiches gilt für die „Verlängerung der ärztlichen Schweigepflicht", die in § 76 Abs. 1 SGB X a.F. geregelt war.

Nicht enthalten war bisher die Möglichkeit, Forschungsfolgefragen zum Anlass zu nehmen, ein Forschungsvorhaben zu verlängern oder Forschungsvorhaben bereits zu einem Zeitpunkt genehmigen zu lassen, zu dem eine konkrete inhaltliche Bestimmung der jeweiligen Forschungsfrage noch nicht möglich ist. Die Anforderungen an eine Einwilligung ergaben sich bisher unmittelbar aus dem SGB X a.F. Dabei ließ § 67a Abs. 1 SGB X a.F. eine Einwilligung für Datenerhebungen (sowohl bei einfachen Sozialdaten als auch bei besonderen Arten personenbezogener Daten i.S.d. § 67 Abs. 12 SGB X a.F.) nicht zu.[250] Nur für die Verarbeitung und Nutzung sah § 67b SGB X a.F. die Einwilligung als taugliche Alternative zur gesetzlichen Ermächtigungsgrundlage an. Das spiegelte sich auch in § 284 Abs. 1 SGB V wider. Über die Verweisung des § 284 Abs. 3 S. 1 Hs. 2 SGB V konnte diese Einschränkung zur Einholung einer Einwilligungserklärung bislang also nicht umgangen werden, da auch diese Verweisung eine Einwilligung zur Erhebung nicht ermöglichte. Inhaltlich war die Einwilligung bisher unter Zugrundelegung eines strengen Zweckbindungsverständnisses eng ausgelegt worden. Erwägungen im Sinne einer breiten Einwilligung fanden sich weder im Gesetz noch in den Gesetzgebungsunterlagen. Die Einwilligung musste in Schriftform erteilt werden und bei besonderen Arten personenbezogener Daten zudem ausdrücklich auf diese Bezug nehmen. Nur beim Eingreifen besonderer Umstände konnte von der Schriftform abgewichen werden.

Die Anforderungen an die Auftragsdatenverarbeitung ergaben sich auch bisher aus § 80 SGB X a.F. Die Anforderungen an einen Auftragsdatenverarbeitungsvertrag wichen nur unwesentlich von denen der geltenden Rechtslage ab. Als zusätzliche Anforderung im Vergleich zu § 80 SGB X sah § 80 Abs. 5 Nr. 2 a.E. SGB X a.F. noch vor, dass in dem Fall, in dem ein Auftragnehmer eine nicht-öffentliche Stelle ist, der überwiegende Teil der Speicherung des gesamten Datenbestands beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben müssen.

Die Vorgaben für Betroffenenrechte folgten aus den §§ 81ff. SGB X a.F. Auskunftsrechte waren in § 83 SGB X a.F., Berichtigung, Löschung und Sperrung waren in § 84 SGB X a.F. geregelt.

250 Sie wurde nur für die Erhebung von Angaben über die „rassische Herkunft" gefordert, vgl. § 67a Abs. 1 S. 3 SGB X a.F.

2.2 Szenario 1

Für Szenario 1 ergaben sich keine wesentlichen Abweichungen zu den diesbezüglichen Ausführungen in Kapitel I, soweit die Datenumgänge auf gesetzliche Ermächtigungstatbestände gestützt werden sollten. Eine Legitimation auf Basis einer Einwilligungserklärung war ebenfalls über § 67c Abs. 2 Nr. 2 SGB X a.F. möglich, wobei sich die Anforderungen, wie bereits erläutert, aus dem SGB X a.F. ergaben, ohne dass diese wesentlich von denen der DSGVO abweichen würden.

Die Anforderungen an technische und organisatorische Maßnahmen folgten aus § 78a SGB X a.F. und der zugehörigen Anlage zu § 78a SGB X a.F.

2.3 Szenario 2

Für Szenario 2 gilt das zu Szenario 1 Gesagte weitgehend ebenfalls. Unterschiede ergaben sich bei der Übermittlung zu Forschungszwecken nach § 75 SGB X a.F. So war zu beachten, dass keine Regelungen bestehen, die eine Weiterverarbeitung zu Forschungsfolgefragen oder eine Genehmigungsfähigkeit von noch nicht konkret bestimmbaren Forschungsvorhaben vorsahen. Weiterhin war eine weite Einwilligung zur Verarbeitung von Sozialdaten zu bestimmten Bereichen der wissenschaftlichen Forschung nach bisherigem Recht nicht vorgesehen.

2.4 Szenario 3

Für Szenario 3 ergaben sich ebenfalls keine weiteren wesentlichen Unterschiede. Wegen der nicht bestehenden Möglichkeiten einer weiten Einwilligung oder der Einbeziehung von Forschungsfolgefragen in ein Forschungsvorhaben oder aber der Genehmigung eines Vorhabens, das noch nicht konkret bestimmt war, waren die Handlungsspielräume einer externen Plattform eingeschränkt.

3 Über die aktuellen Gesetzesentwürfe hinausgehende Reformüberlegungen

3.1 Anforderungen an die Ausgestaltung einer Rechtsgrundlage zur Errichtung und Nutzung einer Datenplattform für die externe Speicherung von Sozial- und Gesundheitsdaten

3.1.1 Notwendigkeit einer Verarbeitung personenbezogener Daten

Wir gehen davon aus, dass eine Arbeit mit anonymen Daten keine praktisch umsetzbare Alternative zum Umgang mit personenbezogenen Daten ist. Dies ist unter anderem darin begründet, dass durch steigende Datenmengen und den Einsatz leistungsfähigerer Datenverarbeitung eine Re-Identifikation nicht mehr mit hinreichender Wahrscheinlichkeit ausgeschlossen werden kann. Zwar ist mit der Rechtsprechung des EuGH zum relativ zu beurteilenden Personenbezug bei IP-Adressen[251] die rechtliche Kategorie der anonymisierten Daten nachhaltig gestärkt worden, nichtsdestotrotz ist die Diskussion um die Frage, ob sich unmittelbar aus medizinischen Daten ein Personenzug ergeben kann, im Fluss. Im Hinblick auf die zunehmende Stratifizierung und Personalisierung der Medizin würde eine Löschung der identifizierenden Daten zudem die Aussagekraft der Daten beeinträchtigen. Entweder stünde eine auf den Fortbestand der Anonymität bauende Argumentation auf tönernen Füßen

251 EuGH, Rs. C-582/14, ECLI:EU:C:2016:779 – Breyer.

oder aber die Datenqualität würde erheblich beeinträchtigt. Um die notwendige Planungssicherheit für Forschungsvorhaben gewährleisten zu können, bedarf es eines rechtlichen Alternativkonstrukts für die Fälle, in denen die Daten nicht anonymisiert sind.

3.1.2 Rechtliche Rahmenbedingungen

Die Rahmenbedingungen ergeben sich zunächst aus den verfassungsrechtlichen Anforderungen, also insbesondere den maßgeblichen Gesetzgebungskompetenzen und den grundrechtlichen Gewährleistungen.

Der grundrechtliche Schutz der informationellen Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG auf nationaler Ebene wird im unionsrechtlich determinierten Bereich des Datenschutzrechts von der Gewährleistung des Art. 8 GRCh überlagert. Die wesentlichen Vorgaben beider Gewährleistungen sind zunächst, dass ein Eingriff in den Schutzbereich einer gesetzlichen Grundlage bedarf oder aber eine Einwilligung des Betroffenen vorliegt und zudem der Zweckbindungsgrundsatz beachtet wird. Grundrechtliche Kollisionen ergeben sich mit den Gewährleistungen zur Forschungsfreiheit nach Art. 5 Abs. 3 S. 1 GG und Art. 13 S. 1 GRCh. Diese sind in schonendem Ausgleich im Sinne einer praktischen Konkordanz zu bringen. Das sekundärrechtliche Unionsdatenschutzrecht ist dabei teilweise geeignet, den Schutzbereich des Art. 8 GRCh auszugestalten.[252]

Vor dem Hintergrund einer fehlenden, umfassenden Gesetzgebungskompetenz des Bundes für den Bereich des Datenschutzrechts oder der Forschung, kann eine entsprechende gesetzliche Grundlage nur eine begrenzte Reichweite erlangen, die sich im Bereich der Sozialdaten aber auf die Gesetzgebungskompetenz des Bundes zur Sozialversicherung (Art. 74 Abs. 1 Nr. 12 GG) stützen könnte. Untauglich erscheint eine solche Lösung allerdings etwa hinsichtlich der Einbeziehung von Daten, die dem Landesrecht unterfallen. Sollte eine Ausweitung auf solche Daten erstrebt werden, könnten Konzepte eines Forschungsstaatsvertrages verfolgt werden.[253] Vorliegend konzentrieren wir uns aber auf eine gesetzliche Grundlage im Sozialgesetzbuch.

3.1.3 Zweckbindung, Erforderlichkeit und Bestimmtheit

Auch wenn man in den Ansätzen einer Forschungsprivilegierung in der DSGVO möglicherweise nicht einen Eingriff, sondern eine normative Prägung des Grundrechts erkennt, die zu einer gelockerten Zweckbindung führen könnte,

252 Vgl. Schorkopf in: Ehlers, Europäische Grundrechte und Grundfreiheiten, 3. Aufl., 2009, § 16.1 Rn. 41. Mit dem Hinweis auf die Frage nach der Abgrenzung zwischen Eingriff und Ausgestaltung Kingreen in: Callies/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., 2016, Art. 8 GRCh Rn. 7.

253 Siehe etwa den Vorschlag von Weichert in: Stiftung Datenschutz (Hrsg.), Big Data und E-Health, 2017, S. 187ff.

kann dies eine Zweckbindung nicht beliebig aufweichen. Eine gleichsam ohne Zweckbindung erfolgende Speicherung von Sozial- und Gesundheitsdaten auf Vorrat durch eine externe Datenplattform wird nicht möglich sein.

Zu fordern wäre wohl mindestens ein – wenn auch sehr weit gefasster – Zweck der Versorgungs- und weiteren Forschung. Eine besondere Herausforderung für die Festlegung der im Einzelnen zu übermittelnden Daten wird in der Folge die möglicherweise noch nicht feststehende Erforderlichkeit für den Forschungszweck darstellen. Um einen hinreichenden Grad an Bestimmbarkeit trotz der Kombination des seinerseits unbestimmten Rechtsbegriffes der Erforderlichkeit und dem weiten Zweck der Forschung zu destillieren und dem zukunftsgewandten Zweck einer solchen Plattform Rechnung zu tragen, könnte die Entscheidung über die Erforderlichkeit unter Gewährung einer weiten Einschätzungsprärogative auf ein qualifiziertes Fachgremium übertragen werden. Es sollte dabei nicht ausschließlich auf die Erforderlichkeit im Zeitpunkt der Übermittlung an die Plattform abgestellt werden.

Aus der Wesentlichkeitslehre folgt, dass der Gesetzgeber Regelungen, die sich intensiv auf die Grundrechtsausübung auswirken, selbst schaffen muss und nicht an die Verwaltung delegieren kann. Andererseits muss gleichsam ein Instrument genutzt werden, das geeignet ist, um die Dynamik der Entwicklung der Datenverarbeitung aufzufangen und zeitnah einer verhältnismäßigen Entscheidung zuführen zu können. Es ist daher unsere Anregung, einen Modus zu wählen, der es ermöglicht, Datensätze anzupassen und ggf. zu erweitern oder zu beschränken.

Zur Kompensation dieser Delegation sind bei einem gelockerten Zweckbindungsverständnis erhöhte Anforderungen an die gesetzlichen Vorgaben zur Bestimmung der erforderlichen Datensätze im konkreten Fall geboten, die die Kriterien für die Entscheidung durch eine hohe legislative Dichte vorprägen. Weiterhin muss eine angemessene Aufsicht über die entscheidende Stelle und die Datenplattform garantiert werden.

3.1.4 Ermächtigungsgrundlagen und Offenbarungsbefugnisse

Erforderlich wäre des Weiteren eine gesetzliche Übermittlungsbefugnis oder -pflicht der Krankenkassen und eine Verarbeitungsbefugnis für die externe Stelle. Die Übermittlung an diese Stelle müsste geeignet sein, die Grenzen der bei den Krankenkassen bestehenden Geheimhaltungspflicht nach § 203 StGB zu überwinden, also eine Offenbarungsbefugnis gegenüber der externen Plattform beinhalten. Gleichzeitig sollten die Mitarbeiter der externen Plattform § 203 StGB unterliegen. Übermittlungsbefugnisse der externen Plattform an Dritte wären auszuschließen. Zur weiteren Sicherung einer Verarbeitung der Daten, die aber gleichzeitig externen Sachverstand nicht ausschließt, könnte der Gesetzgeber sich am Vorbild der On-Site-Datenauswertung nach Bundesstatistikgesetz orientieren und ggf. die Kategorie der „formal anonymisierten“

Daten (vgl. § 5a Abs. 3 Bundestatistikgesetz) übernehmen. Die Beteiligung externer Forscher könnte dann ohne Datentransfer in einer kontrollierten Auswertungsumgebung gewährt werden.

3.1.5 Eigenständiges Institut für Sozialdatenforschung

Eine solche Datenplattform könnte als eigenständige Stelle etwa als „Institut für Sozialdatenforschung" – von den Krankenkassen getrennt – organisatorisch bei einer fachlich geeigneten, selbstständigen Bundesoberbehörde angegliedert werden. In Betracht kämen beispielsweise das Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) oder das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). Die Rechts- oder Fachaufsicht würde durch das Bundesministerium für Gesundheit (BMG) gewährleistet.

3.1.6 Grundrechtskonformes Schutzniveau und Evaluation

Ob eine solche Stelle in § 35 SGB I a.F. aufgenommen werden sollte, ist fraglich und müsste im Einzelnen untersucht werden. Ein Absinken des Datenschutzniveaus ist bei einer entsprechenden Ausgestaltung der zu schaffenden gesetzlichen Grundlage nicht zwingend. Gleichzeitig könnten Probleme bei der Anwendung des Rechts ausgeschlossen werden, wenn nicht der gesamte Kanon des Sozialdatenschutzrechts auf die Datenplattform Anwendung findet und sich die zu Anfang des Kapitels beschriebenen Auslegungsfragen und -widersprüche nicht fortführen lassen würden. Im Hinblick auf die besondere Sensibilität der Daten sind selbstredend besonders hohe Anforderungen an technische und organisatorische Maßnahmen hinsichtlich der Art und Weise der Datenverarbeitung zu stellen.

Um eine dauerhafte Vereinbarkeit der Ausgestaltung mit den kollidierenden Grundrechtsgütern zu gewährleisten, sollte eine fortlaufende Evaluation und Bewertung durch die Exekutive oder eine unabhängige gutachterliche Expertise erfolgen.

3.2 Anforderungen an die Ausgestaltung einer Einwilligung mit breiter Zweckbestimmung (Broad Consent)

Für den Bereich der wissenschaftlichen Forschung ist die Möglichkeit einer erweiterten Einwilligung in Form des Broad Consent in der DSGVO bereits angelegt. Gemäß Erw.Gr. 33 soll es betroffenen Personen möglich sein, ihre Einwilligung für bestimmte Bereiche der wissenschaftlichen Forschung und nicht, wie noch gegenwärtig, ausschließlich für konkrete Vorhaben abzugeben. Damit soll dem Problem der Wissenschaft Rechnung getragen werden,

dass die Zwecke der Datenverarbeitung im Bereich der wissenschaftlichen Forschung zum Zeitpunkt der Datenerhebung oftmals nicht vollständig angegeben werden können.

Die DSGVO fordert in Erw.Gr. 33 ausdrücklich, dass ein Broad Consent unter Einhaltung der anerkannten **ethischen Standards** der wissenschaftlichen Forschung eingeholt werden soll. Diesen Standards und somit der Prüfung der Forschungsvorhaben durch die Ethikkommissionen wird damit zusätzlich eine datenschutzrechtliche Relevanz eingeräumt. Auch wenn ethische Standards bereits gegenwärtig einzuhalten sind, könnten Verstöße künftig zu einer rechtswidrigen Datenverarbeitung führen, wenn die Einwilligung eines Betroffenen diesen Standards nicht genügt.

Die europarechtlichen Vorgaben hat der nationale Gesetzgeber in § 67b Abs. 3 SGB X aufgegriffen und umgesetzt. Für Einwilligungen in die Übermittlung zu Forschungszwecken bestimmt § 67b Abs. 3 SGB X, dass die Einwilligung sowohl in Bezug auf ein bestimmtes Vorhaben als auch im weiteren Umfang für bestimmte Bereiche der wissenschaftlichen Forschung erteilt werden kann. Laut der Gesetzesbegründung soll mit dieser „erweiterten" Einwilligung dem Umstand Rechnung getragen werden, dass konkrete Forschungsvorhaben zum Zeitpunkt der Datenerhebung häufig noch nicht benannt werden können, sondern im Laufe der Zeit sukzessiv entwickelt werden.[254] Das entspricht – systematisch kohärent – auch dem erweiterten Zweckbindungsverständnis in § 75 Abs. 4a SGB X, mit dem die Möglichkeit angelegt wurde, für ein bestimmtes Vorhaben übermittelte Sozialdaten für weitergehende Forschungsfragen des gleichen Forschungsbereichs zu verwenden, soweit die Forschungsfrage im inhaltlichen Zusammenhang zur Ausgangsfrage steht und die Behörde die Verwendung im entsprechenden Umfang genehmigt hat.

3.2.1 Bestimmter Bereich der wissenschaftlichen Forschung

Die Formulierung sowohl der DSGVO als auch des § 67b Abs. 3 SGB X wirft jedoch die Frage auf, was unter einem „bestimmten Bereich der wissenschaftlichen Forschung" zu verstehen ist. Der deutsche Gesetzgeber macht in der Gesetzesbegründung zum SGB X deutlich, dass er auch im Rahmen des Broad Consent an den Grundzügen der bestimmten Einwilligung nach Art. 4 Nr. 11 DSGVO festhält und nicht etwa die Einholung einer Generaleinwilligung erlaubt.[255] So genügt eine pauschale Bezugnahme auf Forschungszwecke allgemein („Open Consent") dem Bestimmtheitsgrundsatz auch im Rahmen des Broad Consent nicht.[256] Zwar muss sich die Einwilligung nicht mehr auf ein konkret benanntes Vorhaben richten. Dennoch ist zumindest der Forschungs-

254 BT-Drs. 18/12611, S. 113; vgl. hierzu auch Erw.Gr. 33 S. 1.
255 BT-Drs. 18/12611, S. 113.
256 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 6 Rn. 9.

bereich vorher explizit festzulegen. Dementsprechend fordert der Gesetzgeber, dass der Forschungsbereich nicht zu allgemein gefasst sein darf und sich auf ein thematisch abgegrenztes Feld beziehen muss, welches schrittweise konkretisiert wird.[257] Wie eng der thematisch begrenzte Forschungsbereich jedoch im Einzelnen sein muss und ob der Betroffene über die Konkretisierung informiert werden muss, geht aus der Gesetzesbegründung nicht hervor. Art. 13 Abs. 1 lit. c) und 14 Abs. 1 lit. c) DS.-GVO bestimmen allerdings, dass die betroffene Person über die „Zwecke der Datenverarbeitung" informiert werden muss. Die Angaben müssen so konkret sein, dass die betroffene Person sich ein klares Bild machen kann, welche Daten von ihr wofür verarbeitet werden.

3.2.2 Bestimmtheit des Forschungsbereichs

Demzufolge ist es empfehlenswert, den gewählten Forschungsbereich, möge er auch vergleichsweise weit gefasst sein, so genau wie möglich zu definieren und bei sehr weitem Verständnis thematisch zu umreißen und entsprechend zu beschreiben. Im Bereich des Sozialdatenschutzrechts wird sich die Begrenzung jedoch unabhängig von der Auslegung des Begriffs des Forschungsbereichs regelmäßig aus dem Erfordernis des inhaltlichen Zusammenhangs mit dem Ausgangsvorhaben (§ 75 Abs. 2, 4a SGB X) ergeben. Eine Einwilligung in der Form, dass neben der Verarbeitung zu Zwecken des Ausgangsvorhabens auch in die Speicherung und den Open Access im Rahmen eines bestimmten Repositoriums zugestimmt wird,[258] dürfte hier ausscheiden. Das Erfordernis des inhaltlichen Zusammenhangs ist dabei nicht zu unterschätzen, da dieser gemäß § 75 Abs. 4a S. 4 SGB X im Rahmen der Anzeige an die Aufsichtsbehörde angezeigt werden muss.

3.2.3 Konkretisierungspflicht

Eine nachträgliche Informationspflicht zur (schrittweisen) Konkretisierung der Folgeforschungsfragen, wie man sie aus der Gesetzesbegründung durchaus herauslesen kann, würde zwar grundsätzlich den Interessen des Betroffenen Rechnung tragen und die effektive Ausübung des Widerspruchsrechts ermöglichen. Andererseits stünde eine solche Pflicht im Widerspruch zur Idee des Broad Consent, der gerade verhindern soll, dass der Verantwortliche für jedes Vorhaben erneut Kontakt zum Betroffenen herstellen und eine Einwilligung einholen muss. Zudem wurde die bereits vielfach diskutierte und in einigen Bereichen bereits umgesetzte Idee des „Dynamic Consent"[259] gerade nicht in die DSGVO aufgenommen. Eine nachträgliche Informationspflicht

257 BT-Drs. 18/12611, S. 113.
258 Vgl. hierzu *Schaar*, ZD 2017, 213 (215).
259 Hierzu im Einzelnen: *Raum*, in: Ehmann/Selmayr, DS-GVO, 2017, Art. 89 Rn. 27.

findet weder in der DSGVO noch in den nationalen Vorschriften eine rechtliche Grundlage.

3.2.4 Zeitliche Reichweite

Im Rahmen der Einwilligung mit breiter Zweckbestimmung stellt sich auch die Frage nach der zeitlichen Dimension: Zum einen, ob eine Einwilligung auch zukünftig erhobene Sozialdaten umfassen kann und zum anderen, wie lange eine einmal erteilte Einwilligung wirksam bleibt.[260]

Erstere Frage stellt sich, wenn bei Erteilung einer Einwilligung das betreffende Datum noch nicht existiert, die betroffene Person also noch gar nicht einschätzen kann, ob sie diesbezüglich mit der Verarbeitung einverstanden sein wird. Hierbei handelt es sich aber um eine typische Problematik der informierten Einwilligung. Es kommt dabei nicht darauf an, dass die betroffene Person die Details eines Datums kennt, sondern die Art der Daten und die Zwecke, zu denen sie verarbeitet werden sollen. Würde man die Forderung erheben, dass jedes einzelne Datum bekannt ist, würde eine im Vorhinein zu erteilende Einwilligung kein taugliches Instrument mehr darstellen. Eine Einwilligung kann also – je nach Ausgestaltung – auch zukünftig erhobene Sozialdaten umfassen.

Die bloße Festlegung auf einen Bereich, anders als bei der Festlegung auf ein konkretes Vorhaben, umfasst zudem gegebenenfalls besonders lange Zeiträume. Zwar existiert im Rahmen der Einwilligung keine Vorgabe zur zeitlichen Geltung der Erklärung. Sofern der Betroffene von der Verarbeitung seiner Daten jedoch keine unmittelbaren Auswirkungen erfährt, könnte jedoch erwogen werden, dass eine Einwilligung verfällt und eine erneute Einwilligung nach dem Ablauf einer gewissen Zeitspanne notwendig ist, damit der Betroffene sein Widerrufsrecht auch nach längerer Zeit noch effektiv wahrnehmen kann.[261] Ein solches Erfordernis lässt sich jedoch nicht aus dem Gesetz ableiten. Nach hier vertretener Ansicht gelten Einwilligungen daher unbefristet. Es kann sich im Interesse des Betroffenen aber empfehlen, diesen im Rahmen der Einwilligung auf den zeitlichen Rahmen eines Vorhabens hinzuweisen (insbesondere bei langer Dauer) und im Zweifel eine Bestätigung oder zumindest einen Hinweis auf die weitere Datenverarbeitung nach dem Ablauf einer längeren Frist vorzusehen.

Im Sozialdatenschutzrecht kann dies im Rahmen von § 75 SGB X entbehrlich sein, da dieses von Gesetzes wegen eine Beschränkung der Verarbeitungs- und Speicherdauer durch die Genehmigung vorsieht.

260 Siehe Pflichtenheft Nr. 3.2.

261 Ausgangspunkt solcher Erwägungen dürfte zumeist die Rechtsprechung zu über längere Zeit ungenutzte Werbeeinwilligungen darstellen, vgl. etwa *LG München*, Urteil vom 8.4.2010, Az. 17 HK O 138/10.

3.2.5 Vorgaben des Art. 89 DSGVO

Für den Broad Consent im Bereich der wissenschaftlichen Forschung gelten ebenso die Vorgaben des Art. 89 DSGVO. Der Verantwortliche hat geeignete Garantien für die Rechte und Freiheiten der Betroffenen zu gewährleisten. Dabei sind geeignete technische und organisatorische Maßnahmen vorzusehen, die dies sicherstellen und insbesondere den Grundsatz der Datenminimierung – unabhängig vom Vorliegen einer legitimierenden Einwilligung – umsetzen.

3.2.6 Einhaltung ethischer Standards

Auch wenn der deutsche Gesetzgeber die Einhaltung ethischer Standards der wissenschaftlichen Forschung nicht unmittelbar in die Vorschriften des SGB X aufgenommen hat, ergibt sich diese Anforderung aus den Erwägungsgründen der DSGVO. Der Gesetzgeber kann aufgrund der Öffnungsklauseln abweichende, strengere Regelungen schaffen. Eine Unterschreitung des Mindeststandards ist jedoch nicht zulässig. Daher spricht viel dafür, auch bei Forschungsvorhaben mit Sozialdaten die ethischen Standards der wissenschaftlichen Forschung einzuhalten, obgleich es sich bei Erwägungsgründen nicht um einen unmittelbar Geltung entfaltenden Verordnungstext handelt. Verbindliche Standards sind insbesondere in der Deklaration von Helsinki[262] kodifiziert. Darüber hinaus spielen aber auch Empfehlungen und Leitlinien zur Sicherung der guten wissenschaftlichen Praxis, Ethik-Kodizes oder Vorgaben der Berufsordnungen eine wesentliche Rolle[263], die allesamt die freiwillige informierte Einwilligung für eine Teilnahme fordern. Die Option des „Broad Consent" ist im Hinblick auf Datenschutz und die Ethikleitlinien nicht unumstritten. Es stellt sich die Frage, wie informiert eine Einwilligung noch sein kann, wenn der teilnehmenden Person die genauen Inhalte einer zukünftigen Verwendung von Daten nicht mitgeteilt werden können.[264] Fraglich ist in diesem Zusammenhang auch, wie „weite Einwilligungen" den Anforderungen der Ethikleitlinien gerecht werden können.[265] Um den Anforderungen an eine möglichst informierte Einwilligung zu genügen, ist bei einem „Broad Consent" die Aufklärung besonders wichtig. Hier sollte dem Teilnehmer erklärt werden, dass die späteren Forschungsprojekte zum Zeitpunkt der Datenerhebung noch unbekannt sind.[266] Außerdem sollte über die geplante Aufbewahrungsdauer gesprochen und eine solche ggf. auch schriftlich festgehalten

262 *Bundesärztekammer*, WMA Deklaration von Helsinki – Ethische Grundsätze für die medizinische Forschung am Menschen, 2013, abrufbar unter: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/International/Deklaration-von-Helsiniki_2013_DE.pdf (abgerufen: 04.09.2017).

263 *Schaar*, ZD 2017, 213 (217); BT-Drucks. 18/12611, S. 113.

264 *Herbst*, DuD 2016, 371 (373).

265 *Schaar*, ZD 2017, 213 (220).

266 *Herbst*, DuD 2016, 371 (373).

werden. Es ist sicherzustellen, dass sich der Teilnehmer über die Tragweite seiner Einwilligung bewusst ist. Auch muss klar sein, dass die Daten zu Forschungszwecken verwendet werden und die Forschung einen Nutzen für die Allgemeinheit bezweckt.[267] Die Zwecke der Datenverarbeitung sollten so genau wie zum Zeitpunkt der Einwilligung möglich beschrieben und eingegrenzt werden.

267 *Herbst*, DuD 2016, 371 (373).

4 Zusammenfassung und Gesamtergebnis

Die Untersuchung der sozialdatenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Gesundheitsdaten zu Zwecken der Forschung, Planung und Qualitätssicherung anhand der im Rahmen des SAHRA-Projekts zu bewertenden Szenarien zeigt die besonderen Herausforderungen des europarechtlich überformten Rechtsgebiets zu einem Zeitpunkt des laufenden Gesetzgebungsprozesses. Eine abschließende Bewertung der Zulässigkeit, also das „Ob" der Datenumgänge auf der einen Seite, aber auch die Anforderungen an die Durchführung, also das „Wie" der Datenverarbeitungen auf der anderen Seite, sind in einem komplexen rechtlichen System eingebettet. Während mit der DSGVO der sekundärrechtliche Rahmen des Unionsrechts gesetzt ist, und auch das Sozialdatenschutzrecht nach den §§ 35 SGB I i.V.m. §§ 67ff. SGB X bereits an die DSGVO angepasst wurde, stehen die wesentlichen Änderungen im fachspezifischen Datenschutzrecht des SGB V noch aus. Der hier gewählte Ansatz, auf Basis des bisher bekannten Gesetzgebungsstandes, eine umfangreiche Untersuchung der rechtlichen Situation durchzuführen, lässt aber bereits eine sehr weitgehende Bewertung zu. Dies gilt insbesondere, da der Bundesgesetzgeber in seiner bisherigen Anpassung des SGB I und SGB X sein Bestreben aus den Gesetzgebungsverfahren auf europäischer Ebene, das nationale Sozialdatenschutzrecht soweit wie möglich beibehalten zu können, konsequent verfolgt hat. Mit den Forschungstatbeständen im SGB X wurde von den gelockerten Zweckbindungsverständnissen zur Privilegierung der wissenschaftlichen Forschung Gebrauch gemacht. Im Übrigen

wurden Struktur und Systematik des Sozialdatenschutzes weitgehend beibehalten. Das lässt darauf schließen, dass auch mit den kommenden Anpassungs- und Umsetzungsgesetzgebungen an die DSGVO ein tendenziell konservativer Ansatz gewählt werden wird, der gewisse Freiheiten für die Forschung mit sich bringen kann. Das soll allerdings nicht bedeuten, dass diese zurückhaltenden Reformen nicht ganz wesentliche Auswirkungen auf die Bereiche der Forschung, Planung und Qualitätssicherung haben können.

Die wesentlichen Prinzipien des Datenschutzrechts ergeben sich – neben den unionsrechtlichen und verfassungsrechtlichen Grundrechtsgewährleistungen – künftig unmittelbar aus der DSGVO. Hierzu gehören

- die Rechtmäßigkeit der Verarbeitung,
- der Zweckbindungsgrundsatz,
- die Verarbeitung nach Treu und Glauben,
- die Datenminimierung,
- Datentransparenz,
- Richtigkeit der Daten,
- Speicherbegrenzungen,
- Integrität und Vertraulichkeit,
- Rechenschaftspflichten,
- der Grundsatz der Direkterhebung und
- das Prinzip der Erforderlichkeit.

Der Begriff der personenbezogenen Daten eröffnet den sachlichen Anwendungsbereich des europäischen und nationalen Datenschutzrechts in Abgrenzung zu anonymen Daten. Der Begriff des Anonymisierens wird zwar in der DSGVO – anders als bisher im nationalen Recht – nicht mehr definiert, allerdings bedeutet dies nicht, dass die Kategorie der anonymen Daten, die ohne datenschutzrechtliche Restriktionen verarbeitet werden können, damit entfallen sei. Vielmehr kann unter Heranziehung von Erwägungsgrund 26 der DSGVO mithilfe der Rechtsprechung des EuGH zum Personenbezug von IP-Adressen davon ausgegangen werden, dass sich der Personenbezug relativ bestimmen wird und dann abzulehnen ist, wenn die Herstellung des Personenbezugs mit einem unverhältnismäßigen Aufwand verbunden wäre.

Dort, wo die DSGVO Öffnungsklauseln für die mitgliedsstaatliche Gesetzgebung bereithält, bleibt jedoch ein Handlungsspielraum, der – insbesondere im öffentlichen Gesundheitswesen – umfassende nationale Regelungen ermöglicht.

Für die Verarbeitung von Sozialdaten der Krankenkassen zu Zwecken der Forschung, Planung und Qualitätssicherung, ggf. unter Einbeziehung einer externen Plattform, bedeutet dies, dass neben der DSGVO das Sozialdatenschutzrecht nach SGB I und SGB X sowie die fachspezifischen Normen des SGB V Anwendung finden.

Hieraus ergeben sich die Voraussetzungen zur Bewertung der im Zentrum dieses Gutachtens stehendenden Szenarien:

Für das eingangs beschriebene **Szenario 1**, bei dem eine Krankenkasse die bei ihr gespeicherten Sozialdaten selbst auswertet und lediglich anonyme Auswertungsergebnisse an externe Partner übermittelt, folgt aus der gegenwärtig bewertbaren Rechtssituation, dass dies nach den Vorgaben gemäß § 67b Abs. 1 S. 1, 2 SGB X i.V.m. § 284 Abs. 3, § 287 SGB V zulässig ist. Die Forschungsvorhaben sind dabei nicht auf medizinische Fragestellungen begrenzt. Probleme bereiten hierbei die Formulierungen zu Anonymisierungsanforderungen, die in ihrer derzeitigen Ausgestaltung nach bisheriger Auslegung geeignet sind, Forschungsvorhaben in ihrem Nutzen für die Allgemeinheit deshalb einzuschränken, weil der verwertbare Datenbestand stark auf bereits abgeschlossene Sachverhalte reduziert wäre. Ein Rückgriff auf allgemeine Forschungsklauseln im SGB X ist nach bisheriger Auslegung des § 287 SGB V nicht möglich. Der Gesetzgeber könnte die anstehende Anpassung an die DSGVO jedoch als Anlass nehmen, dies zu ändern.

Auch die Auswertung von Sozialdaten durch den Leistungsträger auf Grundlage des gesetzlichen Tatbestandes des § 67c Abs. 2 Nr. 2 SGB X ist zulässig. Ob eine Anwendung von § 75 Abs. 2 und Absatz 4 S. 1 SGB X in Betracht kommt, ist allerdings fraglich. Die besseren Argumente sprechen dafür, dass die sich aus dem Wortlaut ergebende Begrenzung auf Forschungsvorhaben eine Anwendung für Planungsvorhaben nicht zulässt.

Die Selbstauswertung durch einen Leistungsträger zum Zwecke der Qualitätssicherung scheidet wegen der strengen Anforderungen des § 299 Abs. 1a SGB V aus. Anderweitige Erlaubnisvorschriften sind insoweit nicht ersichtlich.

Alternativ zu einer gesetzlichen Ermächtigungsnorm kann sowohl ein Forschungsvorhaben, ein Planungsvorhaben als auch ein Qualitätssicherungsvorhaben auf eine Einwilligung gestützt werden. Da der Gesetzgeber von seiner Regelungskompetenz zum vollständigen Ausschluss der Einwilligung im Bereich der Verarbeitung von besonderen Kategorien personenbezogener Daten keinen Gebrauch gemacht hat, ist eine Einwilligung unter Rückgriff auf die DSGVO stets zulässig. Im Rahmen einer denkbaren Anpassung des SGB V an die DSGVO könnte der deutsche Gesetzgeber jedoch die Möglichkeit der Einholung einer Einwilligungserklärung für besondere Kategorien personenbezogener Daten ausschließen oder nur unter erhöhten Anforderungen zulassen.

Bei allen Verarbeitungen sind angemessene, spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen, wie sie sich aus der DSGVO bzw. dem nationalen Datenschutzrecht ergeben. Ein Genehmigungserfordernis besteht ausschließlich bei einer Verarbeitung von Sozialdaten zu Forschungszwecken.

Im **Szenario 2**, in dem Leistungsträger der Gesetzlichen Krankenversicherung und eine externe Einrichtung kooperieren und Sozialdaten für ein bestimmtes Vorhaben an die externe Einrichtung übermitteln, die diese im Sinne des Vorhabens verarbeitet und auswertet, ergibt sich Folgendes:

Die Weitergabe von Sozialdaten an eigenverantwortlich handelnde externe Einrichtungen ist in den Bereichen der wissenschaftlichen Forschung, der Planung im Sozialleistungsbereich sowie der Qualitätssicherung in unterschiedlichem Umfang möglich. Für die Qualitätssicherung ergibt sich die Befugnis zur Übermittlung allein aus der spezialgesetzlichen Norm des § 299 SGB V, die eine Übermittlung ausschließlich nach den Vorgaben der Beschlüsse und Richtlinien des G-BA legitimiert.

Für den Bereich der wissenschaftlichen Forschung ist die Übermittlung an externe Stellen vornehmlich auf Grundlage von §§ 75, 76 SGB X möglich. Dabei stellen die §§ 75, 76 SGB X jedoch detaillierte Regelungen auf, deren Einhaltung im Rahmen eines obligatorischen Genehmigungsverfahrens überprüft wird. So stellen die vorzuhaltenden technischen und organisatorischen Maßnahmen, der Erforderlichkeitsgrundsatz und das grundsätzliche Einwilligungserfordernis, welches aufgrund der Ausweitung des strafrechtlichen Geheimnisschutzes (§ 203 StGB) auf die Übermittlung der von Ärzten stammenden Abrechnungsdaten nach § 76 SGB X auch nicht unter den in § 75 SGB X genannten Voraussetzungen entbehrlich ist, die wesentlichen Anforderungen an die Zulässigkeit des Vorhabens dar. Festzuhalten bleibt abschließend, dass die Übermittlung von Sozialdaten zum Zweck der wissenschaftlichen Forschung einem strengen Genehmigungsvorbehalt unterliegt und der Einwilligung der Betroffenen in Form einer Schweigepflichtentbindung bedarf. Keiner Schweigepflichtentbindung bedarf es in der Regel bei pseudonymisierten Daten, da es insofern an der Offenbarung eines Geheimnisses im Sinne des § 203 StGB fehlen wird, wenn der Empfänger das Pseudonym nicht aufdecken kann.

Für die Planung im Sozialleistungsbereich gestaltet sich die Übermittlung an eigenverantwortlich handelnde, externe Stellen ebenso wie im Bereich der Forschung. Einschränkend kommt hier hinzu, dass die externe Stelle nur eine öffentliche Stelle sein kann, bei der die Planung zum zugewiesenen Aufgabenbereich gehört.

Soll die externe Stelle als Auftragsverarbeiter eingebunden werden, bedarf dies nach hier vertretener Auffassung grundsätzlich keiner gesonderten Ermächtigungsgrundlage. Vielmehr ist die Einbindung als Teil der Verarbeitungstätigkeit des Verantwortlichen zulässig, wenn dieser zu der geplanten Form der Verarbeitung legitimiert ist und die zusätzlichen Anforderungen des Art. 28 DSGVO sowie des § 80 SGB X eingehalten werden. Neben dem Erfordernis eines Auftragsverarbeitungsvertrages ergibt sich aus § 80 Abs. 3 SGB X eine Einschränkung für die Beauftragung von nicht-öffentlichen Stellen, die nur unter den beschriebenen, sehr engen Voraussetzungen einbezogen werden können.

Aus § 78 SGB X folgt sowohl die streng verstandene Zweckbindung hinsichtlich einer Verarbeitung der Sozialdaten durch den Empfänger, der wie eine in § 35 SGB I genannte Stelle an das Sozialgeheimnis gebunden ist, als auch die Befugnis zur Verarbeitung zu diesem Zweck. Auf sonstige Erlaubnistatbestände – insbesondere solche des allgemeinen Datenschutzrechts – kann nicht zur Weiterverarbeitung zurückgegriffen werden. Alternativ wäre es zwar möglich, eine Einwilligung nach den Vorgaben der DSGVO einzuholen, allerdings kann die externe Stelle als durch § 78 Abs. 1 SGB X gebundener Empfänger die erhaltenen Daten nicht zum Zweck der Einholung einer solchen Einwilligung verwenden, sodass praktisch kaum ein Anwendungsfall bestehen dürfte.

Eine Auftragsverarbeitung richtet sich in jedem Fall nach den Vorgaben des § 80 SGB X, in dessen Rahmen sie auch zulässig ist.

Die Verarbeitung nach einer Übermittlung ist von der Genehmigung nach § 75 Abs. 4 SGB X umfasst. Im Falle der Auftragsverarbeitung ist eine Anzeige gegenüber der Rechts- oder Fachaufsicht erforderlich.

In **Szenario 3A** erhält die externe Plattform Sozialdaten von unterschiedlichen Krankenkassen, führt diese zusammen und wertet sie selbst aus. Im Anschluss werden nur die anonymisierten Ergebnisse weitergegeben.

Die Übermittlung und Auswertung von Sozialdaten an eine zu Forschungszwecken folgt analog Szenario 2. Für eine Datensammlung auf Vorrat besteht jedoch keine gesetzliche Grundlage.

Eine Auftragsverarbeitung zu etablieren, wird hingegen kaum derart möglich sein, dass ein Auftragsverarbeiter gleichzeitig für mehrere Auftragsverarbeiter tätig wird, ohne in Konflikt mit den jeweiligen Weisungsrechten zu kommen, zumal der notwendige Konkretisierungsgrad der erforderlichen Verarbeitungsschritte regelmäßig nicht erreicht werden dürfte. Bestünden eigene Entscheidungsspielräume der externen Stelle hinsichtlich der Verarbeitungen, so wäre dies als Auftragsverarbeitung ohnehin nicht abbildbar.

Für weitere Zwecke wird in der Regel nur eine Einwilligung als Ermächtigungsgrundlage in Betracht kommen.

In **Szenario 3B** erhält die externe Plattform Sozialdaten von den unterschiedlichen Krankenkassen, um diese nicht selbst auszuwerten, sondern mit den Daten der anderen Krankenkassen ggf. zusammenzuführen und zu Auswertungszwecken an eine abermals dritte Stelle zu übermitteln.

Abweichend von den Ergebnissen zu Szenario 3A kommt hier auch entsprechend § 67d Abs. 3 SGB X eine Übermittlung von Sozialdaten über Vermittlungsstellen im Rahmen einer Auftragsverarbeitung als zulässige Alternative in Betracht, sodass die folgende Übermittlung an die weitere Stelle im Ergebnis eine Übermittlung der verantwortlichen Krankenkasse darstellen würde, deren Zulässigkeit sich nach den vorbeschriebenen Voraussetzungen bestimmt. Besondere Beachtung findet bei den Weiterübermittlungen die absolute Zweckbindung des § 78 Abs. 1 SGB X.

Abkürzungsverzeichnis

AOK	Allgemeine Ortskrankenkasse (www.aok.de)
BDSG	Bundesdatenschutzgesetz in der Fassung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017[268] (m.W.z. 25.05.2018)
BDSG a.F.	Bundesdatenschutzgesetz in der am 30.09.2017 geltenden Fassung
BSG	Bundessozialgericht
DFG	Deutsche Forschungsgemeinschaft (www.dfg.de)
DSAnpUG-EU	Datenschutz- Anpassungs- und Umsetzungsgesetz
DSGVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)
EG	Europäische Gemeinschaft
Erw.Gr.	Erwägungsgrund der DSGVO
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GKV	Gesetzliche Krankenversicherung
m.W.z.	mit Wirkung zum
PDF	Portable Document Format von Adobe (www.adobe.com)
SAHRA	Smart Analysis – Health Research Access; vom BMWi gefördertes Verbundprojekt zum Aufbau einer Datenplattform für Sozial- und andere Gesundheitsdaten
SGB	Sozialgesetzbuch
SGB I a.F.	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – in der bis zum 25.05.2018 geltenden Fassung
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – in der Fassung des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017[269] (m.W.v. 25.05.2018)
SGB X a.F.	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der bis zum 25.05.2018 geltenden Fassung
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017[270] (m.W.v. 25.05.2018)

268 BGBl. I 2017, 2097.
269 BGBl. I 2017, 2541.
270 BGBl. I 2017, 2541.

StGB	Strafgesetzbuch in der Fassung des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017[271]
StGB a.F.	StGB in der am 30.09.2017 geltenden Fassung
TMF	TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)

271 BGBl. I 2017, 3618.

Literatur

Becker, Ulrich/Kingreen, Thorsten (Hrsg.), SGB V – Gesetzliche Krankenversicherung Kommentar, 5. Auflage 2017

Wolff, Amadeus/Brink, Stefan, Beck'scher Online-Kommentar Datenschutzrecht, 20. Ed. 1.2.2017,

Callies, Christian/Ruffert, Matthias (Hrsg.), Kommentar zum EUV/AEUV mit europäischer Grundrechtecharta, 5. Auflage 2016

Diering, Björn/Timme, Hinnerk (Hrsg.), Lehr- und Praxiskommentar zum SGB X, 4. Auflage 2016

Dovas, Marian-Urania, Joint Controllership – Möglichkeiten oder Risiken der Datennutzung?, Zeitschrift für Datenschutz 2016, S. 51–517.

Eichenhofer, Eberhard/Wenner, Ulrich (Hrsg.), SGB V – Gesetzliche Krankenversicherung Kommentar, 2013

Ehlers, Dirk (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Aufl., 2009

Ehmann, Eugen/Selmeyr, Martin (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2017

Gola, Peter/Schomerus, Rudolf et al., Bundesdatenschutzgesetz Kommentar, 12. Auflage 2015

Hänlein, Andreas/Schuler, Rolf (Hrsg.), Lehr- und Praxiskommentar zum SGB V, 5. Auflage 2016

Hase, Friedhelm, Forschung mit Sozialdaten, Datenschutz und Datensicherheit 2011, S. 875–878

Hauck, Karl/Noftz, Wolfgang/Becker, Ulrich (Hrsg.), Hauck/Noftz SGB I – Allgemeiner Teil Kommentar, Loseblattwerk mit Stand vom Juli 2017

Hauck, Karl/Noftz, Wolfgang (Hrsg.), Hauck/Noftz SGB V – Gesetzliche Krankenversicherung Kommentar, Loseblattwerk mit Stand vom August 2017 (Aktualisierung 08/2017)

Hauck, Karl/Noftz, Wolfgang/Becker, Peter (Hrsg.), Hauck/Noftz SGB X – Soziale Pflegeversicherung Kommentar, Loseblattwerk mit Stand vom August 2017 (Aktualisierung 02/2017)

Herbst, Thomas, Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, Datenschutz und Datensicherheit 2016, S. 371–375

Körner, Anne/Leitherer, Stephan/Mutschler, Bernd (Hrsg.), Kasseler Kommentar Sozialversicherungsrecht, 94. Auflage 2017

Kircher, Philipp, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2017

Kühling, Jürgen/Martini, Mario et al., Die DSGVO und das nationale Recht, 2016

Meier, Andre, Der rechtliche Schutz patientenbezogener Gesundheitsdaten, 2003

Mrozynski, Peter, SGB I – Sozialgesetzbuch Allgemeiner Teil Kommentar, 5. Auflage 2014

Orlowski/Rau/Schermer/Wasem/Zipperer (Hrsg.), GKV-Kommentar – SGB V, Loseblattwerk mit Stand vom August 2017 (45. Aktualisierung)

Paal, Boris/Pauly, Daniel (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2017

Plath, Kai-Uwe (Hrsg.), BDSG/DSGVO Kommentar, 2. Auflage 2016

Roßnagel, Alexander (Hrsg.), Das neue Datenschutzrecht, 2018

Roßnagel, Alexander (Hrsg.), Europäische Datenschutz-Grundverordnung, 2017

Schaar, Katrin, Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte, Zeitschrift für Datenschutz 2017, S. 213–220

Schlegel, Rainer/Voelzke, Thomas (Hrsg.), jurisPK-SGB V, 3. Auflage 2016

Schlegel, Rainer/Voelzke, Thomas (Hrsg.), jurisPK-SGB X, 2013

Schmidt, Bernd/Freund, Bernhard, Perspektiven der Auftragsverarbeitung, Zeitschrift für Datenschutz 2017, S. 14–18

Schmitz, Barbara/von Dall'Armi, Jonas, Auftragsdatenverarbeitung in der DSGVO – das Ende der Privilegierung?, Zeitschrift für Datenschutz 2016, 427–432

Schubert/Köster/Küpper-Nybelen/Ihle, Versorgungsforschung mit GKV-Routinedaten, Bundesgesundheitsblatt 2008, S. 1095–1105

Schütze, Bernd (Hrsg.), von Wulffen/Schütze – SGB X – Sozialverwaltungsverfahren und Sozialdatenschutz Kommentar, 8. Auflage 2014

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Auflage 2014

Spickhoff, Andreas (Hrsg.), Medizinrecht, 2. Auflage 2014

Spindler, Gerald, Big Data und Forschung mit Gesundheitsdaten in der gesetzlichen Krankenversicherung, Medizinrecht 2016, S. 691–699

Stiftung Datenschutz (Hrsg.), Big Data und E-Health, 2017

Taeger, Jürgen/Gabel, Detlev (Hrsg.), BDSG und Datenschutzvorschriften des TKG und TMG, 2. Auflage 2013

II

Spezielle datenschutzrechtliche Fragen der Weiternutzung von Sozial- und Gesundheitsdaten für die medizinische Forschung

Prof. Dr. iur. Alexander Roßnagel
Unter Mitarbeit von Dr. iur. Christian Geminn

Kassel, 31.03.2018

Zusammenfassung

Das Gutachten soll Rechtsfragen zur Nutzung von Sozial- und Gesundheitsdaten beantworten, die durch neue gesetzliche Regelungen verursacht und für das BMWi-Forschungsprojekt „Smart Analysis – Health Research Access" (SAHRA) von Bedeutung sind. Diese neuen Regelungen sollen analysiert und mit der bisherigen Rechtslage verglichen werden.

Die neuen Regelungen

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) gilt vom 25. Mai 2018 an mit all ihren Regelungen in allen Mitgliedstaaten unmittelbar. Sie bestimmt vorrangig das künftige Datenschutzrecht in Europa. Dieses wird aber nicht allein durch die Union geprägt. Vielmehr wird sie in vielen Bereichen und Aspekten ergänzt durch Datenschutzregelungen der Mitgliedstaaten. Dadurch entsteht im Datenschutz eine Ko-Regulierung durch Union und Mitgliedstaaten. Erst das komplizierte Zusammenwirken von Unionsrecht und Recht der Mitgliedstaaten bewirkt das zukünftige Europäische Datenschutzrecht.

Daher sind neben der Datenschutz-Grundverordnung das neue Bundesdatenschutzgesetz vom 30. Juni 2017 (BDSG-neu) und die Neufassung des Sozialdatenschutzes im SGB I und X (SGB I-neu und SGB X-neu) zu beachten. Diese neuen gesetzlichen Regelungen treten am 25. Mai 2018 – zusammen mit dem Geltungsbeginn der Datenschutz-Grundverordnung in Deutschland – in Kraft und werden das bisherige Bundesdatenschutzgesetz (BDSG a.F.) und die bisherigen Regelungen zum Sozialdatenschutz (SGB a.F.) zu diesem Zeitpunkt vollständig ersetzen.

Zu berücksichtigen ist aber auch die Änderung des § 203 StGB durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen. Mit dieser Änderung sollen die Möglichkeiten für Berufsgeheimnisträger erweitert werden, sich im Rahmen ihrer beruflichen oder dienstlichen Tätigkeit ohne (straf-)rechtliches Risiko der Mitwirkung dritter Personen zu bedienen.

Personenbezogene, anonyme und pseudonyme Daten

Die Verarbeitung von personenbezogenen Daten ist die Voraussetzung dafür, dass Datenschutzrecht anwendbar ist. Sind Daten nicht personenbezogen, greift Datenschutzrecht weder nach bisherigem noch nach zukünftigem Recht. Dementsprechend wichtig und umstritten ist der Begriff der personenbezogenen Daten.

Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, … identifiziert werden kann". Auch wenn sich der Wortlaut von § 3 Abs. 1 BDSG a.F. unterscheidet, ist anerkannt, dass das Datenschutzrecht in der Datenschutz-Grundverordnung, in der Datenschutz-Richtlinie und im Bundesdatenschutzgesetz den gleichen Begriff verwendet.

Entscheidend ist die Frage, wie eine Person indirekt identifiziert werden kann – vor allem, welches Zusatzwissen dritter Personen für diese Feststellung zu berücksichtigen ist. Ein absolutes Verständnis des Personenbezugs fordert, das gesamte (weltweit) theoretisch verfügbare Zusatzwissen zu berücksichtigen. Diese Forderung wird vor allem damit begründet, dass nicht ausgeschlossen werden kann, dass auch ursprünglich nicht beteiligte Dritte die Daten erhalten und mit den neuesten Techniken zuordnen können. Dagegen fordert ein relatives Verständnis des Personenbezugs, nur das Wissen zu berücksichtigen, das der Verantwortliche mit verhältnismäßigem Aufwand mobilisieren kann. Die Meinung wird vor allem damit begründet, dass das Datenschutzrecht den Verantwortlichen verpflichtet und daher auch nur auf seine Zuordnungsmöglichkeiten abstellen kann. Danach kann der Personenbezug relativ und von Verantwortlichem zu Verantwortlichem unterschiedlich sein. Die besseren Argumente sprechen für das relative Verständnis. Der Streit war schon immer fruchtlos und dürfte sich seit der Entscheidung des Europäischen Gerichtshofs vom 19. Oktober 2016, der das relative Verständnis ausdrücklich bestätigt hat, praktisch erledigt haben.

Wichtiger ist es, das Zusatzwissen, das der Verantwortliche nach allgemeinem Ermessen wahrscheinlich nutzen wird, für die praktischen Probleme des Datenschutzes aus einer Risikoprognose zu bestimmen. Danach sind alle relevanten objektiven Faktoren zu beachten: der zeitliche Aufwand, die finanziellen Mittel, verfügbare Technologien und technologische Entwicklungen sowie das Interesse an der Zuordnung und die Folgen für die betroffene Person. Die Prognose muss mindestens die Entwicklungsmöglichkeiten in dem Zeitraum berücksichtigen, für den die Daten verarbeitet werden sollen. Das Zusatzwissen Dritter ist dann relevant, wenn die Dritten die Daten vom Verantwortlichen erhalten (sollen) oder sich beschaffen (können), wenn sie mit dem Verantwortlichen in irgendeiner Weise zusammenarbeiten (können), um die Person zu identifizieren, oder wenn sie ihr Zusatzwissen auf andere Weise dem Verantwortlichen zur Verfügung stellen können oder müssen. Das Zusatzwissen Dritter ist aber nur zu berücksichtigen, soweit „nach allgemeinem Ermessen" im konkreten Fall mit seinem Einsatz zu rechnen ist. Dies ist nicht der Fall, wenn die Verwendung des Zusatzwissens gesetzlich verboten ist und keine Anhaltspunkte für einen Rechtsbruch vorliegen. Ebenso sind gesetzliche Zugriffskompetenzen staatlicher Behörden nur zu beachten, wenn es für deren konkrete Ausnutzung Hinweise gibt.

Anonyme Daten sind Angaben zu einer betroffenen Person, die ihr nicht zugeordnet werden können. Sie sind daher keine personenbezogenen Daten. Sie können von Anfang an anonym sein, aber auch aus personenbezogenen Daten entstehen, indem sie dadurch anonymisiert werden, dass aus ihnen alle potenziellen Zuordnungsmerkmale entfernt werden.

Anonyme Daten und Anonymisierung werden in keiner Vorschrift der Datenschutz-Grundverordnung genannt, aber in vielen Vorschriften als existent unterstellt und in Erwägungsgrund 26 Satz 5 und 6 DSGVO erwähnt. Das aus beiden Sätzen erkennbare Verständnis entspricht dem des § 3 Abs. 6 BDSG a.F.

§ 27 Abs. 3 BDSG-neu fordert eine Anonymisierung nur von besonderen Kategorien personenbezogener Daten, sobald dies nach dem Forschungszweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Diese Regelung verstößt insofern gegen die Datenschutz-Grundverordnung, als Art. 89 Abs. 1 Satz 4 DSGVO die Anonymisierung aller Forschungsdaten fordert und die Einschränkung wegen berechtigter Interessen der betroffenen Person nicht vorsieht. In beiden Fällen besteht ein Anwendungsvorrang der Verordnung.

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Anonymisierung vor. Vielmehr muss der Datenverarbeiter im Ergebnis die in Art. 4 Nr. 1 DSGVO niedergelegten Kriterien erfüllen, die eine Einordnung der Daten als personenbezogen ausschließen.

Pseudonymisierung wird – im Gegensatz zur Anonymisierung – in Art. 4 Nr. 5 DSGVO definiert. Die Bedeutung der Pseudonymisierung wird in der Datenschutz-Grundverordnung gegenüber dem bisherigen Datenschutzrecht deutlich erhöht. Dennoch ist der Begriff in Art. 4 Nr. 5 DSGVO mit dem in § 3 Abs. 6a BDSG a.F. identisch. Im Unterschied zur Anonymisierung gibt es bei der Pseudonymisierung eine Stelle, die eine Re-Identifizierung vornehmen kann. Daher ist zwischen dem Kenner der Zuordnungsregel und allen anderen, die die Zuordnungsregel nicht kennen, zu unterscheiden.

Von der Rechtsfolge her können in beiden Vorschriften zwei Arten von pseudonymen Daten unterschieden werden, je nachdem, ob sie die Zuordnung zu einer bestimmten Person für alle, die die Zuordnungsregel nicht kennen, ausschließen oder nur erschweren. Im ersten Fall, sind pseudonyme Daten keine personenbezogenen Daten, im zweiten Fall bleiben sie es. Nicht personenbezogen sind pseudonyme Daten nach dem Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016, wenn die Identifizierung der betroffenen Person gesetzlich verboten ist oder wenn die Identifizierung „praktisch nicht durchführbar" ist, „z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften" erfordert, sodass das Risiko einer Identifizierung de facto vernachlässigbar" ist. Für den Kenner der Zuordnungsregel sind die Daten immer personenbezogen.

Die Datenschutz-Grundverordnung gibt keine spezifischen Verfahren zur Pseudonymisierung vor. Sie erkennt jedoch die verwendeten Verfahren nur dann als Pseudonymisierung nach Art. 4 Nr. 5 DSGVO an, wenn sie zwei Voraussetzungen erfüllen. Sie müssen erstens die Daten so verarbeiten, dass sie „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können". Zweitens müssen die „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".

Eine wirksame Anonymisierung von Daten kann nicht als Umsetzung der Löschpflicht oder des Löschanspruchs nach Art. 17 Abs. 1 DSGVO angesehen werden, da beide unterschiedliche Wirkungen haben. Löschpflicht oder Löschanspruch entfallen jedoch nach Art. 17 Abs. 3 DSGVO. Im Fall der Forschung im öffentlichen Interesse besteht keine Löschpflicht und kein Löschanspruch, soweit voraussichtlich die Verwirklichung der Ziele der Datenverarbeitung unmöglich gemacht oder ernsthaft beeinträchtigt wird. Soweit die Ausnahme des Art. 17 Abs. 3 lit. d DSGVO greift, kann es sein, dass die Löschpflicht oder der Löschanspruch entfallen und an ihre Stelle eine Pflicht und ein Anspruch treten, die Daten zu anonymisieren. Weiterhin ist zu beachten, dass weder die Datenschutz-Grundverordnung noch Art. 17 Abs. 1 DSGVO für anonyme Daten gelten. Wenn die Daten anonymisiert sind, bevor der Löschanspruch oder die Löschpflicht entstehen, kommt die Datenschutz-Grundverordnung nicht zur Anwendung und es besteht weder eine Löschpflicht noch ein Löschanspruch.

Regelungen für wissenschaftliche Forschung

Die sprachliche Änderung von der Datenschutzrichtlinie zur Datenschutz-Grundverordnung hin zu „wissenschaftlichen Forschungszwecken" führt letztlich nicht zu einer Veränderung des rechtlichen Status quo. Vor dem Hintergrund der zunehmenden Verfügbarkeit von Big Data-Analysen ist die mit der Datenschutz-Grundverordnung vorgenommene Präzisierung dennoch grundsätzlich zu begrüßen. Ob sie tatsächlich tauglicher ist, einer unzulässigen Ausweitung des Wissenschaftsbegriffs die Grundlage zu entziehen und eine ungewollte Privilegierung von Big Data zu verhindern als die Vorgängerformulierung der Datenschutzrichtlinie, bleibt aber fragwürdig. Aus einer streng dogmatischen und verfassungsrechtlichen Sicht, ist Forschung ohnehin nur der Teil der Wissenschaft, der nicht Lehre und akademische Freiheit ist. Die „wissenschaftliche Forschung" wäre damit eine Tautologie und die Begrenzung auf „wissenschaftliche Forschungszwecke" würde letztlich lediglich „wissenschaftliche Lehrzwecke" ausschließen. Dies ist jedoch erkennbar nicht die Zielsetzung der Anpassung der Formulierung beim Wechsel von der Datenschutzrichtlinie zur Datenschutz-Grundverordnung. Immerhin leistet

die Formulierung „wissenschaftliche Forschungszwecke“ eine deklaratorische Klarstellung, dass nicht die bloße Anwendung wissenschaftlicher Methoden eine Privilegierung rechtfertigen kann; Forschung muss Primärziel der Verarbeitung personenbezogener Daten sein. Dies war indes aber bereits für die Vorgängerformulierung anerkannt. Die von Schneider[1] formulierten Kriterien behalten im Wesentlichen auch mit der Datenschutz-Grundverordnung ihre Gültigkeit. Eine Pflicht oder Absicht zur Veröffentlichung ist jedoch nicht zu fordern.

Bezogen auf § 27 BDSG-neu ist festzuhalten, dass sich der Gesetzgeber um eine Übernahme bestehender Regelungen aus dem alten Bundesdatenschutzgesetz bemüht hat. § 27 Abs. 3 BDSG-neu, der § 40 Abs. 2 und 3 BDSG a.F. überträgt, ist dabei jedoch insoweit unionsrechtswidrig, als er die Anforderung der Anonymisierung auf besondere Kategorien personenbezogener Daten beschränkt, statt sie wie Art. 89 Abs. 1 Satz 4 DSGVO auf alle Forschungsdaten zu erstrecken.

Abzuwarten bleibt die Anpassung der Landesdatenschutzgesetze und von Spezialgesetzen wie den Landeskrankenhausgesetzen an die Verordnung.

Ausschluss der Auskunftserteilung zum Wohl der betroffenen Person

Das Recht auf Auskunft in Art. 15 DSGVO ist im Wesentlichen deckungsgleich mit seinem Vorgänger aus der Datenschutzrichtlinie und seiner Umsetzung im Bundesdatenschutzgesetz. Es bildet die Basis für die Überprüfung der Rechtmäßigkeit der Verarbeitung durch den Betroffenen. Beschränkungen des Auskunftsrechts sind deshalb in besonderem Maße begründungsbedürftig. Beschränkungsmöglichkeiten für das Recht auf Auskunft enthält etwa § 27 Abs. 2 BDSG-neu.

Ein Ausschluss der Auskunftserteilung zum Wohl der betroffenen Person ist nach § 630g BGB möglich. Diese Vorschrift ist mit Art. 23 Abs. 1 lit. i DSGVO kompatibel. Dem Ausschluss sind dabei hohe Hürden gesetzt.

Auch im Kontext von wissenschaftlichen Forschungsvorhaben ist eine ähnliche Einschränkung – als Ultima Ratio ausgestaltet – grundsätzlich möglich. Diese müsste aber auf einer konkreten Rechtsvorschrift beruhen. Eine solche Rechtsvorschrift existiert derzeit nicht, könnte aber geschaffen werden. Die Beschränkung muss aber auf Art. 23 Abs. 1 DSGVO gestützt werden und kann nicht an der Bevorzugung der wissenschaftlichen Forschung durch die Grundverordnung teilhaben. Unabhängig davon kann das Auskunftsrecht aber auch im Kontext wissenschaftlicher Forschung durch Individualvereinbarung ausgeschlossen werden.

1 U.K. Schneider, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, TMF-Reihe, Band 12, Seite 97/98

Weitergabe von Informationen an „mitwirkende Personen" im Rahmen der medizinischen Forschung

Strafbar macht sich nach § 203 StGB, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Berufsgeheimnisträger im Sinne von Abs. 1 und 2 anvertraut worden oder sonst bekannt geworden ist. Die zunehmende Nutzung von Informationstechnik macht es häufig aber erforderlich, externe Fachkräfte hinzuzuziehen, die außerhalb der Sphäre des Berufsgeheimnisträgers stehen, beispielsweise zur Wartung der eingesetzten Technik. Dabei können diesen Personen jedoch fremde Geheimnisse offenbart werden. Zudem wird zunehmend die eigene Informationstechnik durch externe Technik ergänzt, beispielsweise in Form des Cloud Computing. Aufgrund zahlreicher Meinungsverschiedenheiten in der strafrechtlichen Fachliteratur zu § 203 StGB und fehlender obergerichtlicher Rechtsprechung zum Thema Outsourcing bestand hier eine große Rechtsunsicherheit. Die Änderung des § 203 StGB schafft nun ein deutliches Mehr an Rechtsklarheit.

Der Begriff der „mitwirkenden Person" wird mit der Novelle des § 203 StGB neu in das Strafgesetzbuch eingeführt. Er ist ein Überbegriff und umfasst einerseits den berufsmäßig tätigen Gehilfen und die beim Berufsgeheimnisträger zur Vorbereitung auf den Beruf tätigen Personen und andererseits die sonstigen mitwirkenden Personen. Wesentliches Unterscheidungsmerkmal zwischen dem Gehilfen und der sonstigen mitwirkenden Person ist dabei die fehlende Teilhabe an der Sphäre des Berufsgeheimnisträgers.

Die Forschungstätigkeit des Arztes ist als berufliche Tätigkeit im Sinne von § 203 StGB zu werten. Entscheidend ist dabei, dass der Arzt „als Arzt" forscht. Unterschiede zwischen der ärztlichen Tätigkeit in einem Universitätskrankenhaus, einem sonstigen Krankenhaus und einer Arztpraxis bestehen im Ergebnis nicht. In allen Fällen ist die Forschungstätigkeit des Arztes seiner beruflichen Tätigkeit zuzurechnen und deshalb tatbestandlich im Sinn von § 203 StGB. Nicht als Teil der beruflichen Tätigkeit kann lediglich Forschung gelten, die eine andersartige Nebentätigkeit darstellt. Davon dürfte nur auszugehen sein, wenn der Arzt nicht im medizinischen Kontext forscht. Damit ist die Mitwirkung an der Forschungstätigkeit eines Arztes eine Mitwirkungshandlung im Sinn von § 203 StGB. Die mitwirkende Person unterliegt dabei selbst der Strafbarkeit nach § 203 StGB.

1 Fragestellungen des Gutachtens

Das Gutachten soll Rechtsfragen zur Nutzung von Sozial- und Gesundheitsdaten beantworten, die für das Forschungsprojekt „Smart Analysis – Health Research Access“ (SAHRA) von Bedeutung sind. Das Projekt SAHRA wird vom Bundesministerium für Wirtschaft und Energie gefördert. Hauptziel des SAHRA-Projekts ist es, Sozialdaten der AOK Nordost über eine hochsichere web-basierte Datenplattform (SAHRA-Plattform) mit weiteren Datenquellen des Gesundheitswesens zu verbinden. Die Datenplattform soll datenschutzkonforme Möglichkeiten bieten, Abrechnungs-, Behandlungs-, Struktur- sowie Register- und Studiendaten aus verschiedenen Quellen zu kombinieren, zu referenzieren und zu validieren. Die potenziellen Nutzer der SAHRA-Plattform sollen aus der Wissenschaft, der Versorgung und der Industrie stammen.

Durch die grundlegende Änderung des Rechtsrahmens durch die Datenschutz-Grundverordnung der Europäischen Union und die Anpassung mehrerer deutscher Datenschutzregelungen an die neue Rechtslage stellen sich viele grundsätzliche datenschutzrechtliche Fragestellungen in einem neuen Licht. Vor diesem Hintergrund soll in dem Gutachten untersucht werden, wie die folgenden Fragen[2] nach der zukünftigen Rechtslage, die ab dem 25. Mai 2018 gelten wird, zu beurteilen sind:

2 Der vollständige Fragenkatalog findet sich im Anhang.

- Unterstützt die Datenschutz-Grundverordnung eher das Konzept eines „absoluten" oder eines „relativen Personenbezugs"?
- Wird der Begriff der Pseudonymisierung in der Datenschutzgrundverordnung in einer anderen Weise verstanden als in den Vorschriften des Bundesdatenschutzgesetzes und welche Unterschiede folgen daraus, insbesondere für den Prozess der Pseudonymisierung? Welche Bedeutung hat in Bezug auf die bisherige Rechtslage bei der Nutzung pseudonymer Daten das Urteil des Europäischen Gerichtshofs vom 19.10.2016, C – 582/14 (Breyer)?
- Wird der Begriff des Anonymisierens in Erwägungsgrund 26 der Datenschutz-Grundverordnung in einer anderen Weise verstanden als in der bisherigen Definition des Bundesdatenschutzgesetzes und welche Unterschiede folgen daraus bei der Nutzung anonymer Daten für die wissenschaftliche Forschung?
- Kann eine wirksame Anonymisierung von Daten als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 DSGVO angesehen werden? Ist es für eine wirksame Anonymisierung ausreichend, wenn die Löschung im Rahmen einer Einwilligung vereinbart wurde?
- Führt der Begriff der „wissenschaftlichen Forschungszwecke", wie er in Erwägungsgrund 159 DSGVO verwendet wird, zu einer anderen Interpretation des Begriffs „wissenschaftliche Forschung", als dies bisher der Fall war? Wie verhält sich der neue Rechtsbegriff zu der Rechtsauffassung von Schneider in der TMF-Veröffentlichung von U.K. Schneider, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, Band 12, Seite 97/98?
- Der Bundesrat hat in seinem Beschluss vom 10. März 2017 zum Entwurf der Bundesregierung zu einem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)[3] die Frage aufgeworfen, inwieweit ein Ausschluss der Auskunftserteilung neben den in § 27 BDSG-E genannten Voraussetzungen nach objektiven Kriterien auch aus therapeutischen sowie ethischen Erwägungsgründen zum Wohl der betroffenen Person möglich sein sollte. Auf welcher verfassungs- und europarechtlichen Grundlage können solche Ausnahmen von den Auskunftsrechten für wissenschaftliche Forschungsvorhaben vorgenommen werden?
- § 203 StGB wurde durch das vom Bundestag am 29. Juni 2017 beschlossene Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen in der Form geändert, dass die Weitergabe von Informationen an „mitwirkende Personen" für einen Berufsgeheimnisträger (z.B. Arzt) straflos sein soll, wenn diese an der „beruflichen Tätigkeit" des Berufsge-

3 BT-Drs. 18/11655, 25, Ziff. 27 lit. d.

heimnisträgers mitwirken. Kann eine Mitwirkung an einer Forschungstätigkeit eines Arztes auch als Mitwirkungshandlung im Sinn der neuen Rechtsvorschrift verstanden werden? Wie wird die „berufliche Tätigkeit“ eines Arztes in der Datenschutz-Grundverordnung im Vergleich zum bisherigen Rechtsrahmen definiert? Gibt es Unterschiede zwischen der ärztlichen Tätigkeit in einem Universitätskrankenhaus, in einem sonstigen Krankenhaus und einer Arztpraxis.

Für alle Fragen soll auch geprüft werden, ob die einschlägigen deutschen Umsetzungsgesetze die Vorgaben aus dem europäischen Primärrecht, dem deutschen Verfassungsrecht und aus der Datenschutz-Grundverordnung einhalten.

2 Der neue Rechtsrahmen

Die Datenschutz-Grundverordnung vom 27. April 2016 wird ab dem 25. Mai 2018 in allen Mitgliedstaaten unmittelbar gelten und in diesen das Datenschutzrecht auf eine neue Grundlage stellen. Die Datenschutz-Grundverordnung wird dann Teil der jeweiligen nationalen Rechtsordnung sein, ohne diese aber formell zu verändern.

2.1 Datenschutz-Grundverordnung

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)[4] gilt vom 25. Mai 2018 an mit all ihren Regelungen in allen Mitgliedstaaten unmittelbar. Sie bestimmt vorrangig das künftige Datenschutzrecht in Europa. Dieses wird aber nicht allein durch die Union geprägt. Vielmehr wird sie in vielen Bereichen und Aspekten ergänzt durch Datenschutzregelungen der Mitgliedstaaten. Dadurch entsteht im Datenschutz eine Ko-Regulierung durch Union und Mitgliedstaaten. Erst das komplizierte Zusammenwirken von Unionsrecht und Recht der Mitglied-

4 EU ABl. L 119 vom 4.5.2016, 1.

staaten bewirkt das zukünftige Europäische Datenschutzrecht.[5] Dies widerspricht zwar vielen Erwartungen und Wünschen nach einem einfachen und einheitlichen Datenschutzrecht in der Union,[6] ist aber – nüchtern betrachtet – das Ergebnis des politischen Prozesses, der die Datenschutz-Grundverordnung hervorgebracht hat.[7]

Die Verordnung verfolgt drei Zielsetzungen:[8] Zum einen will sie den Datenschutz angesichts der Herausforderungen der technischen Entwicklung modernisieren und den Schutz der Grundrechte verbessern.[9] Zum anderen will sie das Datenschutzrecht unionsweit harmonisieren und einen soliden, „kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union" schaffen.[10] Schließlich will sie einheitliche Vorgaben für gleiche wirtschaftliche Bedingungen in der Union bieten und damit den Binnenmarkt stärken.[11]

Die Datenschutz-Grundverordnung regelt das von ihr erfasste Datenschutzrecht in elf Kapiteln mit 99 Artikeln. Kapitel I enthält in den Art. 1 bis 4 allgemeine Bestimmungen, Kapitel II nennt in Art. 5 bis 10 die allgemeinen Grundsätze des Datenschutzrechts, Kapitel III regelt in den Art. 11 bis 23 die Rechte der betroffenen Person, Kapitel IV bestimmt in Art. 24 bis 43 die Pflichten des Verantwortlichen und des Auftragsverarbeiters und Kapitel V beschreibt in Art. 44 bis 50 die Vorgaben zur Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen. Nimmt man zu diesen Vorschriften noch die Regelung zur Haftung der Datenverarbeiter in Art. 82 hinzu, so regelt die Datenschutz-Grundverordnung das materielle Datenschutzrecht in nur 51 Artikeln. Die verbleibenden 48 Artikel beantworten überwiegend organisatorische Fragen der Datenschutzaufsicht und der Regelungskompetenzen und betreffen weitere formelle Themen. In Kapitel VI regelt die Verordnung in den Art. 51 bis 59 die Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, in Kapitel VII enthält sie in Art. 60 bis 76 Vorgaben zur Zusammenarbeit und zur Kohärenz der Entscheidungen der Aufsichtsbehörden und in Kapitel VIII regelt sie in Art. 77 bis 84 Rechtsbehelfe und Sanktionen. Kapitel IX enthält in Art. 85 bis 91 Vorschriften für besondere Datenverarbeitungssituationen, Kapitel X gibt in Art. 92 und 93 Vorgaben für delegierte Rechtsakte und Durchführungsrechtsakte und Kapitel XI enthält in Art. 94 bis 99 Schlussbestimmungen.

5 S. näher *Roßnagel*, in: ders. 2018, § 1 Rn. 1ff.
6 Insbesondere von am Entstehungsprozess Beteiligten – s. z.B. *Selmayr/Ehmann*, in: Ehmann/Selmayr 2017, Einleitung Rn. 3; *Albrecht*, CR 2016, 97ff.
7 S. zu diesem ausführlich *Roßnagel*, in: ders. 2018, § 1 Rn. 15ff.
8 Diese werden weitgehend verfehlt – s. *Roßnagel*, in: ders. 2017, § 1 Rn. 27ff.
9 S. hierzu Erwägungsgrund 1, 2, 3a und 5 DSGVO.
10 S. hierzu Erwägungsgrund 3 und 6 DSGVO.
11 S. Erwägungsgrund 4 und 8 DSGVO.

Die neue Verordnung orientiert sich in weiten Teilen weiterhin an den alten Zielen und Grundsätzen der Datenschutzrichtlinie 95/46/EG[12] von 1995.[13] Sie übernimmt unter anderem in Art. 2 und 3 DSGVO weitgehend die Regelungen zum sachlichen und räumlichen Anwendungsbereich, in Art. 5 DSGVO nahezu unverändert die Grundsätze der Datenverarbeitung, in Art. 6 Abs. 1 DSGVO wörtlich die Voraussetzungen für die Zulässigkeit der Datenverarbeitung und in Art. 9 DSGVO grundsätzlich die Regelungen zu besonderen Kategorien personenbezogener Daten. Hinsichtlich der Rechte der betroffenen Person orientiert sie sich in den Art. 12 bis 23 DSGVO ebenfalls stark an der Richtlinie. In Art. 26 und 27 DSGVO greift die Verordnung grundsätzlich auf die Vorgaben der Richtlinie zur Auftragsverarbeitung zurück. In Art. 32 DSGVO übernimmt sie weitgehend die Anforderungen an die Datensicherheit, in Art. 44 bis 50 DSGVO konzeptionell die Grundsätze zur Datenübermittlung in Drittländer und in Art. 51 bis 59 DSGVO die Konzeption der Stellung und Aufgaben der Aufsichtsbehörden. Diese Regelungen werden in der Verordnung präzisiert, neugestaltet oder erweitert, aber konzeptionell nicht weiterentwickelt.

Innovativ ist dagegen in Art. 3 Abs. 2 DSGVO die Ausweitung des räumlichen Anwendungsbereichs durch das Marktortprinzip. Danach ist die Verordnung auch anwendbar, wenn ein Datenverarbeiter personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten. Dies gilt allerdings nur, wenn der Verarbeiter entweder der betroffenen Person Waren oder Dienstleistungen anbietet oder die Datenverarbeitung der Beobachtung ihres Verhaltens in der Europäischen Union dient.[14] Bisher unbekannt ist das Recht für betroffene Personen in Art. 20 DSGVO, ihre Daten, die sie einem Verantwortlichen bereitgestellt haben, auf einen anderen Datenverarbeiter zu übertragen. Innovativ sind auch die Anforderungen an den Datenschutz durch Systemgestaltung und Voreinstellungen in Art. 25 DSGVO und die Datenschutz-Folgenabschätzung in Art. 35 DSGVO. Die engere Zusammenarbeit der Aufsichtsbehörden in der Union erforderte in Art. 60 bis 76 DSGVO eigene Regelungen zu deren Durchführung. Eine auffällige Veränderung bringt auch Art. 83 DSGVO, der für Verstöße gegen Vorgaben der Verordnung drastische Sanktionen ermöglicht. Nach Art. 83 Abs. 5 DSGVO können bei den dort aufgelisteten Verstößen Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist.[15]

12 EG ABl. L 281 vom 23.11.1995, 31.

13 S. Erwägungsgrund 9 DSGVO.

14 Diese Erweiterung sorgt auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union und vereinfacht die Wahrnehmung von Betroffenenrechten.

15 S. z.B. *BfDI* 2016, 18ff.

2.2 Das neue Bundesdatenschutzgesetz

Nationales Datenschutzrecht kann neben der Datenschutz-Grundverordnung mindestens aus drei Gründen anwendbar sein. Es kann erstens eine explizite oder implizite **Öffnungsklausel** der Datenschutz-Grundverordnung ausfüllen, die den Mitgliedstaaten einen Spielraum einräumt, Regelungen, die die Verordnung nicht enthält, weiterhin anzuwenden oder neu zu erlassen. Es kann weiterhin abstrakte Vorgaben der Datenschutz-Grundverordnung **präzisieren** und damit Handlungs- und Bewertungsmaßstäbe bieten, die der Verordnung fehlen, sofern sie nicht Entscheidungen der Verordnung widersprechen. Schließlich kann das nationale Datenschutzrecht Vorgaben der Verordnung **konkretisieren**, die eine unfertige Regelung im Text der Verordnung erst anwendbar machen. Dies ist meist dann der Fall, wenn ursprünglich eine Konkretisierung der Verordnung durch delegierte Rechtsakte oder Durchführungsrechtsakte der Kommission vorgesehen waren, diese Konkretisierungsmöglichkeiten aber entfallen sind.[16]

Die in der Verordnung gegebenen Möglichkeiten hat der deutsche Gesetzgeber inzwischen genutzt und noch in der 18. Legislaturperiode des Deutschen Bundestags ergänzend zur Datenschutz-Grundverordnung mehrere neue Datenschutzgesetze erlassen oder bestehende Gesetze angepasst, darunter ein neues Bundesdatenschutzgesetz und eine Neufassung des Sozialdatenschutzes im Sozialgesetzbuch I und X.

In Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017[17] ist das neue Bundesdatenschutzgesetz enthalten. Dieses tritt mit am 25. Mai 2018 – zusammen mit dem Geltungsbeginn der Datenschutz-Grundverordnung in Deutschland – in Kraft und wird das bisherige Bundesdatenschutzgesetz zu diesem Zeitpunkt vollständig ersetzen. Art. 2 bis 6 DSAnpUG-EU enthalten Anpassungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des Artikel-10-Gesetzes.

Das neue Bundesdatenschutzgesetz regelt nur im zweiten Teil in §§ 22 bis 44 allein die Anpassung des allgemeinen Bundesdatenschutzrechts an die Datenschutz-Grundverordnung. Er enthält Vorgaben für besondere Verarbeitungssituationen, für zulässige Zweckänderungen und für Einschränkungen der Rechte der betroffenen Personen. Im dritten Teil finden sich in §§ 45 bis 84 spezifische Bestimmungen zur Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie

16 S. hierzu *Roßnagel*, in: ders. 2018, § 2 Rn. 15ff.
17 BGBl. I, 2097.

zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie).[18] Der ersten Teil schließlich enthält in §§ 1 bis 21 Regelungen, die sowohl für die Anpassung an die Verordnung als auch der Umsetzung der JI-Richtlinie gelten. Sie betreffen u.a. allgemeine Erlaubnistatbestände sowie die Stellung und die Aufgaben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Mit dem neuen Bundesdatenschutzgesetz hat der deutsche Gesetzgeber die Öffnungsklauseln der Verordnung – insbesondere in Art. 6, 9, 22 und 23 DSGVO – ausgenutzt und darüber hinaus auch ohne Öffnungsklausel die Regelungen in der Verordnung präzisiert, konkretisiert und ergänzt.[19] Er hat diese Kompetenzen aber fast ausschließlich dazu benutzt, alte Definitionen beizubehalten, Möglichkeiten zur Verarbeitung personenbezogener Daten zu erweitern und Rechte der betroffenen Personen zu beschränken.[20]

2.3 Änderungen des SGB I und X

Eine Neuregelung des Sozialdatenschutzes erfolgte durch Art. 19 und 24 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 24. Juli 2017.[21] Der Gesetzgeber stützt sie durchgängig – ohne weitere Differenzierung – auf die Öffnungsklauseln für den öffentlichen Bereich in Art. 6 Abs. 2 und 3 sowie auf die Öffnungsklausel zur Verarbeitung besonderer Kategorien von personenbezogenen Daten in Art. 9 Abs. 2 DSGVO.[22] Neugefasst wurden die Regelung des Sozialgeheimnisses in § 35 SGB I, die Definitionen in § 67 SGB X und die Erlaubnistatbestände in §§ 67a ff. SGB X.

Hinsichtlich des Verhältnisses der Neuregelungen des Sozialdatenschutzes zur Datenschutz-Grundverordnung ist die amtliche Begründung widersprüchlich. Einerseits geht sie davon aus, dass „die datenschutzrechtlichen Regelungen des Sozialdatenschutzes … das bereichsspezifische Datenschutzrecht abschließend regeln". Andererseits nimmt sie an, dass die Verordnung unmittelbare Geltung habe und künftig unmittelbar neben den Regelungen zum Sozialdatenschutz anzuwenden sei.[23] Die Öffnungsklauseln des Art. 6 Abs. 2 und 3 DSGVO sollen jedoch gerade dazu dienen, gewachsene hochkomplexe Datenschutzregelungen, wie sie für die Systeme der sozialen Sicherheit bestehen, die spezifische Eigenheiten der Mitgliedstaaten betreffen, beibehalten zu können.[24] Daher kann auch der deutsche Regelungskomplex des Sozialdatenschutzes als ein in sich abgeschlossenes System beibehalten werden.

18 Richtlinie (EU) 2016/680, EU ABl. 119 vom 4.5.2016, 89.
19 S. hierzu auch *Roßnagel*, DuD 2017, 277; *Geminn*, DuD 2017, 295 (297f.); *Johannes/Richter*, DuD 2017, 300ff.
20 S. *Greve*, NVwZ 2017, 737; *Kühling*, NJW 2017, 1985; *Roßnagel*, DuD 2017, 277 (281).
21 BGBl. I, 2541.
22 Amtliche Begründung, BT-Drs. 18/12611, 104f., 110ff.
23 BT-Drs. 18/12611, 105.
24 S. hierzu *Roßnagel*, DuD 2017, 290 (291f.).

2.4 Änderungen des § 203 StGB

Unabhängig von der Datenschutz-Grundverordnung hat das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017[25] in Art. 1 das Strafgesetzbuch geändert. Die wichtigste Änderung ist die Aufhebung von § 203 Abs. 2a StGB a.F. und die Ersetzung von § 203 Abs. 3 StGB a.F. durch § 203 Abs. 3 und 4 StGB n.F. Damit zielt der Gesetzgeber darauf ab, „die Möglichkeiten für Berufsgeheimnisträger zu erweitern, sich im Rahmen ihrer beruflichen oder dienstlichen Tätigkeit ohne (straf-)rechtliches Risiko der Mitwirkung dritter Personen zu bedienen".[26]

Ergänzend nimmt das Gesetz Änderungen in der Strafprozessordnung in Art. 2, der Bundesrechtsanwaltsordnung in Art. 3, der Bundesnotarordnung in Art. 4, der Patentanwaltsordnung in Art. 5, im Steuerberatungsgesetz in Art. 8 und in der Wirtschaftsprüferordnung in Art. 9 und in vielen weiteren Gesetzen als Folgeänderungen in Art. 10 vor. Diese weiteren Artikel enthalten überwiegend Regelungen zur Inanspruchnahme von Dienstleistungen. Die teilweise schon satzungsrechtlich bestehende Pflicht für bestimmte Berufsgeheimnisträger, ihre Mitarbeiter zur Verschwiegenheit zu verpflichten, wird in die entsprechenden Gesetze überführt.

25 BGBl. I, 3618.
26 BT-Drs. 18/12940, 1; 18/11936, 17.

3 Personenbezogene Daten

Sowohl Art. 1 Abs. 1 DSGVO und Art. 1 Abs. 1 DSRL als auch § 1 Abs. 1 BDSG in der neuen und der alten Fassung wie auch § 35 SGB I i.V.m. § 67 Abs. 1 SGB X a.F. sowie § 67 Abs. 2 SGB X n.F. nennen als Regelungsgegenstand des Datenschutzrechts die Verarbeitung von personenbezogenen Daten. Sind die Daten nicht personenbezogen, greifen die Datenschutzregeln nicht.

3.1 Personenbezug

Kapitel 3.1 beantwortet die Frage 4.1 Satz 4. Diese lautet:

> *Von Interesse ist hier, ob die EU-DSGVO eher das Konzept eines „absoluten" oder eines „relativen Personenbezugs" unterstützt.*

Ohne zu klären, wie sich der Begriff des Personenbezugs bestimmt, lassen sich keine sinnvollen Aussagen zu anonymen und pseudonymen Daten treffen. Die Antwort auf die Frage 4.1 Satz 4 ist daher grundlegend für die Antworten zu den Fragen 4.1, 4.3 und 4.4 und wird daher vor der Beantwortung dieser Fragen im Folgenden gesondert erarbeitet.

Aufgrund des Anwendungsvorrangs der Datenschutz-Grundverordnung ist die Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO entscheidend:

Danach sind personenbezogene Daten

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person') beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann".*

Die Datenschutz-Grundverordnung führt damit weitgehend die Definition des Art. 2 lit. a) DSRL fort. Diese lautet:

> *„Im Sinne dieser Richtlinie bezeichnet der Ausdruck ‚personenbezogene Daten' alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person'); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind".*

Der Unterschied besteht nur in der Ersetzung der Worte „bestimmt oder bestimmbar" durch die Worte „identifiziert oder identifizierbar" und der Ergänzung der Beispiele um „Namen", „Standortdaten" und „Online-Kennung" sowie der Identitäten um die „genetische" Identität.

Der Unterschied zwischen „bestimmt oder bestimmbar" und „identifiziert oder identifizierbar" betrifft nur die jeweils deutschen Übersetzungen des englischen „identified or identifiable". In der englischen Fassung des Art. 2 lit. a) DSRL und des Art. 4 Nr. 1 DSGVO heißt es übereinstimmend „identified or identifiable". In dieser Hinsicht sind also die Datenschutz-Grundverordnung und die Datenschutz-Richtlinie identisch.[27] In der deutschen Fassung wurden diese Worte 1995 mit den Worten „bestimmt oder bestimmbar" und 2017 durch die Worte „identifiziert oder identifizierbar" übersetzt. Die zusätzlichen Beispiele in Art. 4 Nr. 1 DSGVO gelten auch für Art. 2 lit. a) DSRL,[28] ebenso wie die „genetische" Identität auch von Art. 2 lit. a) DSRL erfasst ist. Sie werden nun in Art. 4 Nr. 1 DSGVO explizit im Verordnungstext genannt.

Aus alledem ist davon auszugehen, dass die Definitionen in Art. 4 Nr. 1 DSGVO und Art. 2 lit. a) DSRL in den wesentlichen Merkmalen[29] inhaltlich identisch

27 Ebenso *Laue/Nink/Kremer 2016*, § 1 Rn. 12; *Herbst*, NVwZ 2016, 902 (903): nur unwesentliche Abweichungen.
28 S. z.B. *Laue/Nink/Kremer* 2016, § 1 Rn. 14.
29 Insbesondere wurde nach dem bisher geltenden Datenschutzrecht keine namentliche Identifizierung verlangt – s. z.B. Art. 29 Datenschutzgruppe, WP 136, 14; *Dammann*, in: Simitis, BDSG, § 3 Rn. 22.

sind.[30] Insbesondere hinsichtlich des Merkmals „bestimmt oder bestimmbar" und „identifiziert oder identifizierbar" stimmen sie überein. Da die gleichlautenden Definitionen der personenbezogenen Daten in § 3 Abs. 1 BDSG a.F. und § 67 Abs. 1 SGB X die Definition in Art. 2 lit. a) DSRL umsetzen, ist ihnen trotz eines etwas anderen Wortlauts – unionsrechtskonform – der gleiche Begriff der personenbezogenen Daten zu unterlegen wie in Art. 2 lit. a) DSRL. Zwar darf das Unionsrecht nicht aus dem Blickwinkel des Rechtsverständnisses eines Mitgliedstaats ausgelegt werden.[31] Doch können die Auslegungserkenntnisse zur Datenschutz-Richtlinie auf die Datenschutz-Grundverordnung übertragen werden, die ihre Kontinuität zu dieser Richtlinie ausdrücklich in ihrem Erwägungsgrund 9 betont. Aber auch Literatur und Rechtsprechung zur Definition der personenbezogenen Daten in § 3 Abs. 1 BDSG a.F. und § 67 Abs. 1 SGB X a.F., die die Definition in Art. 2 lit. a) DSRL umsetzen, können trotz eines etwas anderen Wortlauts zum Verständnis des Art. 4 Nr. 1 DSGVO herangezogen werden,[32] wenn der besondere unionsrechtliche Zusammenhang beachtet wird. Dies wird im Folgenden ergänzend zur einschlägigen Literatur und Rechtsprechung zur Datenschutz-Grundverordnung auch geschehen.

3.1.1 Bedeutung des Personenbezugs

Das Datenschutzrecht geht davon aus, dass von einer Datenverarbeitung Risiken für das Grundrecht auf den Datenschutz nach Art. 8 GRCh und für das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nur dann ausgehen können, wenn die Daten mit einer bestimmten Person in Verbindung gebracht werden können.[33] Daher greift das Datenschutzrecht als Gefahrenabwehrrecht erst und nur dann, wenn die zu verarbeitenden Daten einen Personenbezug haben und damit auf eine bestimmte Person verweisen.[34] Aus diesem Grund ist der Personenbezug der zu verarbeitenden Daten der zentrale Begriff, der über die Anwendung des Datenschutzrechts entscheidet.

Der Personenbezug der Daten ist entscheidend für den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung, aber auch der anderen genannten Datenschutzregelungen. Werden personenbezogene Daten verarbeitet, gilt auch der persönliche und räumliche Anwendungsbereich. Die Vorschriften der Datenschutz-Grundverordnung gelten dann für alle Verantwortlichen und Auftragsverarbeiter. Nach den Legaldefinitionen in Art. 4 Nr. 7

30 S. auch *Laue/Nink/Kremer 2016*, § 1 Rn. 13; *Karg*, DuD 2015, 520 (521); *Brink/Eckhardt*, ZD 2015, 205; *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 2; *Klabunde*, in: Ehmann/Selmayr, Art. 4 Rn. 6; *Ernst*, in: Paal/Pauly, Art. 4 Rn. 3; *Ziebarth*, in: Sydow, Art. 4 Rn. 7; *Krügel*, ZD 2017, 455 (455f.).

31 S. genau für diese Frage *Hofmann/Johannes*, ZD 2017, 221f. m.w.N.

32 S. z.B. *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 20.

33 S. hierzu kritisch *Roßnagel/Scholz*, MMR 2000, 721 (727f.); *Roßnagel* 2007, 185ff.

34 Zur Notwendigkeit, die Gefahrenabwehr um eine Risikovorsorge zu ergänzen s. z.B. *Roßnagel/Geminn/Jandt/Richter* 2016, 125f., 137.

und 8 DSGVO sind dann alle natürlichen oder juristischen Personen, die personenbezogene Daten allein oder im Auftrag verarbeiten, Adressaten der Datenschutzregelungen. Es wird nach Art. 3 DSGVO jede Datenverarbeitung von den Datenschutzregelungen erfasst, die im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt oder die in Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten in der Union zu beobachten.

Nur wenn personenbezogene Daten verarbeitet werden, gelten die datenschutzrechtlichen Grundsätze der Datenverarbeitung nach Art. 5 DSGVO. Nur bei Personenbezug der Daten ist eine Legitimation für die Verarbeitung der Daten erforderlich, die entweder in einer Einwilligung der betroffenen Person oder in einer gesetzlichen Erlaubnis zur Datenverarbeitung liegen kann. Nur wenn ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten verarbeitet, gelten für sie die spezifischen datenschutzrechtlichen Pflichten.[35] Nur bei einem Bezug der Daten auf die betroffene Person kann diese ihre Rechte und Rechtsbehelfe geltend machen. Nur die Verarbeitungen von personenbezogenen Daten unterliegen der Aufsicht durch die zuständige Aufsichtsbehörde und begründen deren Aufgaben und Befugnisse.[36] Nur wenn personenbezogene Daten verarbeitet werden, kann ein Verstoß gegen datenschutzrechtliche Pflichten die drakonischen Sanktionen der Datenschutz-Grundverordnung auslösen.[37]

Entscheidend dafür, ob alle diese Rechte und Pflichten, Aufgaben und Befugnisse gelten, ist der Personenbezug der verarbeiteten Daten. Nur die mit ihnen verbundenen Risiken begründen die Notwendigkeit, den Verantwortlichen und die Auftragsverarbeiter den Regelungen des Datenschutzrechts zu unterwerfen.

3.1.2 Identifizierung durch Daten

Nach Art. 4 Nr. 1 DSGVO sind Daten personenbezogen, wenn die Informationen, die den Daten entnommen werden können, „sich auf eine identifizierte oder identifizierbare natürliche Person" beziehen.[38] Von einer Identifikation ist auszugehen, wenn diese sich aus den Daten selbst ergibt.[39] Wann eine Person im Sinn des Art. 4 Nr. 1 DSGVO „*identifiziert*" ist, wird in der Verordnung nicht erläutert. Eine natürliche Person ist identifiziert, wenn sie sich von anderen Personen einer Gruppe ohne Weiteres eindeutig unterscheiden lässt.[40] Wichtig ist, dass feststeht, dass sich die Daten auf diese und nicht auf eine

35 S. auch *Hofmann/Johannes*, ZD 2017, 221 (222).
36 S. z.B. Roßnagel, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 41ff.
37 S. auch *Hofmann/Johannes*, ZD 2017, 221 (222).
38 S. z.B. *Klar/Kühling,* in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 18.
39 S. z.B. *Klar/Kühling,* in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 18.
40 Art. 29-Datenschutzgruppe, WP 136, 14; *Buchner*, in: Taeger/Gabel, § 3 Rn. 9.

andere Person beziehen. Die Identifikation kann über eindeutige Merkmale, wie den Namen, erfolgen. Sie kann aber auch – ohne dass der Name bekannt ist[41] – allein durch bestimmte Merkmale von allen anderen Personen der relevanten Gruppe unterschieden und damit individualisiert werden.[42] Im Ergebnis ist eine Person als identifiziert anzusehen, wenn ausreichende Informationen (gemeinsam) vorliegen, die zu einer eindeutigen Identifikation notwendig sind.[43] Wie Erwägungsgrund 26 DSGVO deutlich macht, spielt es keine Rolle, durch welche Mittel diese eindeutige Zuordnung erreicht wurde. Dies kann auch durch Aussondern erfolgen.[44]

Eine natürliche Person ist *identifizierbar*, wenn sie gemäß Art. 4 Nr. 1 DSGVO und Art. 2a) DSRL „direkt oder indirekt identifiziert werden kann". Es genügt die Möglichkeit.[45] Diese kann sich etwa aus der „Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen" ergeben. Diese besonderen Merkmale können die Identifizierung einer Person ermöglichen, weil sie „Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind". Ob der Schluss von den bekannten besonderen Merkmalen auf die Identität der Person möglich ist, hängt von dem verfügbaren „Zusatzwissen" ab, das eine Verbindung von den bekannten Daten zu der spezifischen Person herstellen kann.[46] Eine Person ist somit mit Hilfe der bekannten Daten identifizierbar, wenn weitere Kenntnisse verfügbar sind, die einen Schluss von den Daten zu einer eindeutig unterscheidbaren Person ermöglichen.[47]

Wenn für die Identifizierbarkeit einer bestimmten Person durch ein Datum oder mehrere Daten das Zusatzwissen entscheidend ist, das den Schluss von den Daten zu der identifizierten Person zulässt, stellt sich die Frage, auf wessen Zusatzwissen abzustellen ist. Zu dieser Frage gibt es unterschiedliche Antworten, je nachdem, ob man sie mit Blick auf die Daten, um die es geht, oder mit Blick auf den Verantwortlichen, der die Daten verarbeitet, beantwortet. In der Literatur wird hierzu ein Meinungsstreit ausgemacht, der dadurch bestimmt ist, ob das Konzept eines „absoluten Personenbezugs" oder das Konzept eines „relativen Personenbezugs" verfolgt wird.[48]

41 S. *Husemann*, in: Roßnagel 2018, § 3 Rn. 6; *Karg*, DuD 2015, 520 (523); für die DSRL Art. 29-Datenschutzgruppe, WP 136, 14.

42 S. z.B. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 22 – Breyer; Art. 29-Datenschutzgruppe, WP 136, 14.

43 S. *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 20; *Karg*, ZD 2012, 257.

44 Erwägungsgrund 26 Satz 3.

45 Wie diese bestimmt wird, wird im Folgenden in der Auseinandersetzung mit der „absoluten" und der „relativen" Konzeption der Bestimmung des Personenbezugs ausführlich dargestellt.

46 *Damann*, in: Simitis, § 3 Rn. 26; *Roßnagel/Scholz*, MMR 2000, 723; *Roßnagel*, digma 2011, 161.

47 Art. 29-Datenschutzgruppe, WP 136, 15; s. hierzu auch *Gola/Schomerus*, § 3 Rn. 10; *Roßnagel/Scholz*, MMR 2000, 723.

48 Ausführliche Darstellung des Streitstands *Bergt*, ZD 2015, 365; *Haase* 2015, 259ff.; *Brink/Eckhardt*, ZD 2015, 205; *Herbst*, NVwZ 2016, 902.

3.1.3 Konzept des „absoluten Personenbezugs“

Zum einen wird eine Rechtsaufassung identifiziert, die in unterschiedlicher Weise und mit unterschiedlicher Begründung davon ausgeht, dass das absolut vorhandene Wissen berücksichtigt werden muss. Nimmt man diese Meinung ernst, kommt es auf das gesamte (weltweit) theoretisch verfügbare Zusatzwissen an: Wenn ein Datum von irgendjemandem einer bestimmten Person zugeordnet werden kann, ist es personenbezogen. Danach ist der Personenbezug absolut, allein vom Datum her zu bestimmen. Er gilt unabhängig davon, ob der Verantwortliche über das notwendige Zusatzwissen verfügen kann oder sicher davon ausgeschlossen ist.[49]

Allein aus dem Wortlaut lässt sich weder bei Art. 4 Nr. 1 DSGVO noch bei Art. 2 lit. a DSRL oder § 3 Abs. 1 BDSG oder § 67 Abs. 1 SGB X a.F. oder § 67 Abs. 2 SGB X-neu ein Hinweis auf einen relativen oder einen absoluten Ansatz ableiten. Da der Wortlaut der neuen und der bisherigen Fassungen dieser Vorschriften in den entscheidenden Punkten identisch ist,[50] können sie gemeinsam erörtert werden und die Rechtsprechung und die Literatur zur Datenschutzrichtlinie und zum bisherigen Bundesdatenschutzgesetz können auch zur Auslegung des gleichen Wortlauts in Art. 4 Nr. 1 DSGVO genutzt werden.

Die Vertreter eines absoluten Personenbezugs beziehen sich bisher auf Erwägungsgrund 26 der Datenschutzrichtlinie. Dieser lautet:

> *„(26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist …“*

Aus Satz 2, der für die Bestimmbarkeit fordert, nicht nur alle Mittel der verantwortlichen Stelle zu berücksichtigen, sondern auch die Mittel, die „von einem Dritten eingesetzt werden könnten“, schließen sie, dass die Richtlinie und mit ihr das deutsche Datenschutzrecht es ausreichen lassen, wenn irgendein Dritter über das erforderliche Zusatzwissen verfügt.[51] Aus Erwägungsgrund 26 DSRL lässt sich jedoch keine Aussage darüber ableiten, ob im Sinn der absoluten Sichtweise alle beliebigen Dritten gemeint sind oder im Sinn

49 S. z.B. *Pahlen-Brandt*, DuD 2008, 34ff.; *Pahlen-Brandt*, K & R 2008, 289; *Breyer*, ZD 2014, 400 (402ff.); *Schaar* 2002, Rn. 168ff. vor allem für IP-Adressen; Beschluss des Düsseldorfer Kreises vom 26./27.11.2009 in Bezug auf IP-Adressen; nicht eindeutig *Weichert*, in: Däubler u.a., § 3 Rn. 13, 15; *LG Berlin*, K&R 2007, 603; *VG Wiesbaden*, MMR 2009, 432; für ein faktisch-absolutes Verständnis *Herbst*, NVwZ 2016, 902 (905); *Bergt*, ZD 2015, 365 (369f.).

50 S. ausführlich Kap. 3.1.

51 *Pahlen-Brandt*, DuD 2008, 38.

der relativen Sichtweise nur solche Dritte, auf deren Zusatzwissen die verantwortliche Stelle zurückgreifen kann.[52]

Dennoch werden für einen „objektiven Beurteilungsmaßstab“[53] auch die „europäischen Datenschutzbehörden“ herangezogen: Sie sollen im Arbeitspapier 136 der Art. 29-Datenschutzgruppe zum Begriff personenbezogene Daten[54] im Anschluss an Satz 2 des Erwägungsgrunds 26 DSRL einer absoluten Sichtweise folgen.[55] Diese „europäische Betrachtungsweise“ wird einer deutschen Position gegenübergestellt und es wird gefragt, wie lange sich diese deutsche Besonderheit[56] ihr noch entziehen könne.[57]

3.1.4 Konzept des „relativen Personenbezugs“

Die herrschende Meinung geht dagegen davon aus, dass nur das Zusatzwissen, das die verantwortliche Stelle hat oder über das sie verfügen kann, entscheidend sein kann. Danach ist der Personenbezug relativ, nämlich jeweils von der verantwortlichen Stelle aus zu bestimmen, deren Datenumgang zu beurteilen ist.[58] Ist eine Person durch das Zusatzwissen einer verantwortlichen Stelle identifizierbar, kann dies bei einer anderen verantwortlichen Stelle, die über weniger Zusatzwissen verfügt, nicht so sein. Das Zusatzwissen und damit auch der Personenbezug sind eben vom Verwendungskontext der Daten und dem verfügbaren Zusatzwissen einer jeden verantwortlichen Stelle abhängig.[59]

Für den relativen Begriff des Personenbezugs sprechen vor allem systematische und teleologische Gründe, aber auch Überlegungen der Rechtsfolgenbewertung.[60] Systematisch und funktional besteht ein enger Bezug des Begriffs „per-

52 Ebenso *Sachs*, CR 2010, 549f.

53 So nennen *Stiemerling/Hartung*, CR 2012, 63f. das Konzept des „absoluten“ Personenbezugs.

54 Art. 29-Datenschutzgruppe, WP 136, 14ff.

55 *Stiemerling/Hartung*, CR 2012, 63f.; *Karg*, ZD 2012, 256.

56 Gemeint ist damit das Konzept des relativen Personenbezugs. Dagegen wird für das Konzept des „absoluten“ Personenbezugs beansprucht, dass nur dieses der europäischen Konzeption der Datenschutzrichtlinie entspreche.

57 *Stiemerling/Hartung*, CR 2012, 63f.

58 Für die DSRL und das BDSG a.F. s. aus der Rspr. z.B. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 49 – Breyer; *BGH*, NJW 2017, 2416 Rn. 24ff.; *BGH*, ZD 2015, 80, Rn. 32; *BGH*, MMR 2011, 341 (344); *OLG Hamburg*, MMR 2011, 281ff.; *OLG München*, ZD 2011, 182; *LG Berlin*, K&R 2000, 603; *LG Berlin*, ZD 2013, 618; aus der Lit. s. z.B. *Dammann*, in: Simitis, § 3 Rn. 32; *Gola/Schomerus*, § 3 Rn. 10; *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 22; *Schaffland/Wiltfang*, § 3 Rn. 17; *Bizer/Hornung*, in: Roßnagel 2013, § 12 TMG Rn. 44, *Kroschwald* 2015, 58, 69; *Roßnagel/Banzhaf/Grimm* 2003, 150f.; *Nink/Pohle*, MMR 2015, 563 (565f.); *Schmitz*, in: Hoeren/Sieber, Kap. 16.2 Rn. 83f.; *Roßnagel/Pfitzmann/Garstka* 2001, 61; *Roßnagel*, digma 2011, 160ff.; *Roßnagel/Scholz*, MMR 2000, 721f.; *Arning/Forgó/Krügel*, DuD 2006, 700; *Voigt*, MMR 2009, 377; *Caspar*, DÖV 2009, 966; *Meyerdierks*, MMR 2009, 9; *Sachs*, CR 2010, 548; *Eckhardt*, CR 2011, 342; *Eckhardt*, CR 2015, 113 (115); *Knopp*, DuD 2015, 527 (528); *Brink/Eckhardt*, ZD 2015, 205 (207ff.); *Krüger/Maucher*, MMR 2011, 436; *Härting*, NJW 2013, 2066; *Kühling/Klar*, NJW 2013, 3611 (3615); *Kühling/Klar*, ZD 2017, 28; *Klar* 2012, 144f.; *Krügel*, ZD 2017, 455 (458f.); einschränkend *Buchner*, in: Taeger/Gabel, § 3 Rn. 13.

59 S. z.B. Art. 29-Datenschutzgruppe, WP 136, 15; *Dammann*, in: Simitis, § 3 Rn. 38; *Tinnefeld*, in: Roßnagel, Kap. 4.1 Rn. 22; *Roßnagel/Scholz*, MMR 2000, 722f.

60 Die Argumente in *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779 – Breyer, werden in Kap. 3.1.5 ausführlich zur Bestimmung des Personenbezugs in der DSGVO herangezogen.

sonenbezogene Daten" zum Begriff der „verantwortlichen Stelle", wie er gemäß § 3 Abs. 7 BDSG a.F. verwendet wird. § 3 Abs. 1 BDSG a.F. bestimmt den Anwendungsbereich des Datenschutzrechts und § 3 Abs. 7 BDSG a.F. den durch das Datenschutzrecht Verpflichteten. Das gemäß § 3 Abs. 1 BDSG a.F. anwendbare Datenschutzrecht richtet sich an die gemäß § 3 Abs. 7 BDSG verantwortliche Stelle. Das Datenschutzrecht muss für sie anwendbar sein. Das ist es nur, wenn die Daten, die sie erhebt, verarbeitet oder nutzt, für sie personenbezogen sind.

Auch bei genauer Lektüre des Arbeitspapiers 136 der Art. 29-Datenschutzgruppe, das Vertreter der absoluten Theorie als Hauptbeweismittel anführen, wird deutlich, dass diese Gruppe keinen absoluten, sondern einen relativen Begriff der personenbezogenen Daten vertritt. Sie sieht den Personenbezug abhängig vom jeweiligen Kontext,[61] in dem die Daten verarbeitet werden, bezieht sich immer auf den „für die Verarbeitung Verantwortlichen"[62] und stellt auf den Zweck ab, den dieser verfolgt, sowie auf die Mittel, die er vernünftigerweise einsetzen kann. Die in Satz 2 des Erwägungsgrunds 26 DSRL erwähnten „Dritten" werden nicht so verstanden, dass es beliebige Dritte sein können, sondern Dritte, denen Daten vom Verantwortlichen übermittelt werden, Dritte, die selbst zu Verantwortlichen werden (können), oder Dritte, auf deren Zusatzwissen der Verantwortliche zurückgreifen kann.[63] Immer aber wird der Bezug zu einem Verantwortlichen gewahrt und gefragt, ob „der für die Verarbeitung Verantwortliche oder eine andere beteiligte Person" über die Mittel verfügen, den Personenbezug herzustellen.[64] Ist dies dem einen Verantwortlichen möglich, einem anderen jedoch nicht, sind die Daten nur für den ersten personenbezogen.[65]

Nach Art. 2 lit. a DSRL, § 3 Abs. 1 BDSG a.F. und § 67 Abs. 1 SGB X a.F. spricht also alles für ein relatives Verständnis des Personenbezugs, das auf das Zusatzwissen des Verantwortlichen abstellt, über das er verfügt oder über das er mit einem für ihn verhältnismäßigen Aufwand mobilisieren kann.[66] Der Personenbezug ist danach relativ und kann sich von Verantwortlichem zu Verantwortlichem unterscheiden.

3.1.5 Personenbezug nach der Datenschutz-Grundverordnung

Hat sich dieses Verständnis des Personenbezugs durch die Datenschutz-Grundverordnung verändert? Diese Frage wird überwiegend verneint und auch für

61 Art. 29-Datenschutzgruppe, WP 136, 15, 24.
62 Art. 29-Datenschutzgruppe, WP 136, 16, 18, 19, 20, 23.
63 Art. 29-Datenschutzgruppe, WP 136, 18ff.
64 Art. 29-Datenschutzgruppe, WP 136, 19, 23.
65 Art. 29-Datenschutzgruppe, WP 136, 23.
66 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – Breyer; *BGH,* NJW 2017, 2416 Rn. 24ff.;

die Datenschutz-Grundverordnung ein relativer Personenbezug angenommen.[67]

3.1.5.1 Wortlaut

Der Wortlaut des Art. 4 Nr. 1 DSGVO ist hinsichtlich des zu berücksichtigenden Zusatzwissens nicht eindeutig.[68] Er stellt nur fest, dass eine natürliche Person dann als identifizierbar angesehen wird, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung identifiziert werden kann. Wer diese Zuordnung vornehmen muss oder kann, bestimmt die Definition nicht. Sie lässt damit gerade die umstrittenste Frage des Begriffs „personenbezogene Daten" offen.

3.1.5.2 Erwägungsgründe

Die Datenschutz-Grundverordnung erläutert ihr Verständnis der personenbezogenen Daten nach Art. 4 Nr. 1 in Erwägungsgrund 26 DSGVO wie folgt:

> *„Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten 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, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten 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. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."*

67 S. z.B. *Hofmann/Johannes*, ZD 2017, 221; *Barlag*, in: Roßnagel 2017, § 3 Rn. 9; *Husemann*, in: Roßnagel 2018, § 3 Rn. 7; *Roßnagel/Kroschwald*, ZD 2014, 495 (496f.); *Schantz*, NJW 1841 (1843); *Schantz*, in: Schatz/Wolf 2017, Rn. 279ff.; *Marnau*, DuD 2016, 428, (430); *Kartheuser/Gilsdorf*, MMR-Aktuell 2016, 382533; *Moos/Rothkegel*, MMR 2016, 845 (847); *Laue/Nink/Kremer 2016*, § 1 Rn. 116; *Ziebarth*, in: Sydow, Art. 4 Rn. 37; *Gola*, in: ders., Art. 4 Rn. 17; *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 26; *Krügel*, ZD 2017, 455 (458f.); a.A. *Buchner*, DuD 2016, 155 (156); widersprüchlich *Albrecht/Jotzo* 2017, Teil 3 Rn. 3, die eine „absolute Betrachtung", aber zugleich eine Prüfung des Einzelfalls bei jedem Verantwortlichen fordern.

68 Ebenso *Buchner* DuD 2016, 155 (156); *Hofmann/Johannes*, ZD 2017, 221 (222).

Zwar gehören die Erwägungsgründe nicht zum verfügenden Teil der Verordnung und sind daher nicht rechtsverbindlich.[69] Jedoch geben sie die Ziele an, auf die sich die unterschiedlichen Unionsorgane, die zusammen den Unionsgesetzgeber bilden, geeinigt haben und nennen zu jeder Vorschrift die nach Art. 296 UAbs. 2 AEUV erforderliche Begründung. Auch wenn sie nicht rechtsverbindlich sind, können die Erwägungsgründe wichtige Hinweise zur Auslegung einer Vorschrift bieten. Allerdings können sie keine vom Wortlaut abweichende Auslegung rechtfertigen.[70] Der Europäische Gerichtshof nutzt regelmäßig die Erwägungsgründe zur Auslegung von Vorschriften des Unionsrechts.[71]

Erwägungsgrund 26 Satz 3 DSGVO könnte im Sinn eines absoluten Personenbezugs verstanden werden, wenn danach „alle Mittel berücksichtigt werden" sollen, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren".[72] Allerdings stellt dieser Satz nicht auf die absolute Möglichkeit einer Identifizierung ab, sondern bezieht sich auf die Wahrscheinlichkeit, dass der konkrete Verantwortliche oder eine andere konkrete Person, die über die Daten verfügt, die Mittel nutzen wird. Die Formulierung „genutzt werden" ist ganz konkret und stellt auf die relativen Möglichkeiten des Verantwortlichen ab. Die Identifizierbarkeit hängt hier erkennbar vom gegebenen Kontext ab.[73] Nicht in das Konzept des absoluten Personenbezugs passt es auch, dass die Bestimmung auf den Verantwortlichen abstellt. Für dieses Konzept ist es nämlich unerheblich, wer die Identifizierung vornehmen kann.

Für die Feststellung der Wahrscheinlichkeit einer Identifizierung sollen nach Satz 4 des Erwägungsgrunds 26 DSGVO „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden". Auch sollen die „zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen" berücksichtigt werden. Die Bestimmung der Wahrscheinlichkeit, dass verfügbare Mittel zur Identifizierung einer natürlichen Person genutzt werden, und die Aufforderung, die Kosten und den Aufwand der Identifizierung sowie die verfügbare Technologie zu berücksichtigen, sprechen gegen das Konzept eines absoluten Personenbezugs.[74] Denn diese wären dafür irrelevant. Vielmehr kann die zu bestimmende Wahrscheinlichkeit von Person zu Person unterschiedlich sein.[75] Dies gilt sowohl für das Interesse, die betroffene Person zu identifizieren, als auch

69 *EuGH*, Urteil vom 19.11.1998 – C 162/97 – ECLI:EU:C:1998:554, Rn. 54 – Nilsson u.a.; *EuGH*, Urteil vom 24.11.2005 – C 316/04 – ECLI:EU:C:2005:716, Rn. 32 – Deutsches Milchkontor.
70 *EuGH*, Urteil vom 19.11.1998 – C 162/97 – ECLI:EU:C:1998:554, Rn. 54 – Nilsson u.a.
71 *EuGH*, Urteil vom 13.5.2014 – C 131/12 – ECLI:EU:C:2014:317, Rn. 54 – Google Spain und Google.
72 So z.B. *Buchner*, DuD 2016, 155 (156).
73 *Husemann*, in: Roßnagel 2018, § 3 Rn. 7.
74 So im Ergebnis auch *Hofmann/Johannes*, ZD 2017, 221 (224f.); *Kroschwald* 2015, 58.
75 S. auch *Hofmann/Johannes*, ZD 2017, 221 (224).

für die jeweiligen Mittel zur Identifizierung, über die der Verantwortliche verfügen kann. Die individuelle Wahrscheinlichkeit der Identifizierung kann jedenfalls nicht allgemein danach bestimmt werden, dass irgendwo auf der Welt ausreichende Mittel zur Verfügung stehen, um die betroffene Person zu identifizieren.[76] Erwägungsgrund 26 DSGVO spricht daher für ein relatives Verständnis des Personenbezugs.

Eindeutig geht Erwägungsgrund 30 DSGVO von einem relativen Personenbezug aus. Dieser geht davon aus, dass natürliche Personen nur „unter Umständen" Online-Kennungen „wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet" werden können. Dies ist dann der Fall, wenn die IP-Adressen und Cookie-Kennungen „in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren". Nach diesem Erwägungsgrund gibt es also Verantwortliche, für die diese Daten personenbezogen sind, weil sie sie mit eindeutigen Kennungen kombinieren können, und andere Verantwortliche, für die sie mangels dieses Zusatzwissens nicht personenbezogen sind.[77]

3.1.5.3 Systematik

Die Verwendung des Begriffs der personenbezogenen Daten in anderen Vorschriften oder die Nichtanwendung der Datenschutz-Grundverordnung auf bestimmte Daten können Rückschlüsse auf das Verständnis des Begriffs personenbezogene Daten in Art. 4 Nr. 1 DSGVO bieten.

Anonyme Daten werden von der Datenschutz-Grundverordnung – im Gegensatz zu § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8 SGB X a.F. – in keiner Vorschrift geregelt.[78] Dies erfolgt nur indirekt in Erwägungsgrund 26 Satz 5 DSGVO, der darlegt, dass anonyme Daten von der Verordnung nicht erfasst werden. Dieser Ausschluss anonymer Daten aus dem Anwendungsbereich der Verordnung in Erwägungsgrund 26 Satz 5 DSGVO stützt den Standpunkt, von einem relativen Personenbezug auszugehen. Müsste man nämlich von einem absoluten Verständnis des Personenbezugs ausgehen, gäbe es so gut wie keine anonymen Daten, da es irgendjemandem nahezu immer möglich ist, den Personenbezug herzustellen, sodass anonyme Daten nie aus dem Anwendungsbereich der Verordnung ausgeschlossen wären.[79]

76 S. z.B. *Kroschwald* 2015, 58.

77 S. *Schantz*, NJW 2016, 1841 (1843); *Brink/Eckhardt*, ZD 2015, 205 (209).

78 S. zu anonymen Daten näher Kap. 3.2.

79 *Roßnagel/Kroschwald*, ZD 2014, 495 (497); *Herbst*, NVwZ 2016, 902 (905); *Barlag*, in: Roßnagel 2017, § 3 Rn. 9; *Hofmann/Johannes*, ZD 2017, 221 (223); *Kühling/Klar,* NJW 2013, 3611 (3616); *Nink/Pohle*, MMR 2015, 563 (565f.); *Eckart*, CR 2015, 113 (115).

„Pseudonymisierung" von personenbezogenen Daten definiert Art. 4 Nr. 5 DSGVO so, dass personenbezogene Daten in einer Weise verarbeitet werden, dass sie ohne Hinzuziehung zusätzlicher Informationen „nicht mehr einer spezifischen betroffenen Person zugeordnet werden können".[80] Soweit pseudonymisierte Daten nicht mehr einer bestimmten Person zuordenbar sind, sind sie nicht mehr personenbezogen. Der Personenbezug kann allerdings unter Hinzuziehung zusätzlicher Informationen, einer Zuordnungsregel, wieder hergestellt werden.[81] Daher fordert die Definition in Art. 4 Nr. 5 DSGVO vom Inhaber der zusätzlichen Informationen Sicherungsmaßnahmen, „diese zusätzlichen Informationen gesondert" aufzubewahren sowie technische und organisatorische Maßnahmen zu ergreifen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden". Diese rechtliche Konstruktion geht von relativen Bezügen aus. Sie unterstellt, dass die personenbezogenen Daten so pseudonymisiert werden können, dass die Daten für alle außer dem Inhaber der Zuordnungsregel nicht mehr einer bestimmten Person zuordenbar sind,[82] dem Inhaber der Zuordnungsregel aber schon.[83] Die Definition des Art. 4 Nr. 5 DSGVO spricht daher für einen relativen Personenbezug.[84]

3.1.5.4 Sinn und Zweck

Dies entspricht auch einer teleologischen Betrachtung der Datenschutz-Grundverordnung: Der Verantwortliche nimmt durch seine Verarbeitung der Daten der betroffenen Person einen Eingriff in ihr Grundrecht auf Datenschutz und informationelle Selbstbestimmung vor.[85] Vor diesem Eingriff, sofern er rechtswidrig ist, soll das Datenschutzrecht die betroffene Person schützen – immer, aber auch nur gegenüber dem jeweils Eingreifenden. Das Datenschutzrecht soll die Gefahr einer Verletzung dieser Grundrechte ausschließen. Eine solche Gefahr kann aber von einem bestimmten Verantwortlichen nur ausgehen, wenn er zumindest die Möglichkeit hat, die Daten der betroffenen Person zuzuordnen. Wenn diese Zuordnung ausgeschlossen ist, dann ist auch die Gefahr einer Grundrechtsverletzung durch diesen Verantwortlichen ausgeschlossen. Für das Datenschutzrecht besteht dann kein Schutzauftrag.

Das Grundrecht auf Datenschutz soll – ebenso wie das Grundrecht auf informationelle Selbstbestimmung[86] – den betroffenen Personen gewährleisten,

80 S. zu pseudonymen Daten ausführlich Kap. 3.3.
81 S. *Roßnagel/Scholz*, MMR 2000, 721ff.
82 S. hierzu näher Kap. 3.3.1.
83 Daher bleiben die Daten nach Erwägungsgrund 26 Satz 2 DSGVO für alle, die über die zusätzlichen Informationen verfügen können, personenbezogen.
84 Ebenso *Hofmann/Johannes*, ZD 2017, 221 (222f.); *Marnau*, DuD 2016, 428 (430).
85 S. ausführlich *Roßnagel/Pfitzmann/Garstka* 2002, 46ff.
86 Zum Verhältnis zwischen dem Grundrecht auf Datenschutz und dem Grundrecht auf informationelle Selbstbestimmung s. z.B. *Masing*, NJW 2012, 2305ff; *Danwitz*, DuD 2015, 581ff.; *Geminn/Roßnagel*, JZ 2015, 703ff.

dass sie immer „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".[87] Dies ist die Voraussetzung, damit sie das Wissen ihres Gegenübers über ihre Situation einschätzen können. Nur dann sind sie frei, sich diesem Wissen entsprechend zu entscheiden und zu verhalten. Für dieses Ziel der informationellen Selbstbestimmung und des Datenschutzes ist also entscheidend, was jeweils derjenige, der die Daten des Betroffenen verarbeitet, über ihn weiß. Die normativen Anforderungen der informationellen Selbstbestimmung sollen somit eine soziale Beziehung gestalten. Sie gewährleisten Transparenz und Freiheit der Selbstbestimmung jeweils gegenüber dem Verantwortlichen. Wer diese Freiheit nicht bedroht, weil er die Daten nicht in einer Beziehung zum Betroffenen nutzen kann, muss die Anforderungen der informationellen Selbstbestimmung und des Datenschutzes nicht erfüllen. Diesem Schutzziel entspricht ein relatives Verständnis des Begriffs „personenbezogene Daten", nicht ein absolutes.

Umgekehrt betrachtet, ist die Anwendung des Datenschutzrechts mit seinem Grundsatz, dass es dem Verantwortlichen nicht erlaubt, Daten der betroffenen Person zu verarbeiten, solange er hierfür keine Einwilligung der betroffenen Person oder keine Erlaubnis eines Rechtsetzers hat, ein Eingriff in die Grundrechte des Verantwortlichen aus Art. 5 Abs. 1 und 3, 12 Abs. 1 und 2 Abs. 1 GG[88] sowie Art. 11, 13, 15 und 16 GrCh. Dieser Eingriff ist nur gerechtfertigt, wenn er geeignet, erforderlich und zumutbar ist, um eine Gefahr für das Grundrecht auf Datenschutz nach Art. 8 GRCh und auf informationelle Selbstbestimmung des Betroffenen nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abzuwehren.[89] Nach der absoluten Sichtweise muss der Verantwortliche diesen Grundrechtseingriff jedoch hinnehmen, auch wenn von der Datenverarbeitung in keiner Weise eine Gefahr für die informationelle Selbstbestimmung und den Datenschutz der betroffenen Person ausgehen kann – weil er die Daten ihr nicht zuordnen kann.[90] In diesem Fall ist der Eingriff in die Grundrechte des Verantwortlichen aber weder geeignet noch erforderlich noch ihm zumutbar.[91]

Die absolute Betrachtungsweise würde sogar dazu führen, dass Verantwortliche, die ein bestimmtes Datum verarbeiten, datenschutzrechtliche Pflichten erfüllen müssen, wenn auch nur eine einzige Stelle auf der Welt in der Lage sein könnte, das Datum einer bestimmten Person zuzuordnen. Es gibt keinen Grund, warum deren Wissen zulasten aller anderen Verantwortlichen wirken und bei diesen Grundrechtseingriffe begründen sollte.[92] Im Gegenteil verstößt

87 S. *BVerfGE* 65, 1 (43).

88 S. z.B. *Roßnagel/Pfitzmann/Garstka* 2001, 48ff.

89 S. z.B. *Buchner*, in: Täger/Gabel, § 3 Rn. 12f.; *Stiemerling/Hartung*, CR 2012, 64.

90 Dass das *BVerfGE* 65, 1 (46) feststellt, dass es unter den Bedingungen der modernen Datenverarbeitung „kein harmloses" Datum gibt, begründet zwar ein Schutzbedürfnis der betroffenen Person bezogen auf die Verarbeitung aller personenbezogenen Daten, aber nicht einen Grundrechtseingriff durch alle Verantwortlichen – insbesondere, wenn diese keinen Personenbezug herstellen können.

91 Im Ergebnis ebenso *Hofmann/Johannes*, ZD 2017, 221 (225).

92 S. *BGH*, ZD 2015, 80, Rn. 28; *Brink/Eckhardt*, ZD 2015, 205 (209).

eine solche Sichtweise gegen das Bestimmtheitsgebot, weil die Anwendbarkeit des Datenschutzrechts davon abhinge, ob irgendjemand weitere Kenntnisse hat, ohne dass der Verantwortliche dies wissen oder beeinflussen kann.[93] Auch wäre der Verantwortliche, der den Bezug zur betroffenen Person gar nicht kennt, nicht in der Lage, seine Pflichten zur Information, zur Auskunft, zur Berichtigung oder zur Löschung zu erfüllen. Grundrechtskonform kann das Datenschutzrecht daher nur angewendet werden, wenn sein jeweiliger Adressat eine „Grundrechtsgefahr" darstellt. Dies ist – mit dem relativen Begriff des Personenbezugs – nur dann der Fall, wenn der Adressat mit Hilfe seines verfügbaren Zusatzwissens die betroffene Person bestimmen kann.[94]

3.1.5.5 Bedeutungslosigkeit des Theorienstreits

Das Konzept des „absoluten" Personenbezugs ist nur dann konsequent, wenn seine Vertreter die Meinung vertreten, dass es auf das weltweit verfügbare Wissen über die Zuordnungsmöglichkeit eines Datensatzes zu einer bestimmten Person ankommt. Dies führt dazu, dass nahezu jedes Datum personenbezogen ist und jedes Datum die datenschutzrechtlichen Pflichten und Rechte, Aufgaben und Befugnisse[95] hervorruft.[96] Denn zu jedem Datum kann objektiv zumindest ein Bezug zu seinem Erzeuger, Verarbeiter, Verwender oder der betroffenen Person hergestellt werden. Dieses Ergebnis wäre – jenseits der vielen Gründe, die gegen dieses Konzept vorgetragen wurden – absurd.

Den Vertretern des Konzepts des „absoluten" Personenbezugs kommt der Verdienst zu, darauf hingewiesen zu haben, dass unter den Bedingungen von ubiquitous computing, Internet-Tracking und Big Data jedem Datum ein Bezug zu einer natürlichen Person zukommen kann. Auch wenn die Daten statistisch aggregiert, pseudonymisiert, anonymisiert, verschlüsselt oder auf sonstige Weise ihres Bezugs zu einer bestimmten Person beraubt zu sein scheinen, ist nicht auszuschließen, dass irgendjemand zu einem späteren Zeitpunkt diesen Bezug herstellen kann.[97] Dieses Risiko besteht und ist ernst zu nehmen.[98] Dem Anliegen der Vertreter des Konzepts eines absoluten Personenbezugs muss dadurch entsprochen werden, dass alle denkbaren Möglichkeiten der Identifizierung nachgegangen wird und auch die Zukunftsdynamik Berücksichtigung findet.

93 *Meyerdierks*, MMR 2009, 8 (11); *Ziebarth*, in: Sydow, Art. 4 Rn. 39.
94 *Roßnagel/Scholz*, MMR 2000, 723.
95 S. Kap. 3.1.1.
96 S. z.B. *Husemann*, in: Roßnagel 2018, § 3 Rn. 7; *Brink/Eckhardt*, ZD 2015, 205 (207); *Nink/Pohle*, MMR 2015, 563 (565).
97 S. z.B. *Bergt*, ZD 2015, 365 (369); *Herbst*, NVwZ 2016, 902 (904); s. hierzu auch *Brink/Eckhardt*, ZD 2015, 205 (206).
98 Ihm müsste mit einem Konzept der Datenschutzvorsorge begegnet werden – s. z.B. *Roßnagel/Scholz*, MMR 2000, 721 (728ff.); *Roßnagel* 2007, 185ff.; *Roßnagel/Geminn/Jandt/Richter* 2016, 137.

Dieses Risiko begründet jedoch nicht, es jedem Datenverarbeiter zuzurechnen und ihn zur Bekämpfung dieses Risikos mit allen datenschutzrechtlichen Pflichten zur Gefahrenabwehr zu belasten. Wenn aber zwischen der NSA und Google einerseits und dem „Bäcker um die Ecke" andererseits differenziert werden muss, dann kann nur ein Konzept rechtlich vertreten werden, das den Personenbezug risikobezogen und relativ von den Handlungsmöglichkeiten des Verarbeiters her bestimmt.[99] Mit dieser Erkenntnis löst sich der Streit zwischen den beiden Konzepten auf und wendet sich pragmatisch den Fragen zu, welches mögliche Zusatzwissen dem jeweiligen Datenverarbeiter zuzurechnen ist.

3.1.5.6 Praktisch verfügbares Zusatzwissen

Entscheidend ist also, über welches Zusatzwissen der Verantwortliche verfügen kann. Nach Erwägungsgrund 26 Satz 3 DSGVO ist für das Zusatzwissen auf die Mittel abzustellen, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren". Demnach soll anhand einer Risikoprognose geprüft werden, ob „auf Grund allgemeiner Lebenserfahrung oder auf Grund wissenschaftlicher Expertise ... mit einer Aufdeckung des Personenbezugs zu rechnen ist".[100] Die „rein hypothetische Möglichkeit zur Bestimmung der Person" reicht nicht aus, um die Person als ‚bestimmbar' anzusehen".[101] Ein Personenbezug scheidet somit aus, wenn die Wahrscheinlichkeit einer Bestimmung so gering ist, dass das Risiko praktisch vernachlässigbar ist.[102] Die Bestimmbarkeit ist demnach nicht absolut zu beurteilen, sondern nach ihrer faktischen Durchführbarkeit.[103] Ob eine Angabe tatsächlich zugeordnet werden kann, ist daher eine Frage der Wahrscheinlichkeit.[104]

Das Wahrscheinlichkeitsurteil ergibt sich aus einer Zweck-Mittel-Abwägung. Nach Erwägungsgrund 26 Satz 4 DSGVO sind hinsichtlich der eingesetzten Mittel für das Gewinnen des Zusatzwissens die „Kosten der Identifizierung und der dafür erforderliche Zeitaufwand" sowie „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen". Es sollen „alle objektiven Faktoren" bedacht werden. Die Aufzählung „Kosten und Zeit" ist nicht abschließend, sondern ausdrücklich exemplarisch. „Alle" deutet auf eine umfassende Berücksichtigung der Aufwandsfaktoren hin.[105] Entscheidend für die Prognose über die Verwendung

99 Eine Modifikation des Konzepts des absoluten Personenbezugs kann es nicht geben, da es bei Einschränkungen nicht mehr absolut ist.

100 *Roßnagel/Scholz*, MMR 2000, S. 721 (723).

101 Art. 29-Datenschutzgruppe, WP 136, 17 zur insoweit identischen Datenschutzrichtlinie.

102 *Dammann*, in: Simitis, § 3 Rn. 23; Art. 29-Datenschutzgruppe, WP 136, 17.

103 So *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – Breyer; *BGH* 2017, 2416 Rn. 24ff. zur insoweit identischen Datenschutzrichtlinie.

104 *Hofmann/Johannes*, ZD 2017, 221 (224); *Roßnagel/Scholz*, MMR 2000, 726; *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 23.

105 *Hofmann/Johannes*, ZD 2017, 221 (224).

der Mittel ist auch das im Rahmen einer Risikobetrachtung zu ermittelnde Interesse, das der Verantwortliche oder die andere Person an der Identifizierung haben. Es kann für einen von beiden mit der Identifizierung beispielsweise ein hohes wirtschaftliches Interesse verbunden sein.[106] Daher ist auch der Wert[107] oder der wirtschaftliche Nutzen[108] einer personenbezogenen Zuordnung für den Verantwortlichen oder Dritten in die Wahrscheinlichkeitsprognose einzustellen.[109] Außerdem sollten „der beabsichtigte Zweck, die Strukturierung der Verarbeitung, der von dem für die Verarbeitung Verantwortlichen erwartete Vorteil, die auf dem Spiel stehenden Interessen für die Personen sowie die Gefahr organisatorischer Dysfunktionen (z.B. Verletzung von Geheimhaltungspflichten) und technischer Fehler … ebenfalls Berücksichtigung finden".[110]

Schließlich sind die möglichen Folgen für die betroffene Person zu berücksichtigen. Die nach allgemeinem Ermessen zu bestimmende Wahrscheinlichkeit muss umso geringer sein, je größer der Schaden eines Missbrauchs der Daten für die betroffene Person wäre. Je weniger belastende Folgen für sie anzunehmen sind, desto geringer darf der Anspruch sein, sie zu vermeiden.[111] Die Anforderungen an den Ausschluss der Identifizierung dürften daher im Gesundheitsbereich in der Regel höher sein als im Bereich Online-Spiele.

Letztlich wird die Wahrscheinlichkeit nach einem objektiven Maßstab bestimmt durch eine Kosten-Nutzen-Risiko-Relation, die für den jeweiligen Verantwortlichen oder Auftragsverarbeiter anzustellen ist.[112] Nur wenn danach wahrscheinlich ist, dass er in der Lage ist, die Daten und sein erreichbares Zusatzwissen zu nutzen, um die betroffene Person zu identifizieren, handelt es sich für ihn um personenbezogene Daten.

Erwägungsgrund 30 DSGVO gibt einen Hinweis, wie verfügbare Technologien für die Identifizierung von natürlichen Personen genutzt werden können:

> *„Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren."*

106 *Hofmann/Johannes*, ZD 2017, 221 (224).
107 *Dammann*, in: Simitis, § 3 Rn. 25.
108 *Gola/Schomerus*, § 3 Rn. 44.
109 *Hofmann/Johannes*, ZD 2017, 221 (224); *Kroschwald* 2015, 58f.; *Nink/Pohle*, MMR 2015, 563 (565); *Marnau*, DuD 2016, 428, (430).
110 Art. 29-Datenschutzgruppe, WP 136, 18.
111 Zu der aus dem Grundrechtsschutz und dem Verhältnismäßigkeitsgrundsatz abgeleitete Je-Desto-Formel s. *BVerfGE* 49, 89 (136ff.).
112 S. z.B. auch *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 23; *Kroschwald* 2015, 58f.; *Dammann*, in: Simitis, § 3 Rn. 25.

Datenspuren, die im Internet oder im Ubiquitous Computing hinterlassen werden, können durch Kombination mit anderen Daten wie eindeutigen Kennungen und anderen eingehenden Daten dazu benutzt werden, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren. Sowohl die erfassten Datenspuren als auch die aus ihnen angelegten Profile sollen somit als personenbezogene Daten betrachtet werden und dem Datenschutzrecht unterfallen. Damit ist für IP-Adressen[113] und Cookies eindeutig geklärt, dass sie personenbezogene Daten sein können.

Die Zweck-Mittel-Relation ist nicht statisch, sondern kann sich mit der Zeit verändern.[114] Daher muss für die Bestimmung möglichen Zusatzwissens auch die Zeitdimension einbezogen werden. Der Aufwand zur Bestimmung von Personen kann sich etwa mit der fortlaufenden Erweiterung der zugänglichen Datenmenge sowie mit den Möglichkeiten zur technischen Zusammenführung und Verknüpfung von Daten reduzieren.[115] Aktuell als nicht personenbezogen eingestufte Daten können zukünftig personenbezogen werden.[116] Daher fordert Satz 4 des Erwägungsgrunds 26 DSGVO, neben der „zum Zeitpunkt der Verarbeitung verfügbare(n) Technologie" auch die „technologische(n) Entwicklungen zu berücksichtigen".[117] Hierfür ist zumindest für die nähere Zukunft die Dynamik der absehbaren technischen Entwicklungen in die Prognose der Identifizierbarkeit aufzunehmen.[118] Wenn der Verantwortliche in absehbarer Zeit über neue technische Mittel zur Identifizierung verfügt oder verfügen kann, bestimmen diese die Wahrscheinlichkeit der Identifizierung. Die Prüfung des Personenbezugs muss – so die Art. 29-Datenschutzgruppe zur insoweit identischen Datenschutzrichtlinie – zumindest „die Entwicklungsmöglichkeiten in dem Zeitraum berücksichtigen …, für den die Daten verarbeitet werden".[119] Dabei ist eine Abwägung vorzunehmen zwischen der zeitlichen Verfügbarkeit neuer technischer Mittel und dem Wert und der Verwendbarkeit von Informationen im Zeitablauf. Wenn die Daten nur kurzfristig aufbewahrt werden, ist ein langer Blick in die Zukunft voraussichtlich nicht notwendig. „Bei einer Aufbewahrungsdauer von zehn Jahren hingegen sollte der für die Verarbeitung Verantwortliche die Möglichkeit der Identifizierung berück-

113 Die hM nimmt ohnehin einen Personenbezug an, s. *Dammann*, in: Simitis 2014, § 3 Rn. 63 m.w.N.; s. auch *EuGH*, Urteil vom 24.11.2011, Rs. C-70/10, ECLI:EU:C:2011:771, Scarlet Extended; *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Breyer; *BGH*, ZD 2015, 80; zum Streit um den Personenbezug von IP-Adressen s. z.B. Düsseldorfer Kreis 2009; *Eckhardt*, CR 2011, 339; *Krüger/Maucher*, MMR 2011, 433; *Meyerdierks*, MMR 2009, 8; *Nink/Pohle*, MMR 2015, 563; *Pahlen-Brandt*, K&R 2008, 286; *Sachs*, CR 2010, 547; *Breyer*, ZD 2014, 400.

114 S. z.B. *Kroschwald* 2015, 59; *Marnau*, DuD 2016, 428, (429).

115 S. *BVerfGE* 65, 1 (45).

116 *Dammann*, in: Simitis, § 3 Rn. 36; *Kroschwald* 2015, 59f.; *Kühling/Klar*, NJW 2013, 3613f.

117 Die Bewertung der Identifizierungsmöglichkeiten sind daher nach Erwägungsgrund 26 DSGVO nicht auf den Zeitpunkt der Datenverarbeitung beschränkt, so *Kühling/Klar*, NJW 2013, 3611 (3613), sondern berücksichtigt auch absehbare technische Entwicklungen, so auch *Marnau*, DuD 2016, 428, (429); *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 24; *Schantz*, in: Schatz/Wolf 2017, Rn. 283.

118 Im Ergebnis ebenso *Hofmann/Johannes*, ZD 2017, 221 (224f.)

119 Art. 29-Datenschutzgruppe, WP 136, 18; *Kroschwald* 2015, 60.

sichtigen, die im neunten Jahr der Aufbewahrungsdauer der Daten entstehen könnte und die sie in diesem Moment zu personenbezogenen Daten machen würden. Das System sollte diesen Entwicklungen angepasst werden können und dann zum gegebenen Zeitpunkt die geeigneten technischen und organisatorischen Maßnahmen einbeziehen."[120]

3.1.5.7 Zusatzwissen Dritter

Nach Satz 3 des Erwägungsgrunds 26 DSGVO sollten bei der Entscheidung, ob eine Person identifizierbar ist, auch „alle Mittel berücksichtigt werden, die von ... einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren". Mit diesen Dritten sind nicht beliebige Dritte gemeint. Die Frage nach dem Personenbezug stellt sich immer in einer Situation, in der über die Anwendbarkeit des Datenschutzrechts auf einen bestimmten Umgang mit bestimmten Daten entschieden werden muss. Für die Auslegung des Erwägungsgrunds 26 Satz 3 DSGVO kann auf die Rechtsprechung und Literatur zu dieser Frage in der Datenschutzrichtlinie zurückgegriffen werden. Danach ist für diesen Datenumgang das Zusatzwissen Dritter dann relevant, wenn die Dritten

- Daten vom Verantwortlichen oder Auftragsverarbeiter erhalten (sollen) (Veröffentlichung, Übermittlung) oder sich beschaffen (können), sodass sie in Bezug auf diese Daten selbst zum Verantwortlichen werden,[121]
- mit dem Verantwortlichen oder dem Auftragsverarbeiter in irgendeiner Weise zusammenarbeiten (können), um die Person zu identifizieren[122] oder
- ihr Zusatzwissen auf andere Weise dem Verantwortlichen oder Auftragsverarbeiter zur Verfügung stellen können oder müssen.[123]

Allerdings kann eine Weitergabe der Daten von dem Dritten an weitere Dritte oft „nach allgemeinem Ermessen" nicht ausgeschlossen werden. Dadurch kann der Kreis des einzubeziehenden Zusatzwissens stark erweitert werden.[124] In diesem Fall ist auch dieses Zusatzwissen für die Frage der Identifizierbarkeit der betroffenen Person zu berücksichtigen. Macht also ein Verantwortlicher Daten, mit denen er keine betroffene Person identifizieren kann, einem Dritten zugänglich, der – wie etwa ein großes Unternehmen mit umfangreichen Sammlungen von Persönlichkeitsprofilen oder ein Geheimdienst – Iden-

120 Art. 29-Datenschutzgruppe, WP 136, 18. *Kühling/Klar*, NJW 2013, 3613f.; *Dammann*, in: Simitis, § 3 BDSG, Rn. 38; *Kroschwald* 2015, 60.

121 S. z.B. Art. 29-Datenschutzgruppe, WP 136, 18ff.; *Dammann*, in: Simitis, § 3 Rn. 33f.; *Eckhardt*, CR 2011, 343f.

122 S. z.B. Art. 29-Datenschutzgruppe, WP 136, 22f.

123 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 43f. – Breyer; *BGH* 2017, 2416 Rn. 24ff.; *Kühling/Klar*, ZD 2017, 28.

124 *Dammann*, in: Simitis, § 3 Rn. 34.

tifizierungen vornehmen kann, so handelt es sich um personenbezogene Daten.[125]

Das Zusatzwissen Dritter ist aber nur zu berücksichtigen, soweit „nach allgemeinem Ermessen" mit seinem Einsatz zu rechnen ist. Es kommt also auf die Frage an, ob der Verantwortliche oder die andere Person die ihm oder ihr zur Verfügung stehenden technischen oder rechtlichen Möglichkeiten vernünftigerweise nutzen wird.[126] Dementsprechend qualifiziert der Europäische Gerichtshof dynamische IP-Adressen dann als personenbezogen, wenn dem Verantwortlichen rechtliche Mittel wie etwa Auskunftsansprüche zur Verfügung stehen, mit deren Hilfe er an Zusatzinformationen gelangen kann, die einem Dritten vorliegen.[127] Dabei reicht die grundsätzliche Berechtigung, ein rechtliches Mittel geltend zu machen, aus, ohne dass es auf die tatsächliche Durchsetzbarkeit der Ansprüche im konkreten Fall ankommt.[128]

Zusatzwissen Dritter ist für die Frage, ob der Betroffene identifizierbar ist, in der Regel nicht zu berücksichtigen, wenn die Verwendung des Zusatzwissens gesetzlich verboten ist.[129] Selbstverständlich ist illegales Verhalten zu berücksichtigen, wenn es stattfindet.[130] In einem Rechtsstaat kann aber nicht jedem Beteiligten ohne Anlass eine Neigung oder gar Absicht zum Rechtsbruch unterstellt werden, wenn die Befolgung eines Weitergabe- oder Verwendungsverbots weitgehend gesichert ist.[131] Dabei ist es gleichgültig, ob das rechtliche Verbot an den Verantwortlichen oder an den Dritten, der über das Zusatzwissen verfügt, gerichtet ist. Entscheidend ist, ob dem Zusammenbringen beider Komponenten Hindernisse von einer Qualität entgegenstehen, dass damit „nach allgemeinem Ermessen" praktisch nicht zu rechnen ist.[132] Ein Rechtsbruch ist daher zu berücksichtigen, wenn es Hinweise darauf gibt, dass rechtliche Verbote nicht beachtet, nicht kontrolliert oder nicht durchgesetzt werden. Eine gesetzliche oder vertragliche Verpflichtung, etwa ein Verbot zur

125 S. z.B. *Kroschwald* 2015, 68; *Kühling/Klar*, NJW 2013, 3611 (3615); *Klar* 2012, 145; *Gola*, in: ders., Art. 4 Rn. 21; *Gola/Schomerus*, § 3 Rn. 10, 44a; *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 27. Dies ist ein Hauptargument der Vertreter für einen „absoluten" Personenbezug, dem aber auch das Konzept eines „relativen" Personenbezugs gerecht werden kann.

126 *Hofmann/Johannes*, ZD 2017, 221 (224); *Haase* 2015, 304; *Ziebarth*, in: Sydow, Art. 4 Rn. 37.

127 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 49 – Breyer; *Kühling/Klar*, ZD 2017, 28.

128 S. *Hofmann/Johannes*, ZD 2017, 221 (224); *Weinhold*, ZD-Aktuell 2016, 05366.

129 Gegen die Berücksichtigung z.B. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – Breyer; *BGH* 2017, 2416 Rn. 24ff.; *BGH*, ZD 2015, 80, Rn. 32; *AG München*, ZUM-RD 2009, 414; *Hofmann/Johannes*, ZD 2017, 221 (224); *Nink/Pohle*, MMR 2015, 563 (565); *Meyerdierks*, MMR 2009, 8 (11ff.); *Krüger/Maucher*, MMR 2011, 433 (437f.); *Arning/Forgó/Krügel*, DuD 2006, 700 (703); *Eckhardt*, CR 2011, 342; *Kühling/Klar*, NJW 2013, 3611 (3613); *Kühling/Klar*, ZD 2017, 28; *Brink/Eckhardt*, ZD 2015, 205 (211); *Eckhardt*, CR 2015, 113 (115); a.A. und für die Berücksichtigung z.B. *Weichert*, DuD 2010, 681; *ders.*, in: Däubler u.a. 2010, § 3 Rn. 47; *Pahlen-Brandt,* K&R 2008, 286 (289); *Dammann*, in: Simitis, § 3 Rn. 36; *Bergt*, ZD 2015, 365 (370); *Herbst*, NVwZ 2016, 902 (905); *AG Berlin-Mitte*, K&R 2007, 601.

130 *Brink/Eckhardt*, ZD 2015, 205 (211).

131 *Meyerdierks*, MMR 2009, 8 (11f.); *Krüger/Maucher*, MMR 2011, 433 (437f.); *Arning/Forgó/Krügel*, DuD 2006, 700 (703).

132 *Dammann*, in: Simitis, § 3 Rn. 33; *Kroschwald* 2015, 67. Vertragliche Absprachen reichen hierfür nicht aus.

Datenherausgabe, kann in solchen Fällen allein nicht ausreichen, um den Personenbezug zu verneinen und das Datenschutzrecht für unanwendbar zu erklären.[133]

In Fällen mit internationalem Datenverkehr und erschwerter Durchsetzung von rechtlichen Regelungen wird zu der rechtlichen Beschränkung, den Personenbezug herzustellen, noch eine tatsächliche Beschränkung, mit den Daten die betroffene Person identifizieren zu können, hinzukommen müssen.[134] Diese könnte beispielsweise in technisch-organisatorischen Maßnahmen bestehen.[135] Existieren nicht nur rechtliche, sondern auch technische und organisatorische Hürden, kann für den Dritten eine Bestimmung des Betroffenen „nach allgemeinem Ermessen" unverhältnismäßig sein, sodass ein Personenbezug entfällt. Die Art. 29-Datenschutzgruppe hat diese Anforderungen, bezogen auf die insoweit identische Vorschrift des Art. 2 lit. a DSRL, wie folgt zusammengefasst:

> *Ist „die Reidentifizierung in Übermittlungs- und Verfahrensvorschriften ausgeschlossen" und ist „die Identifizierung … keinesfalls beabsichtigt oder zu erwarten, weswegen geeignete technische Maßnahmen (z.B. Verschlüsselung, nicht rücknehmbares Hashing) getroffen wurden, die genau dies verhindern sollen, … sind die vom ursprünglichen Verantwortlichen verarbeiteten Informationen nicht als Daten anzusehen, die sich auf bestimmte oder bestimmbare Personen beziehen, wenn alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden. Die Bestimmungen der Richtlinie finden somit auf ihre Verarbeitung keine Anwendung." Dies soll selbst dann gelten, „wenn ungeachtet aller Übermittlungsvorschriften und Maßnahmen (aufgrund unvorhersehbarer Umstände wie die zufällige Zuordnung von Eigenschaften, die die Identität einzelner Personen offenbaren) einzelne Personen identifiziert werden".*[136]

Wenn geprüft wird, welche Daten in einem zu beurteilenden Fall in personenbezogener Form vorliegen, ist nach diesen Kriterien zu verfahren. Um feststellen zu können, für welchen Verantwortlichen oder Auftragsverarbeiter und für welchen Datenverarbeitungsvorgang Datenschutzrecht anwendbar ist, ist differenziert zu untersuchen, bei welcher Stelle in welcher Phase der Datenverarbeitung Daten vorliegen, für die ein Personenbezug hergestellt werden kann.

133 *Ziebarth*, in: Sydow, Art. 4 Rn. 23, 37; *Brink/Eckhardt*, ZD 2015, 205 (211); *Dammann*, in: Simitis, § 3 Rn. 28; *Meyerdierks*, MMR 2009, 8 (11f.), und *Krüger/Maucher*, MMR 2011, 433 (437f.), nehmen die „Kosten" illegalen Handelns in die Aufwand-Nutzen-Abwägung mit auf; s. auch *Kroschwald* 2015, 67.

134 Nicht durchsetzbare rechtliche Verbote in Drittstaaten reichen hierfür nicht aus – s. z.B. *Kroschwald* 2015, 68.

135 *Weichert*, in: Däubler u.a., § 3 Rn. 1.

136 Art. 29-Datenschutzgruppe, WP 136, 23, Hervorhebung im Original.

3.1.6 Ergebnis zum Personenbezug

Nur wenn ein Verantwortlicher personenbezogene Daten verarbeitet, untersteht er dem Datenschutzrecht. Sind die Daten nicht personenbezogen, greift Datenschutzrecht weder nach bisherigem noch nach zukünftigem Recht. Dementsprechend wichtig und umstritten ist der Begriff der personenbezogenen Daten.

Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, … identifiziert werden kann". Auch wenn sich der Wortlaut gegenüber Art. 2 lit. a DSRL und § 3 Abs. 1 BDSG a.F. unterscheidet, ist anerkannt, dass das Datenschutzrecht in der Datenschutz-Grundverordnung, in der Datenschutz-Richtlinie und im Bundesdatenschutzgesetz den gleichen Begriff verwendet.

Entscheidend ist die Frage, wie eine Person indirekt identifiziert werden kann – vor allem, welches Zusatzwissen dritter Personen für diese Feststellung zu berücksichtigen ist. Nach dem herrschenden und richtigen „relativen" Verständnis des Personenbezugs ist nur das Wissen zu berücksichtigen, das der Verantwortliche mit verhältnismäßigem Aufwand mobilisieren kann. Daher kann der Personenbezug relativ und von Verantwortlichem zu Verantwortlichem unterschiedlich sein. Diese Sichtweise wurde durch die Entscheidung des Europäischen Gerichtshofs vom 19. Oktober 2016 bestätigt.

Das Zusatzwissen, das der Verantwortliche „nach allgemeinem Ermessen wahrscheinlich"[137] nutzen wird, ist für die praktischen Probleme des Datenschutzes aus einer Risikoprognose zu bestimmen. Danach sind alle relevanten objektiven Faktoren zu beachten: der zeitliche Aufwand, die finanziellen Mittel, verfügbare Technologien und technologische Entwicklungen sowie das Interesse an der Zuordnung und die Folgen für die betroffene Person. Die Prognose muss mindestens die Entwicklungsmöglichkeiten in dem Zeitraum berücksichtigen, für den die Daten verarbeitet werden sollen. Das Zusatzwissen Dritter ist dann relevant, wenn die Dritten die Daten vom Verantwortlichen erhalten (sollen) oder sich beschaffen (können), wenn sie mit dem Verantwortlichen in irgendeiner Weise zusammenarbeiten (können), um die Person zu identifizieren, oder wenn sie ihr Zusatzwissen auf andere Weise dem Verantwortlichen zur Verfügung stellen können oder müssen. Das Zusatzwissen Dritter ist aber nur zu berücksichtigen, soweit „nach allgemeinem Ermessen" im konkreten Fall mit seinem Einsatz zu rechnen ist. Dies ist nicht der Fall, wenn die Verwendung des Zusatzwissens gesetzlich verboten ist und keine Anhaltspunkte für einen Rechtsbruch vorliegen. Ebenso sind gesetzliche Zugriffs-

137 Erwägungsgrund 26 Satz 3 DSGVO.

kompetenzen staatlicher Behörden nur zu beachten, wenn es für deren konkrete Ausnutzung Hinweise gibt.

3.2 Anonymisierung personenbezogener Daten

Das folgende Kapitel beantwortet die Frage 4.3. Diese lautet:

> *Bitte vergleichen Sie die bisherige Definition des Anonymisierens nach BDSG mit dem Erwägungsgrund 26 der EU-DSGVO und führen Sie aus, wo aus Ihrer Sicht Unterschiede im Vergleich zur bisherigen Rechtslage bei der Nutzung anonymer Daten für die wissenschaftliche Forschung bestehen.*

Eng mit dem Begriff der personenbezogenen Daten ist der Begriff der anonymen Daten verbunden. Diese sind Angaben zu einer betroffenen Person, die ihr nicht zugeordnet werden können. Sie fallen daher nicht unter den Begriff der personenbezogenen Daten und daher auch nicht unter das Datenschutzrecht.[138] Diese Daten können vom Zeitpunkt ihrer Entstehung her anonym sein, sie können aber auch aus personenbezogenen Daten entstehen, indem sie dadurch anonymisiert werden, dass ihnen alle potenziellen Zuordnungsmerkmale entfernt werden.

3.2.1 Anonymisierung nach der Datenschutz-Grundverordnung

Anonyme Daten und Anonymisierung werden in keiner Vorschrift der Datenschutz-Grundverordnung genannt, aber in vielen Vorschriften als existent unterstellt und in Erwägungsgrund 26 Satz 5 und 6 DSGVO erwähnt. Diese beiden Sätze in dem Erwägungsgrund zu personenbezogenen Daten lauten:

> *„Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."*

Sowohl in Satz 5 als auch in Satz 6 wird die Rechtsfolge festgehalten: Anonyme Daten unterfallen nicht der Datenschutz-Grundverordnung. Sie ergibt sich nicht aus dem Erwägungsgrund,[139] sondern aus der Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO. Die Rechtsfolge gilt auch, wenn die anonymen Daten für Forschungszwecke verarbeitet werden. Diese Rechtsfolge

138 *Roßnagel/Scholz*, MMR 2000, 721 (723); *Weichert*, in: Däubler u.a., § 3 Rn. 49; *Kroschwald* 2015, 72.
139 S. hierzu Kap. 3.1.5.2.

dürfte auch der Grund sein, warum die Datenschutz-Grundverordnung keine Regelung für anonyme Daten – auch keine Definition – enthält.

Satz 5 benennt anonyme Daten, für die diese Rechtsfolge gilt. Danach gibt es zwei Arten anonymer Daten. Zum einen können Daten deshalb anonym sein, weil sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Ihnen fehlen von Anfang an Merkmale, die es ermöglichen, sie einer bestimmten natürlichen Person zuzuordnen. Zum anderen können Daten anonym sein, weil sie in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. In dieser Alternative waren Daten personenbezogen, haben dann aber durch einen Anonymisierungsprozess die Merkmale verloren, die zuvor ermöglicht haben, die von ihnen betroffene Person zu identifizieren.[140] In beiden Varianten wird die Anonymität von ihrem Ergebnis her definiert und ist in beiden Varianten gleich: Die Daten sind deshalb anonym, weil sie keine Zuordnung zu einer bestimmten Person ermöglichen.[141]

Anonyme Daten sind das Gegenteil von personenbezogenen Daten.[142] Sie grenzen sich definitorisch von diesen dadurch ab, dass sie gerade keine personenbezogenen Daten sind.[143] Anonymisierung und Personenbezug korrelieren insofern negativ. Daten sind anonym und damit nicht identifizierbar, wenn sie mit den verfügbaren Mitteln nach allgemeinem Ermessen nicht einer bestimmten Person zugeordnet werden können. Die Begriffe der anonymen Daten und nicht-personenbezogenen Daten weichen im Wesentlichen in einem Punkt voneinander ab: Soweit ein anderes Merkmal als die Bestimmbarkeit aus der Begriffsdefinition der personenbezogenen Daten zu verneinen ist und entsprechend kein Personenbezug vorliegt, sind die Daten nicht automatisch anonym. Handelt es sich beispielsweise um keine Einzelangaben, beschreiben die Informationen keine persönlichen oder sachlichen Verhältnisse oder beziehen sich diese Informationen nicht auf eine natürliche Person, kann auch nicht von anonymen Daten gesprochen werden.[144] Es sind vielmehr Informationen, die zu keiner (natürlichen) Person gehören.[145] Entscheidend ist, dass die Daten zwar Angaben zu einer bestimmten Person enthalten, dass mit ihnen aber kein Bezug zu einer identifizierten oder identifizierbaren natürlichen Person hergestellt werden kann. Da sie keiner natürlichen Person zugeordnet werden können, geht von ihnen auch kein Risiko aus. Das ist der inhaltliche Grund, warum sie von der Datenschutz-Grundverordnung nicht erfasst werden.

140 *Roßnagel/Scholz*, MMR 2000, 721 (723).
141 *Forgó/Krügel*, MMR 2010, 19; *Meyerdierks*, MMR 2009, 10; *Kroschwald* 2015, 57f.
142 S. z.B. *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 31.
143 S. *Hofmann/Johannes*, ZD 2017, 223.
144 S. z.B. *Kroschwald* 2015, 71f.
145 *Roßnagel/Scholz*, MMR 2000, 721 (723).

Die Datenschutz-Grundverordnung hat anonyme Daten – im Gegensatz zu § 3 Abs. 6 BDSG a.F. und § 67 Abs. 8 SGB X a.F. – nicht definiert. Ebenso haben das neue Bundesdatenschutzgesetz und das neue Sozialgesetzbuch wie die Datenschutz-Grundverordnung auf eine Definition verzichtet. Daher kann ihr auch keine ausdrückliche Antwort auf die Frage entnommen werden, mit welcher Wahrscheinlichkeit der Personenbezug der Daten ausgeschlossen sein muss. Diese Antwort bietet auch Erwägungsgrund 26 DSGVO nicht. Dort heißt es nur, dass sich die Daten „nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen" und dass „die betroffene Person nicht oder nicht mehr identifiziert werden kann". Da diese Frage nur die nach personenbezogenen Daten umkehrt, kann auf die Ausführungen zu personenbezogenen Daten[146] Bezug genommen werden. Entsprechend den Ausführungen in Kapitel 3.5 ist diese Frage nach dem dort beschriebenen pragmatischen Konzept zu beantworten.[147]

Ob die Daten anonym sind und einen Personenbezug ausschließen, ist – ausgehend von einem relativen Konzept[148] – nach einer Risikoprognose zu bestimmen, die sowohl das Interesse möglicher Datenverarbeiter als auch die von ihnen mobilisierbaren Mittel der Zuordnung berücksichtigt. Diese Sichtweise liegt der Definition des § 3 Abs. 6 BDSG a.F. und des § 67 Abs. 8 BDSG X a.F. zugrunde, nach der die Daten dann anonym sind, wenn „sie nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können". Nach dieser im geltenden Recht zu findenden pragmatischen Sichtweise kann für die Bewertung als anonym die Zuordnung zwar theoretisch möglich sein, muss aber mit einer jeweils ausreichenden Wahrscheinlichkeit ausgeschlossen sein. Die Zuordnung muss im Verhältnis zu dem dazu notwendigen Aufwand so unverhältnismäßig sein, dass eine Identifizierung nach allgemeiner Lebenserfahrung oder dem Stand der Wissenschaft und Technik nicht zu erwarten ist.[149] Zu berücksichtigen sind dabei das vorhandene oder erwerbbare Zusatzwissen des Verantwortlichen, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit.[150] In diese Betrachtung müssen aber zusätzlich zur Verhältnismäßigkeit des Aufwands für den jeweiligen Datenverarbeiter auch die möglichen Folgen für die jeweils betroffene Person eingehen. Danach wären die Daten dann anonym, wenn die Wahrscheinlichkeit der Zuordnung zu einer betroffenen Person angesichts des Verhältnisses von Nutzen und Aufwand für den jeweiligen Datenverarbeiter und angesichts der jeweiligen Gefährdung der Grundrechte der betroffenen Person ausreichend gering ist. Ein absoluter Ausschluss der

146 S. insb. Kap. 3.1.5.
147 Nach *Laue/Nink/Kremer* 2016, § 1 Rn. 19 ist davon auszugehen, dass die bisherigen Definitionen von anonymen und anonymisierten Daten ihre Gültigkeit behalten.
148 S. Kap. 3.1.3 bis 3.1.5.
149 *Roßnagel/Scholz*, MMR 2000, 721 (724); *Härting*, NJW 2013, 2065 (2066); *Laue/Nink/Kremer* 2016, § 1 Rn. 21.
150 *Roßnagel/Scholz*, MMR 2000, 721 (724); *Laue/Nink/Kremer* 2016, § 1 Rn. 21

Zuordnung ist nicht erforderlich. In der Literatur wird diese pragmatische Sichtweise[151] als faktische Anonymität bezeichnet.[152]

Diese Bestimmungen einer ausreichenden Anonymität entsprechen den Argumenten für die Abgrenzung von personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO.[153] Hier wie dort geht es um die Bestimmung des relevanten Zusatzwissens für die Definition personenbezogener Daten. Allerdings ist die Argumentation durch eine fehlende Definition anonymer Daten in der Datenschutz-Grundverordnung erschwert.

Es ist daher ergänzend zu prüfen, ob andere Vorschriften der Datenschutz-Grundverordnung als Art. 4 DSGVO andere Hinweise auf das Verständnis von anonymen Daten liefern. Einen solchen Hinweis könnte Art. 89 Abs. 1 DSGVO bieten. Diese Öffnungsklausel für die Regelung verschiedener Verarbeitungszwecke, u.a. Forschungszwecke, fordert in Satz 4, die Daten nur noch ohne Personenbezug weiterzuverarbeiten, wenn der Forschungszweck den Personenbezug nicht mehr erfordert. Die Verordnung fordert somit eine Anonymisierung von Daten, ohne diesen Begriff ausdrücklich zu benennen. Diese Vorschrift beinhaltet keine ausdrückliche Erklärung für das geforderte Maß an Anonymisierung. Sie führt aber zu folgender Überlegung:[154] Wollte die Verordnung einen absoluten Ausschluss der Zuordnung, also auf die Möglichkeiten aller Menschen zur Identifizierung abstellen, bestünde die Möglichkeit zur Anonymisierung kaum mehr und würde die Weiterverarbeitung von Daten für viele Forschungsinstitutionen ausgeschlossen. Angesichts des Grundrechts auf Forschung in Art. 13 GRCh (und Art. 5 Abs. 3 GG) sprechen die besseren Argumente dafür, dass die Verordnung auf das Potenzial des Verantwortlichen zur Re-Identifizierung abstellt, auf die er oder ein Dritter „nach allgemeinem Ermessen wahrscheinlich" zurückgreifen kann. Das Gleiche gilt für jene Dritte, die „nach allgemeinem Ermessen" die Identifizierung der betroffenen Person betreiben könnten. Das können wissenschaftliche Kooperationspartner, interessierte Unternehmen, aber auch staatliche Stellen mit Zugriffsrechten sein, nicht aber alle Dritte weltweit. Für staatliche Stellen genügt jedoch nicht die abstrakte gesetzliche Möglichkeit, sondern es muss „nach allgemeinem Ermessen" damit gerechnet werden können, dass sie auf die (scheinbar) anonymen Daten zugreifen und mit diesen die betroffene Person identifizieren.[155]

Im Ergebnis ist daher festzuhalten: Erwägungsgrund 26 Satz 5 und 6 DSGVO erläutert den Begriff der personenbezogenen Daten in Art. 4 Nr. 1 DSGVO durch den Rückgriff auf den Begriff der anonymen oder anonymisierten Daten.

151 S. z.B. *Dammann*, in: Simitis, § 3 Rn. 23; *Gola/Schomerus*, § 3 Rn. 43f.; *Hornung*, DuD 2004, 429; *Roßnagel/Scholz*, MMR 2000, 721 (724ff.); *Buchner*, in: Taeger/Gabel, § 3 Rn. 44.

152 S. z.B. *Härting*, NJW 2013, 2065; *Laue/Nink/Kremer*, § 1 Rn. 21; *Ziebarth*, in: Sydow, Art. 4 Rn. 98.

153 S. Kap. 3.1.5.

154 S. zu dieser *Hofmann/Johannes*, ZD 2017, 223.

155 S. z.B. *Brink/Eckhardt*, ZD 2015, 211;

Er verwendet dabei diesen Begriff in einer Weise, die dem bisherigen Verständnis der pragmatischen Sichtweise einer faktischen Anonymität[156] entspricht.[157]

3.2.2 Anonymisierung nach § 27 Abs. 3 BDSG-neu

§ 27 BDSG-neu enthält in Ausfüllung der Öffnungsklausel in Art. 89 Abs. 1 DSGVO besondere Regelungen für die Datenverarbeitung zu Forschungs- und Statistikzwecken. Abs. 3 enthält Vorgaben zu geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person für den Fall, dass der Verantwortliche besondere Kategorien personenbezogener Daten verarbeitet. § 27 Abs. 3 BDSG-neu lautet:

> *„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."*

Der amtlichen Begründung zu § 27 Abs. 1 BDSG-neu kann entnommen werden, dass die gesamte Vorschrift des § 27 BDSG für „die öffentliche und private Forschung durch öffentliche und nicht-öffentliche Stellen gilt".[158] Abs. 3 wird in der amtlichen Begründung nur mit dem Hinweis erläutert, dass diese Regelung § 40 Abs. 2 BDSG a.F. „entlehnt" ist.[159]

Sie ist jedoch nicht mit § 40 Abs. 2 BDSG a.F. identisch. Denn dessen Satz 1 lautet:

> *„Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist."*

§ 40 Abs. 2 Satz 1 BDSG a.F. ist auf Forschungsinstitutionen beschränkt und bezieht sich auf alle personenbezogenen Daten, die zu Forschungszwecken verarbeitet werden. Die Vorschrift fordert, diese zu anonymisieren, sobald dies möglich ist. § 27 Abs. 3 Satz 1 BDSG-neu gilt dagegen auch für Statistik-

156 S. Fn. 149f.
157 S. z.B. *Laue/Nink/Kremer*, § 1 Rn. 21; *Gola*, in: Gola, Art. 4 Rn. 40; *Ziebarth*, in: Sydow, Art. 4 Rn. 98; *Schantz*, in: Schantz/Wolff, Rn. 297ff.; *Husemann*, in: Roßnagel 2018, § 3 Rn. 7.
158 BT-Drs. 18/11325, 98; *Greve*, NVwZ 2017, 737 (739).
159 BT-Drs. 18/11325, 98.

zwecke und schränkt die Forderung nach Anonymisierung auf besondere Kategorien personenbezogener Daten ein.[160]

Mit § 27 Abs. 3 BDSG-neu setzt der deutsche Gesetzgeber Art. 9 Abs. 2 lit. j DSGVO in Bezug auf Gesundheitsdaten um. Art. 9 Abs. 2 lit. j DSGVO erlaubt dem Mitgliedstaat jedoch nicht, Regelungen zu Daten zu treffen, die nicht Gesundheitsdaten sind. Auch ist er nach dieser Öffnungsklausel nicht befugt, Regelungen zur Datenverarbeitung in der Forschung zu treffen. Für die Datenverarbeitung in der Forschung ist – auch wenn es um medizinische Forschung geht – Art. 89 DSGVO die speziellere Norm. Daher muss der deutsche Gesetzgeber sowohl zur Forschung mit Gesundheitsdaten als auch zur Forschung mit anderen Daten Art. 89 Abs. 1 DSGVO beachten.

Art. 89 Abs. 1 DSGVO fordert in Satz 1, dass „die Verarbeitung zu … Forschungszwecken … geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung" unterliegt. Nach Satz 2 soll „mit diesen Garantien … sichergestellt (werden), dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird". Hierzu sollen nach der missglückten Formulierung in Satz 4 „in allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, … diese Zwecke auf diese Weise erfüllt" werden. Die Anonymisierung der Daten, die nicht mehr als personenbezogene Daten für Forschungszwecke benötigt werden, ist eine gesetzlich vorgesehene Garantie, die Art. 89 Abs. 1 Satz 1 DSGVO fordert. Die englische Fassung des Art. 89 Abs. 1 Satz 4 DSGVO lautet:

> *"Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."*

Sie wird durch die deutsche Sprachfassung korrekt wiedergegeben. Das in der englischen Fassung verwendete Wort „shall" bedeutet im Deutschen kein „soll", sondern – wie in allen anderen Regelungen der Verordnung, in denen das Hilfsverb „shall" genutzt wird – ein „muss".

Diesen Anforderungen des Art. 89 Abs. 1 DSGVO wird § 27 Abs. 3 BDSG-neu nicht gerecht. Weder die Garantien nach Art. 89 Abs. 1 Satz 1 DSGVO noch die Pflicht zur Anonymisierung nach Art. 89 Abs. 1 Satz 4 DSGVO sind auf besondere Kategorien personenbezogener Daten beschränkt. Indem § 27 Abs. 3 Satz 1 BDSG-neu – im Gegensatz zu § 40 Abs. 2 Satz 1 BDSG a.F. – diese Einschränkung vornimmt, verstößt die Vorschrift gegen Art. 89 Abs. 1 Satz 1 und 4 DSGVO und ist unionsrechtswidrig.[161] In dieser Hinsicht greift der Anwendungsvorrang

160 *Johannes/Richter*, DuD 2017, 300 (304).
161 *Johannes/Richter*, DuD 2017, 300 (302).

der Unionsverordnung und es gilt allein Art. 89 Abs. 1 Satz 4 DSGVO für alle personenbezogenen Daten.[162]

Außerdem kann nach Art. 89 Abs. 1 Satz 4 DSGVO von der Anonymisierung nur abgesehen werden, wenn dies zu Forschungszwecken zwingend erforderlich ist. Daher ist auch die Ausnahme in § 27 Abs. 3 Satz 1 BDSG-neu unionsrechtswidrig, nach der die Anonymisierung entfallen kann, wenn „berechtigte Interessen der betroffenen Person … dem entgegen" stehen.[163] Die Ausnahme kann nicht angewendet werden.[164]

Soweit § 27 Abs. 3 Satz 1 BDSG-neu eine Anonymisierung vorsieht, entspricht dies der „Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist", in Art. 89 Abs. 1 Satz 4 DSGVO und der Beschreibung der Anonymisierung in Erwägungsgrund 26 Satz 5 DSGVO. Auch § 27 Abs. 3 Satz 1 BDSG-neu erwähnt die zwei Entstehungsmöglichkeiten anonymer Daten, die in Erwägungsgrund 26 Satz 5 DSGVO genannt sind. Insofern ergibt sich aus § 27 Abs. 3 Satz 1 BDSG-neu kein anderer Bedeutungsgehalt als der in Erwägungsgrund 26 Satz 5 DSGVO.[165]

3.2.3 Anforderungen an die Anonymisierung für die wissenschaftliche Forschung

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Anonymisierung vor. Vielmehr muss der Datenverarbeiter im Ergebnis die in Art. 4 Nr. 1 DSGVO niedergelegten Kriterien erfüllen, die eine Einordnung der Daten als personenbezogen ausschließen.[166] Ob ein Personenbezug ausgeschlossen ist, richtet sich nicht nach der Einhaltung eines bestimmten Verfahrens, sondern nach dem Erreichen des notwendigen Ergebnisses: Eine Identifizierbarkeit der betroffenen Person muss mit den verfügbaren Mitteln nach allgemeinem Ermessen ausgeschlossen sein.

Für eine Anonymisierung muss der Personenbezug für alle Beteiligten irreversibel entfernt sein.[167] Nach dem Maßstab der faktischen Anonymität[168] ist auszuschließen, dass diese nicht oder nur unter unverhältnismäßigem Aufwand in der Lage sind, die Daten einer natürlichen Person zuzuordnen. Nur soweit eine Zuordnung der anonymen Daten nach der allgemeinen Lebenserfahrung oder – in Ermangelung entsprechender Erfahrungswerte – auf Grundlage einer

162 Im Ergebnis ebenso *Greve*, NVwZ 2017, 737 (739), der die Datenschutz-Grundverordnung für die Daten, die nicht besonderen Kategorien unterfallen, ergänzend anwenden will.
163 *Johannes/Richter*, DuD 2017, 300 (304).
164 Lebenswichtige Interessen der betroffenen Person können nach Art. 6 Abs. 1 UAbs. 1 lit. d DSGVO berücksichtigt werden.
165 S. hierzu Kap. 3.1.5.2.
166 S. z.B. *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 33; *Klabunde*, in: Ehmann/Selmayr, Art. 4 Rn. 16.
167 *Dammann*, in: Simitis, § 3 Rn. 200.
168 S. Kap. 3.2.1 und insb. Fn. 149f. und 155.

Risikoprognose auf dem Stand der Wissenschaft nicht zu erwarten ist,[169] ist ein ausreichendes Maß der Anonymisierung erreicht.[170] Dabei sind nach Erwägungsgrund 26 Satz 4 DSGVO auch zukünftige „technologische Entwicklungen", die gegebenenfalls eine Re-Identifikation ermöglichen, zu berücksichtigen.[171]

Die Methode der Anonymisierung hängt vom Aufbau und Inhalt des jeweiligen Datenbestands ab.[172] Unerlässlich ist wohl die irreversible Entfernung und Löschung der expliziten oder direkten Identifikationsmerkmale wie Namen und Anschriften, Personenkennzeichen, Kontonummern.[173] Dies kann aber in vielen Fällen unzureichend sein, insbesondere wenn der Verantwortliche Zusatzwissen mobilisieren kann, das dann auch ohne direkte Identifikationsmerkmale eine Identifizierung ermöglicht. Weitere Maßnahmen[174] sind etwa die Merkmalsaggregation, also das Ersetzen konkreter Angaben durch allgemein gehaltene Ersatzangaben,[175] oder auch der kontrollierte Einbau von Zufallsfehlern.[176] Stärken und Schwächen von Anonymisierungstechniken hat die Art. 29-Datenschutzgruppe analysiert.[177]

Nach Erwägungsgrund 26 Satz 4 DSGVO sind bei der Feststellung des Personenbezugs von Daten „alle objektiven Faktoren, wie ... die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen". Daraus folgt, dass die eingesetzten Anonymisierungsverfahren dem aktuellen Stand der Technik[178] und den absehbaren technischen Entwicklungen im Zeitraum der Datenspeicherung entsprechen müssen.

Ist das Risiko einer Re-Identifizierung entscheidendes Differenzierungsmerkmal zwischen anonymen und personenbeziehbaren Daten, erfordert die Dynamik der Risikoentwicklung zwei Reaktionen: Zum einen ist bei der Festlegung der Anonymisierungsverfahren eine „Schutzreserve" vorzusehen, die zukünftigen Risiken vorbeugt.[179] Zum anderen ist eine einmalige Risikoanalyse unzureichend. Insbesondere wenn die anonymen Daten zur Datenanalyse (etwa im Zusammenhang mit „Big Data-Anwendungen" oder bei „Webtracking Tools") genutzt werden, ist regelmäßig zu prüfen, ob im Laufe der

169 *Roßnagel/Scholz*, MMR 2000, 724.
170 *Kroschwald* 2015, 72f.
171 Für die DSGVO z.B. *Marnau*, DuD 2016, 428, (429); *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 24; *Kühling/Klar*, NJW 2013, 3611 (3613); *Schantz*, in: Schatz/Wolf 2017, Rn. 283. *Hofmann/Johannes*, ZD 2017, 221 (224f.); *Krügel*, ZD 2017, 455 (456); für die DSRL bereits z.B. Art. 29-Datenschutzgruppe, WP 136, 18; *Kroschwald* 2015, 60; *Weichert*, in: Däubler u.a., § 3 Rn. 47.
172 *Dammann*, in: Simitis, § 3 Rn. 205.
173 S. zu diesen z.B. *Dammann*, in: Simitis, § 3 Rn. 206.
174 Verfahren der Anonymisierung – *Dammann*, in: Simitis § 3 Rn. 209
175 Z.B. indem bei einer Altersangabe der Wert „103 Jahre" durch die Gruppierung „Alter über 80 Jahre" ersetzt wird, *Dammann*, in: Simitis, § 3 Rn. 207.
176 *Dammann*, in: Simitis, § 3 Rn. 207ff.
177 Art. 29-Datenschutzgruppe, Stellungnahme 5/2014, WP 216, 13ff. und Anhang, 33ff.
178 So *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 33.
179 *Schaar*, ZD 2016, 224 (225).

Zeit erworbenes Zusatzwissen, etwa durch verbesserte Analyse- und Verknüpfungsmöglichkeiten, nicht zwischenzeitlich eine Identifizierung der ursprünglich anonymen Daten ermöglicht.[180]

3.2.4 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Die Datenschutz-Richtlinie kennt ebenfalls keine Regelung zur Anonymisierung. Sie wird lediglich in Erwägungsgrund 26 Satz 3 DSRL erwähnt.[181] Dieser ist im Wesentlichen identisch mit der Erwähnung der Anonymisierung in Erwägungsgrund 26 Satz 5 DSGVO. Wie nach der Datenschutz-Grundverordnung ergibt sich das Verständnis der anonymen Daten und der Anonymisierung aus der Umkehr der Definition personenbezogener Daten in Art. 2 lit. a DSRL. Insofern können alle Erkenntnisse zur Anonymisierung nach der Datenschutz-Richtlinie auch auf die Datenschutz-Grundverordnung übertragen werden.

Dagegen hat das Bundesdatenschutzgesetz a.F. „Anonymisieren" in § 3 Abs. 6 wie folgt definiert:

> *Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.*

Die Definition in § 67 Abs. 8 SGB X a.F. ist bis auf den Austausch der Worte „personenbezogener Daten" durch „Sozialdaten" mit der Definition in § 3 Abs. 6 BDSG a.F. identisch.

Danach sind Daten „anonym" und damit nicht personenbezogen,[182] wenn sie nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können. Für diese faktische Anonymität ist ein vollständiger Ausschluss der Zuordnung der Daten zu einer bestimmten Person nicht erforderlich. Dies entspricht auch dem Erwägungsgrund 26 Satz 5 DSGVO. Sowohl nach diesem Erwägungsgrund als auch nach § 3 Abs. 6 BDSG a.F. und § 67 Abs. 8 SGB X a.F. genügt eine faktische Anonymisierung.[183]

Daher ist festzustellen, dass die Datenschutz-Grundverordnung weder für den Begriff noch für die Funktion für die Rechtsfolgen der Anonymisierung und

180 *Laue/Nink/Kremer* 2016, § 1 Rn. 22.
181 S. den Text des Erwägungsgrunds 26 in Kap. 3.1.3.
182 S. z.B. *Gola/Schomerus*, § 3 Rn. 11, 43; *Buchner*, in: Taeger/Gabel, § 3 Rn. 44f.; 9; *Roßnagel/Scholz* MMR 2000, 723f.; *Roßnagel*, digma 2011, 161; *Schaar*, ZD 2016, 224 (225); dagegen Verwirrung suchend *Härting*, NJW 2013, 2066.
183 *Schaar*, ZD 2016, 224 (225).

anonymer Daten gegenüber der Rechtslage unter dem bisherigen Bundesdatenschutzgesetz und dem bisherigen Sozialgesetzbuch wesentliche Änderungen gebracht hat.

Zur Erläuterung dieses Ergebnisses sei noch einmal darauf hingewiesen, dass die Datenschutz-Grundverordnung weder eine Definition noch eine Regelung zur Anonymität von Daten und ihrer Rechtsfolgen enthält. Der Begriff der Anonymität von Daten muss aus dem Begriff des Personenbezugs von Daten als dessen Gegenteil erschlossen werden. Hierzu hält die Erläuterung von personenbezogenen Daten in Erwägungsgrund 26 Satz 5 und 6 DSGVO nur fest, dass anonyme Daten, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen", nicht dem Datenschutzrecht unterfallen. Da Art. 4 Nr. 1 DSGVO den Begriff der personenbezogenen Daten in den wesentlichen Aspekten identisch mit den Definitionen in Art. 2 lit. a DSRL und § 3 Abs. 1 BDSG a.F. definiert, muss diese Identität auch für anonyme Daten als ihr Gegenteil gelten.

3.2.5 Ergebnis zur Anonymisierung

Anonyme Daten sind Angaben zu einer betroffenen Person, die ihr nicht zugeordnet werden können. Sie sind daher keine personenbezogenen Daten. Sie können von Anfang an anonym sein, aber auch aus personenbezogenen Daten entstehen, indem sie dadurch anonymisiert werden, dass aus ihnen alle potenziellen Zuordnungsmerkmale entfernt werden.

Anonyme Daten und Anonymisierung werden in keiner Vorschrift der Datenschutz-Grundverordnung genannt oder geregelt, aber in vielen Vorschriften als existent unterstellt und in Erwägungsgrund 26 Satz 5 und 6 DSGVO erwähnt. Das aus beiden Sätzen erkennbare Verständnis entspricht dem des § 3 Abs. 6 BDSG a.F.

§ 27 Abs. 3 BDSG-neu fordert eine Anonymisierung nur von besonderen Kategorien personenbezogener Daten, sobald dies nach dem Forschungszweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Diese Regelung verstößt insofern gegen die Datenschutz-Grundverordnung, als Art. 89 Abs. 1 Satz 4 DSGVO die Anonymisierung aller Forschungsdaten fordert und die Einschränkung wegen berechtigter Interessen der betroffenen Person nicht vorsieht. In beiden Fällen besteht ein Anwendungsvorrang der Verordnung.

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Anonymisierung vor. Vielmehr muss der Datenverarbeiter im Ergebnis die in Art. 4 Nr. 1 DSGVO niedergelegten Kriterien erfüllen, die eine Einordnung der Daten als personenbezogen ausschließen.

3.3 Pseudonymisierung personenbezogener Daten

Das folgende Kapitel beantwortet die Fragen 4.1 Satz 1 bis 3. Diese lauten:

> *Vergleichen Sie bitte den Pseudonymisierungsbegriff aus den bisherigen Vorschriften des BDSG mit jenen aus der EU-Datenschutzgrundverordnung. Sind diese gleichbedeutend oder ergeben sich unterschiedliche Anforderungen an den Pseudonymisierungsprozess? Gehen Sie in Bezug auf die bisherige Rechtslage bei der Nutzung pseudonymer Daten auch auf das EUGH-Urteil vom 19.10.2016 (Patrick Breyer gegen Bundesrepublik Deutschland, Aktz. C – 582/14) ein.*

Im Gegensatz zur Datenschutz-Richtlinie, die Pseudonymisierung gar nicht ausdrücklich berücksichtigt, und zum Bundesdatenschutzgesetz a.F., das Pseudonymisierung zwar in § 3 Abs. 6a BDSG a.F. definiert, aber nur in § 3a BDSG a.F. als eine beispielhafte Maßnahme der Datensparsamkeit erwähnt,[184] etabliert die Datenschutz-Grundverordnung Pseudonymisierung als den „Kernpfeiler" der technisch-organisatorischen Maßnahmen des Datenschutzes.[185]

3.3.1 Pseudonymisierung nach der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung nennt in vielen Vorschriften die Pseudonymisierung als zentrales Mittel, um die Rechte und Freiheiten der betroffenen Person zu wahren und ihr ausreichende Garantien zu bieten. So ist Pseudonymisierung in Art. 6 Abs. 4 lit. e DSGVO als angemessene Garantie bei der Bestimmung der Vereinbarkeit von Zwecken zu berücksichtigen.[186] Ebenso wird Pseudonymisierung in Art. 25 Abs. 1 DSGVO als ein Weg genannt, Privacy by Design umzusetzen.[187] Art. 32 Abs. 1 lit. a DSGVO nennt Pseudonymisierung als ein Instrument technisch-organisatorischer Sicherung des Datenschutzes.[188] Verhaltensregeln können nach Art. 40 Abs. 2 lit. d DSGVO Anforderungen an personenbezogene Daten branchenspezifisch konkretisieren. Art. 89 Abs. 1 Satz 3 DSGVO bietet Pseudonymisierung als eine der technisch-organisatorischen Maßnahmen an, um die von Art. 89 Abs. 1 Satz 1 DSGVO geforderten Garantien bei der Verarbeitung personenbezogener Daten für wissenschaftliche, statistische und archivarische Zwecke zu gewährleisten.[189]

Pseudonymisierung ist in Art. 4 Nr. 5 DSGVO folgendermaßen definiert:

184 S. *Scholz*, in: Simitis, § 3a Rn. 45ff.
185 *Marnau*, DuD 2016, 428 (430); *Albrecht/Jotzo* 2017, Teil 3 Rn. 4: „besonderer Stellenwert der Pseudonymisierung"; *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 5 Rn. 4: „leicht gesteigerte Bedeutung".
186 S. z.B. *Buchner/Petri*, in: Kühling/Buchner, Art. 6 Rn. 191.
187 Erwägungsgrund 78 DSGVO; s. z.B. *Barlag*, in: Roßnagel 2017, § 3 Rn. 225.
188 S. z.B. *Barlag*, in: Roßnagel 2017, § 3 Rn. 197.
189 S. hierzu auch Erwägungsgrund 156 DSGVO; s. hierzu z.B. *Johannes*, in: Roßnagel 2017, § 4 Rn. 63.

> *„Pseudonymisierung ist 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."*

Aufgrund dieser Definition in der Datenschutz-Grundverordnung haben das neue Bundesdatenschutzgesetz und das neue Sozialgesetzbuch auf eine eigene Definition der Pseudonymisierung verzichtet.

Im Rahmen des Erwägungsgrunds 26 DSGVO zur Definition personenbezogener Daten widmet sich Satz 2 der Pseudonymisierung und stellt fest:

> *„Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden."*

Die Literatur zur Datenschutz-Grundverordnung orientiert sich überwiegend am Wortlaut des Erwägungsgrunds und stellt ohne weitere Differenzierung fest, dass pseudonyme Daten personenbezogene Daten sind.[190]

Zwischen der Definition in Art. 4 Nr. 5 DSGVO und dem Erwägungsgrund 26 Satz 2 DSGVO besteht jedoch ein Widerspruch, den es aufzulösen gilt.[191] Nach Art. 4 Nr. 5 DSGVO können die pseudonymen Daten ohne zusätzliche Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Sie sind also für den Verantwortlichen, der keinerlei Möglichkeiten hat, die zusätzlichen Informationen zur Kenntnis zu nehmen, entsprechend der Definition in Art. 4 Nr. 1 HS 2 DSGVO keine personenbezogenen Daten. Dagegen sollen nach Erwägungsgrund 26 Satz 2 DSGVO genau diese Daten „als Informationen über eine identifizierbare natürliche Person betrachtet werden", also als personenbezogene Daten gelten. Dieser Widerspruch kann nur dadurch aufgelöst werden, dass die jeweiligen Aussagen präzisiert und damit eingeschränkt werden. Dabei sind die allgemeinen Regeln für die Feststellung personenbezogener Daten zu berücksichtigen.

Als identifizierbar wird eine natürliche Person nach Art. 4 Nr. 1 HS 2 DSGVO angesehen, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung … identifiziert werden kann". Dabei kommt es auf das vorhandene und in verhältnismäßiger Weise mobilisierbare Zusatzwissen des Verantwort-

190 S. z.B. *Albrecht/Jotzo* 2017, Teil 3 Rn. 4; *Klabunde*, in: Ehmann/Selmayr, Art. 4 Rn. 15; *Gola*, in: ders., Art. 4 Rn. 39, in Widerspruch zu Art. 4 Rn. 19f.; *Laue/Nink/Kremer* 2016, § 1 Rn. 26, in Widerspruch zu § 1 Rn. 29f.

191 Ein Problem sehen *Klar/Kühling*, in: Kühling/Buchner, Art. 4 Nr. 5 Rn. 12, ohne jedoch eine Lösung anzubieten.

lichen oder Auftragsverarbeiters an.[192] Dieses Zusatzwissen kann auch bei Dritten vorhanden sein, wenn der Datenverarbeiter eine praktisch realisierbare Möglichkeit hat, dieses zur Kenntnis zu nehmen.[193] Dies muss auch für pseudonyme Daten gelten. Wenn es praktisch ausgeschlossen ist, dass der Datenverarbeiter die Zuordnungsregel für die pseudonymen Daten erlangen kann, dann können die Daten entsprechend der Definition des Art. 4 Nr. 5 DSGVO von ihm „nicht mehr einer spezifischen betroffenen Person zugeordnet werden".[194]

Da dies der Definition in Art. 4 Nr. 5 DSGVO widersprechen würde, kann Satz 2 des Erwägungsgrunds 26 DSGVO nicht absolut verstanden werden.[195] Vielmehr ist dieser Satz so zu verstehen, dass die „einer Pseudonymisierung unterzogene(n) personenbezogene(n) Daten" dann „als Informationen über eine identifizierbare natürliche Person betrachtet werden" sollen, wenn sie „durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten". Dies ist dann der Fall, wenn der Datenverarbeiter irgendeine realistische Möglichkeit hat, die Zuordnungsregel für die pseudonymen Daten zu erlangen (oder auf andere Weise zuordnen kann). Dies ist immer dann der Fall, wenn die Zuordnungsregel beim Verantwortlichen oder Auftragsverarbeiter verbleibt (interne Pseudonymisierung). Dies gilt auch, wenn die Datenverarbeitung und die Aufbewahrung der Zuordnungsregel innerhalb des Verantwortlichen organisatorisch – etwa in unterschiedlichen Abteilungen – getrennt sind. Dies gilt schließlich auch dann, wenn zwar ein Dritter die Zuordnungsregel aufbewahrt, aber nicht sichergestellt ist, dass der Datenverarbeiter sie nicht erfahren kann.

Somit ist Erwägungsgrund 26 Satz 2 DSGVO mit der Definition in Art. 4 Nr. 5 DSGVO vereinbar, wenn in Satz 2 der Relativsatz als Bedingung verstanden wird. Umgekehrt ist Art. 4 Nr. 5 DSGVO mit Erwägungsgrund 26 Satz 2 DSGVO vereinbar, wenn durch die in Nr. 5 genannten Maßnahmen im Ergebnis sichergestellt ist, dass die pseudonymen Daten durch den Datenverarbeiter „nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden" können.

Nach diesem Verständnis von Definition und Erwägungsgrund gibt es somit zwei Arten von pseudonymen Daten mit unterschiedlichen Voraussetzungen und unterschiedlichen Rechtsfolgen.

Die erste Art pseudonymer Daten bewirkt, dass für den Verantwortlichen die Zuordnung der Daten zu einer bestimmten Person ausgeschlossen ist. Diese pseudonymen Daten sind vom Ergebnis her zu bestimmen. Sie sind, weil eine

192 S. Kap. 3.1.5.6 und 3.1.5.7.
193 S. näher Kap. 3.1.5.6 und 3.1.5.7.
194 Im Ergebnis ebenso *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 49 – Breyer; *Gola*, in: ders., Art. 4 Rn. 19f.; *Ziebarth*, in: Sydow, Art. 4 Rn. 91, 97.
195 So aber z.B. *Klabunde*, in: Ehmann/Selmayr, Art. 4 Rn. 15.

Identifizierung der betroffenen Person durch sie ausgeschlossen ist,[196] entsprechend der Definition in Art. 4 Nr. 1 DSGVO keine personenbezogenen Daten.[197] Insbesondere für den Gesundheitsbereich hat die Art. 29-Datenschutzgruppe festgestellt, dass pseudonyme Daten, wenn der Verantwortliche die Zuordnungsregel nicht kennen kann, keine personenbezogenen Daten sind.[198] Werden z.B. im Rahmen eines Forschungsprojekts mögliche Identifizierungsmerkmale ausreichend sicher von den erhobenen Nutzdaten getrennt und durch ein Pseudonym ersetzt und wird die Zuordnungsregel einer anderen unabhängigen Stelle übergeben (z.B. Notar), der sie den Forschenden nicht zugänglich machen darf, sind die Nutzdaten für die Forschenden anonym. Dies dürfte für die Nachnutzung der pseudonymen Nutzdaten durch andere Forscher aus einer anderen Forschungseinrichtung vielfach der Fall sein.

Die zweite Art pseudonymer Daten bewirkt, dass die Risiken der Datenverarbeitung für die betroffene Person vermindert werden.[199] Diese risikoreduzierende Wirkung erreichen sie dadurch, dass im Verarbeitungsprozess die zu verarbeitenden Daten und das Zusatzwissen, das die Identifizierung der betroffenen Person ermöglicht, sicher getrennt sind. Diese Sicherungen erreichen jedoch nicht das Niveau, dass eine Zuordnung der Daten durch den Datenverarbeiter ausreichend verlässlich ausgeschlossen ist. Diese zweite Art pseudonymer Daten sind für den Verarbeiter personenbezogen und unterfallen der Datenschutz-Grundverordnung.[200] Mit dieser zweiten, risikomindernden Art pseudonymer Daten würden z.B. Forschende arbeiten, die zwar in der Regel nur das Pseudonym kennen, aber in einem Ausnahmefall bei dem Inhaber der Zuordnungsregel die Aufhebung der Pseudonymität fordern können, um Inkonsistenzen oder Unplausibilitäten aufzulösen. Für sie wären die Nutzdaten nicht anonym, sondern personenbezogen.

Diese Unterscheidung kennen auch die Definitionen des § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F., wenn sie Pseudonymisieren definieren als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren". „Die Bestimmung des Betroffenen auszuschließen", entspricht der anonymisierenden Wirkung der Pseudonymisierung für den Verantwortlichen, der die Zuordnungsregel nicht kennen kann. „Die

196 S. zu den Anforderungen an diese Art der Pseudonymisierung Kap. 3.3.3.

197 S. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 47–49 – Breyer; *Ziebarth*, in: Sydow, Art. 4 Rn. 25, 91, 98; *Ziebarth*, CR 2015; 687 (691); *Laue/Nink/Kremer*, § 1 Rn. 29f.; *Knopp*, DuD 2015, 527 (528); *Kroschwald* 2015, 74; *Buchner*, in: Taeger/Gabel, § 3 Rn. 47f.; *Scholz*, in: Simitis, § 3 Rn. 217a; *Gola/Schomerus*, § 3 Rn. 46; *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 30; grundsätzlich *Roßnagel/Scholz*, MMR 2000, 721 (724f.); *Roßnagel/Pfitzmann/Garstka* 2002, 103; *Stiemerling/Hartung*, CR 2012, 60 (63). Unklar *Karg*, DuD 2015, 520 (524): „wirkt … anonym, ohne es ggfs. rechtlich zu sein"; a.A. z.B. *Schaar* 2002, 74.

198 Art. 29-Datenschutzuppe, WP 136, 20.

199 S. hierzu auch *Gola*, in: ders., Art. 4 Rn. 41.

200 S. zu den Anforderungen an diese Art der Pseudonymisierung Kap. 3.3.3.

Bestimmung des Betroffenen zu erschweren", entspricht der zweiten, der risikomindernden Art pseudonymer Daten. Diese pseudonymen Daten sind aber weiterhin personenbezogene Daten.[201]

Zwar unterscheidet sich der Wortlaut[202] der Definition von Pseudonymisierung in Art. 4 Nr. 5 DSGVO, die lautet

> *„Pseudonymisierung ist 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",*

vom Wortlaut der Definition in § 3 Abs. 6a BDSG a.F., die deutlich kürzer gefasst ist als

> *„Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."*

Bezogen auf die Nutzdaten fordern beide Definitionen, dass diese nach der Pseudonymisierung nicht mehr ohne die Zuordnungsregel einer spezifischen betroffenen Person zugeordnet werden können. Nach beiden Definitionen muss dadurch der Personenbezug der Nutzdaten ausgeschlossen sein. Im Gegensatz zu Art. 4 Nr. 1 DSGVO differenziert § 3 Abs. 6a BDSG a.F. diese Folge dahingehend, dass die Bestimmung des Betroffenen ausgeschlossen oder wesentlich erschwert sein kann. Diese zweite Alternative entsteht für die Datenschutz-Grundverordnung aber ebenfalls, wenn der Widerspruch zwischen Art. 4 Nr. 1 DSGVO und Erwägungsgrund 26 Satz 2 DSGVO durch ein Nebeneinander zweier möglicher Folgen aufgelöst wird.[203] In dieser Interpretation sind die Anforderungen an die Nutzdaten in beiden Definitionen identisch.[204]

Bezogen auf die Zuordnungsregel geht Art. 4 Nr. 1 DSGVO jedoch über die Definition in § 3 Abs. 6a BDSG hinaus. Während das Bundesdatenschutzgesetz a.F. den Umgang mit der Zuordnungsregel nur implizit durch die beiden Folgen regelt, nach denen die Zuordnung ausschließt oder erschwert, stellt die Datenschutz-Grundverordnung explizite Forderungen: Sie muss gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen

201 S. hierzu auch *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 30; *Knopp*, DuD 2015, 527 (528).
202 Zum Vergleich des Wortlauts des Art. 4 Nr. 5 und § 3a BDSG a.F. und § 67 Abs. 8a SGB X a.F. s. auch Kap. 3.3.4.
203 S. hierzu oben.
204 So z.B. auch *Gola*, in: Gola, Art. 4 Rn. 36.

unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können. Diese Forderung gilt für beide möglichen Folgen gleichermaßen – können sich aber danach unterscheiden, dass sie den Personenbezug der Nutzdaten ausschließen oder erschweren. Insofern enthält die Definition in Art. 4 Nr. 1 präzisiere Vorgaben als die Definition in § 3 Abs. 6a BDSG a.F., ist aber auch wie diese am Erfolg orientiert.

Für den Inhaber der Zuordnungsregel sind beide Arten pseudonymer Daten personenbezogen. Dies ist der entscheidende Unterschied zur Anonymisierung. Während eine wirksame Anonymisierung die Identifizierung der betroffenen Person auch für denjenigen ausschließt, der sie durchführt, behält derjenige, der eine Pseudonymisierung durchführt, zusätzliche Informationen (Zuordnungsregel), die ihm ermöglichen ein Pseudonym einer betroffenen Person zuzuordnen.[205]

Diese zweite Art risikomindernder pseudonymer Daten wird von Erwägungsgrund 28 DSGVO angesprochen:

> *„Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der ‚Pseudonymisierung' in dieser Verordnung ist nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen."*

Für die erste Art der Pseudonymisierung besteht der Anreiz darin, dass der Datenverarbeiter, der die Zuordnungsregel nicht kennen kann, keine personenbezogenen Daten verarbeitet und damit aus dem Anwendungsbereich der Datenschutz-Grundverordnung herausfällt. Die Anreize für die zweite Art der Pseudonymisierung, die nur risikomindernd, aber nicht anonymisierend wirkt, sind Thema des Erwägungsgrunds 29 DSGVO:

> *„Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden. Der für die Verarbeitung der personenbezogenen Daten Verantwortliche, sollte die befugten Personen bei diesem Verantwortlichen angeben."*

205 S. hierzu *Roßnagel/Scholz*, MMR 2000, 721ff.

Für die Pseudonymisierung der zweiten Art liegt der Anreiz für den Verantwortlichen in der Erleichterung der Datenverarbeitung. Mit der Verwendung pseudonymer Daten kann er

- eher eine für sich günstige Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO durchführen,
- eher eine mit dem Primärzweck vereinbare Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO annehmen,
- seiner Pflicht zu einer datenschutzfreundlichen Systemgestaltung nach Art. 25 Abs. 1 DSGVO genügen,
- sich seine Aufgabe der Datensicherung nach Art. 32 Abs. 1 DSGVO erleichtern,
- allgemein seiner Verantwortung nach Art. 5 Abs. 2 und 24 DSGVO gerecht werden,
- sich Benachrichtigungen bei Datenschutzverletzungen gemäß Art. 34 Abs. 3 lit. a DSGVO ersparen,
- leichter eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO bestehen und
- seiner Pflicht, ausreichende Garantieren für eine Datenverarbeitung für statistische, wissenschaftliche und archivarische Zwecke nach Art. 89 Abs. 1 Satz 1 und 3 DSGVO zu bieten, genügen.

Wie Erwägungsgrund 29 Satz 1 DSGVO ausdrücklich festhält, sollten durch risikomindernde Pseudonymisierung – gemäß Art. 6 Abs. 1 UAbs. 1 lit. f und Abs. 4 DSGVO – mit den pseudonymen Daten allgemeine Analysen bei demselben Verantwortlichen zulässig sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 4 Nr. 5 DSGVO getroffen hat. Dadurch sollen statistische Untersuchungen und ähnliche Maßnahmen in Unternehmen, Unternehmensgruppen[206] und Behörden, insbesondere aber auch in der Forschung möglich sein, obwohl es sich bei diesen pseudonymen Daten um personenbezogene Daten entsprechend Erwägungsgrund 26 Satz 2 DSGVO handelt. Die Pseudonymisierung kann der Verantwortliche in diesem Fall selbst vornehmen.[207]

3.3.2 Bewertung der Pseudonymisierung durch den Europäischen Gerichtshof

Das Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016[208] befasst sich zwar nicht ausdrücklich mit dem Thema der Pseudonymisierung, sondern mit der Frage des Personenbezugs von IP-Adressen, wenn ein Dritter über die relevanten Zusatzinformationen verfügt. Genau diese Konstellation kann aber auch bei pseudonymen Daten vorliegen. Von manchen werden IP-Adressen auch als

206 S. *Laue/Nink/Kremer* 2016, § 1 Rn. 31.
207 S. z.B. *Albrecht/Jotzo* 2017, Teil 3 Rn. 4
208 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Breyer.

pseudonyme Daten angesehen. Insofern können aus dem Urteil Schlussfolgerungen abgeleitet werden, wenn es um die Frage geht, ob die pseudonymen Daten für einen Verantwortlichen personenbezogen sind, wenn die Zuordnungsregel ihm unbekannt ist, aber bei einem Dritten liegt. Diese Frage bezieht sich nur auf die erste Art pseudonymer Daten, die die Wirkung anonymer Daten haben können. Folgende Erkenntnisse aus dem Urteil sind übertragbar:

Der Europäische Gerichtshof geht zwar von einem relativen Personenbezug aus. IP-Adressen stellen isoliert betrachtet kein personenbezogenes Datum dar.[209] Das muss auch für pseudonymisierte Daten gelten. Er hat aber festgestellt, dass nicht allein auf das Zusatzwissen des Verantwortlichen abzustellen ist, sondern dass unter bestimmten Bedingungen auch das Zusatzwissen eines Dritten relevant sein kann.[210] Dieses Zusatzwissen Dritter ist dem Verantwortlichen dann zurechenbar, wenn das Zusatzwissen des Dritten „ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann".[211] Der Gerichtshof nennt zwei Gründe, nach denen dies nicht der Fall ist. Erstens ist die Berücksichtigung des Zusatzwissens Dritter dann ausgeschlossen, „wenn die Identifizierung der betreffenden Person gesetzlich verboten" ist. Zweitens bleibt das Zusatzwissen Dritter unberücksichtigt, wenn die Identifizierung „praktisch nicht durchführbar" ist, „z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften" erfordert, sodass das Risiko einer Identifizierung de facto vernachlässigbar" ist.[212] Dabei sind auch mögliche Umwege, auf denen das Zusatzwissen zum Verantwortlichen gelangen kann, zu berücksichtigen. Auch wenn es nicht erlaubt ist, die Daten direkt zu übermitteln, kann es – wie im zu entscheidenden Fall – möglich sein, das Zusatzwissen über Akteneinsicht bei einer zuständigen Behörde zu erlangen.[213] In diesem Fall verfügt der Verantwortliche über vernünftigerweise einsetzbare rechtliche Mittel.[214]

Der Europäische Gerichtshof stellt letztlich auf das Risiko der Identifizierung ab. Dies entfällt, wenn die Preisgabe des Zusatzwissens und die Identifizierung der betroffenen Person „gesetzlich verboten" ist. Der Gerichtshof musste in dem zu entscheidenden Fall nicht darüber entscheiden, wie wahrscheinlich die Verwendung nur rechtswidrig zu erlangender Zusatzinformationen sein muss. So bleibt nach dem Urteil offen, ob die Risikoprognose auch den Anreiz rechtswidrigen Verhaltens, die Leichtigkeit der Grenzübertretung und Anhaltspunkte für die Gefahr eines nicht rechtskonformen Zugriffs auf das Zusatzwissen berücksichtigen muss.[215]

209 S. *Moos/Rothkegel*, MMR 2016, 845 (846).
210 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 43, Breyer.
211 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 44, Breyer.
212 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46, Breyer.
213 S. hierzu ausführlich *Moos/Rothkegel*, MMR 2016, 845 (846).
214 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 47–49, Breyer.
215 Dafür wohl *Kühling/Klar*, ZD 2017, 28.

3.3.3 Anforderungen an den Pseudonymisierungsprozess

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Pseudonymisierung vor. Sie erkennt jedoch die verwendeten Verfahren nur dann als Pseudonymisierung nach Art. 4 Nr. 5 DSGVO an, wenn sie zwei Voraussetzungen erfüllen. Sie müssen erstens die Daten so verarbeiten, dass sie „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können". Zweitens müssen die „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".

Allerdings fordert die Datenschutz-Grundverordnung – jedoch nicht ausdrücklich – ein bestimmtes Maß an Qualität der Pseudonymisierung.[216] Solche Qualitätsanforderungen ergeben sich aber indirekt durch die Einordnung der pseudonymen Daten in den Begriff der personenbezogenen Daten.[217] Je nach intendiertem Charakter der pseudonymen Daten sind unterschiedliche Anforderungen an den Pseudonymisierungsprozess zu stellen:

Sollen die pseudonymen Daten der ersten Art unterfallen und für den sie nutzenden Verantwortlichen die Eigenschaft anonymer Daten haben, dürfen sie im Ergebnis keine personenbezogenen Daten sein. Sie müssen also ausschließen, dass der Verantwortliche durch sie bestimmte natürliche Personen identifizieren kann. Hierfür gelten die gleichen Anforderungen wie für die Anonymisierung.[218] Ob ein Personenbezug ausgeschlossen ist, richtet sich nicht nach der Einhaltung eines bestimmten Verfahrens. Auch die gesonderte und gesicherte Aufbewahrung der „zusätzlichen Informationen" garantiert keine Anonymität. Vielmehr muss eine Identifizierbarkeit der betroffenen Person mit den verfügbaren Mitteln nach allgemeinem Ermessen ausgeschlossen sein.

Um ausreichend sicherzugehen, dass eine Identifizierung der betroffenen Person ausgeschlossen ist, muss neben einem guten Verfahren zum Ersetzen der identifizierenden Merkmale[219] auch die besondere Schwachstelle, das Vorhandensein zusätzlicher identifizierender Informationen, ausreichend abgesichert werden.

Die Wiederherstellbarkeit des Personenbezugs führt daher zu einem fortdauernden Schutzbedarf der betroffenen Person. Es muss dauerhaft sichergestellt sein, dass nur der berechtigte Inhaber der Zuordnungsregel über diese verfü-

216 *Marnau*, DuD 2016, 428 (430).
217 S. hierzu *Roßnagel/Scholz*, MMR 2000, 721 (723f.).
218 S. Kap. 3.2.3.
219 Art. 29-Datenschutzgruppe, Stellungnahme 5/2014, WP 216, 13ff.

gen kann und alle anderen sicher davon ausgeschlossen sind.[220] Dies kann zum einen dadurch gewährleistet werden, dass die Pseudonymisierung von einem vertrauenswürdigen unabhängigen Dritten durchgeführt wird, der auch die Zuordnungsregel aufbewahrt. Dieser muss ausreichende Garantien dafür bieten, dass er die Zuordnungsregel keinem anderen zur Kenntnis kommen lässt. Hier können die Kriterien des Europäischen Gerichtshofs für die Bestimmung personenbezogener Daten unter Zurechnung des Wissens Dritter[221] in umgekehrter Weise zur Anwendung kommen. Für den Verantwortlichen darf es keinen rechtlich möglichen Weg geben, die Zuordnungsregel zu erfahren, und auch keinen anderen praktisch gangbaren Weg, mit verhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskräften an die Zuordnungsregel zu gelangen.

Um besonders sicherzugehen, dass die pseudonymen Daten nur in den wenigen vorgesehenen Fällen (z.B. bei der medizinischen Forschung Kontakt mit der betroffenen Person in deren Interesse) zugeordnet werden können, kann eine mehrfache Pseudonymisierung erfolgen. Werden z.B. Daten in einem Krankenhaus gewonnen, kann dieses die erste Pseudonymisierung vornehmen, bevor die pseudonymen Daten an ein Forschungsprojekt weitergegeben werden. Dort kann dann ein Treuhänder die pseudonymen Daten ein zweites Mal pseudonymisieren und die Zuordnungsregel aufbewahren. Das Forschungsprojekt arbeitet dann mit faktisch anonymen Daten, da es selbst keine Möglichkeit hat, die betroffene Person zu identifizieren. Das Pseudonym kann nur aufgedeckt werden (und die betroffene Person kontaktiert werden), wenn zwei Stellen zusammenarbeiten, nämlich der Treuhänder und das Krankenhaus. Sollen die Daten aus dem Forschungsprojekt weitergegeben werden, empfiehlt sich eine dritte Pseudonymisierung durch das Forschungsprojekt.[222]

Sollen die pseudonymen Daten für den sie nutzenden Verantwortlichen die Eigenschaft von risikomindernden zusätzlichen Garantien für betroffene Personen haben, bleiben sie personenbezogene Daten. Sie sind allerdings in besonderer Weise gesichert, sodass von ihnen ein erheblich geringeres Risiko für die betroffenen Personen ausgeht als von sonstigen personenbezogene Daten. Für diese zweite Art pseudonymer Daten genügt ein Pseudonymisierungsverfahren, das die Anforderungen der gesonderten und gesicherten Aufbewahrung der „zusätzlichen Informationen" gemäß Art. 4 Nr. 5 DSGVO erfüllt. Für diese Art pseudonymer Daten ist keine Pseudonymisierung durch einen Dritten notwendig. Nach Erwägungsgrund 29 DSGVO ist für sie sogar eine interne Pseudonymisierung möglich, wenn der Verantwortliche „die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten". Hierfür hat er „sicherzustellen …, dass zusätzliche Informationen, mit denen die

220 *Knopp*, DuD 2015, 527 (529).
221 S. Kap. 3.3.2.
222 S. hierzu *Herbst*, DuD 2016, 371 (375).

personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden". In diesem Fall hat der Verantwortliche die bei ihm für die gesonderte Aufbewahrung „befugten Personen" anzugeben. Diese Personen sind in die Dokumentation nach Art. 30 DSGVO aufzunehmen. Die Sicherungsmaßnahmen für die gesondert aufbewahrte Zuordnungsregel müssen den Vorgaben des Art. 32 DSGVO entsprechen. Diese müssen sicherstellen, dass der Verantwortliche, der die pseudonymen Daten nutzt, keinen Zugang zu der Zuordnungsregel hat.

3.3.4 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Der Begriff „Pseudonymisieren" wurde erst im Jahr 2001 im Bundesdatenschutzgesetz und im Sozialgesetzbuch X legaldefiniert. Nach § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. ist Pseudonymisieren „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren".[223] Obwohl Art. 4 Nr. 5 DSGVO einen anderen Wortlaut hat, enthält er keine andere inhaltliche Aussage als § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F.[224]

Wie für Art. 4 Nr. 5 und Erwägungsgrund 26 Satz 2 DSGVO analysiert, kennen auch die Definitionen des § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. zwei Arten von pseudonymen Daten, nämlich solche, die in der Lage sind, „die Bestimmung des Betroffenen auszuschließen", und solche, die die Identifizierung wesentlich erschweren sollen. Dementsprechend ist auch für das Bundesdatenschutzgesetz und für das Sozialdatenschutzrecht anerkannt, dass es pseudonyme Daten geben kann, die für den Verantwortlichen, der ihre Aufdeckungsregel nicht kennen kann, anonyme Daten sein können,[225] und dass es pseudonyme Daten gibt, die personenbezogene Daten sind, weil sie die Identifikation des Betroffenen nur erschweren, aber nicht ausschließen. Wie für Art. 4 Nr. 5 DSGVO gibt es auch Gegenmeinungen, die dem Konzept einer absoluten Bestimmung personenbezogener Daten anhängen.[226]

Die Anforderung der gesicherten und getrennten Aufbewahrung der Zuordnungsregel, die in Art. 4 Nr. 5 DSGVO ausdrücklich aufgenommen ist, ist auch für § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. eine ungeschriebene, aber notwendige Voraussetzung, um von Pseudonymisieren und pseudonymen Daten reden zu können.[227]

223 Zum Vergleich des Wortlauts des Art. 4 Nr. 5 und § 3a BDSG a.F. s. auch Kap. 3.3.1.
224 S. Kap. 3.3.1 sowie aus der Literatur z.B. *Gola*, in: ders., Art. 4 Rn. 36.
225 *Scholz*, in: Simitis, § 3 BDSG, Rn. 217a ff.; *Roßnagel/Scholz*, MMR 2000, 721 (724); *Stiemerling/Hartung*, CR 2012, 60 (63); *Kroschwald* 2015, 74.
226 S. z.B. *Schaar* 2002, 74, Rn. 218; *Pahlen-Brandt*, DuD 2008, 34 (35).
227 *Roßnagel/Scholz*, MMR 2000, 721 (724); *Scholz*, in: Simitis, § 3 BDSG, Rn. 217a ff.

Das Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016[228] hat der absoluten Bestimmung des Personenbezugs eine klare Absage erteilt und im Rahmen des Konzepts eines relativen Personenbezugs Fragen zur Zuordnung von Zusatzwissen bei Dritten geklärt. Diese von ihm gegebenen Feststellungen gelten für die Datenschutz-Richtlinie und damit auch für § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. Sie entsprechen der von der herrschenden Meinung vertretenen Auffassung. Diese Feststellungen sind auch auf Pseudonyme nach Art. 4 Nr. 5 DSGVO übertragbar.[229]

Im Ergebnis ändert sich durch den Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25. Mai 2018 für den Begriff, die Funktion und die Rechtswirkungen der Pseudonymisierung nichts Wesentliches.

3.3.5 Ergebnis zur Pseudonymisierung

Pseudonymisierung wird – im Gegensatz zur Anonymisierung definiert – und zwar in Art. 4 Nr. 5 DSGVO. Trotz eines unterschiedlichen Wortlauts ist der Begriff in Art. 4 Nr. 5 DSGVO mit dem in § 3 Abs. 6a BDSG a.F. identisch. Im Unterschied zur Anonymisierung gibt es bei der Pseudonymisierung eine Stelle, die eine Re-Identifizierung vornehmen kann. Daher ist zwischen dem Inhaber der Zuordnungsregel und allen anderen, die die Zuordnungsregel nicht kennen, zu unterscheiden.

Von der Rechtsfolge her können in beiden Vorschriften zwei Arten von pseudonymen Daten unterschieden werden, je nachdem, ob sie die Zuordnung zu einer bestimmten Person für alle, die die Zuordnungsregel nicht kennen, ausschließen oder nur erschweren. Im ersten Fall sind pseudonyme Daten für den Verantwortlichen keine personenbezogenen Daten, im zweiten Fall bleiben sie es. Nicht personenbezogen sind pseudonyme Daten nach dem Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016, wenn die Identifizierung der betroffenen Person gesetzlich verboten ist oder wenn die Identifizierung „praktisch nicht durchführbar" ist, „z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften" erfordert, sodass „das Risiko einer Identifizierung de facto vernachlässigbar" ist. Für den Kenner der Zuordnungsregel sind die Daten immer personenbezogen.

Die Datenschutz-Grundverordnung gibt keine spezifischen Verfahren zur Pseudonymisierung vor. Sie erkennt jedoch die verwendeten Verfahren nur dann als Pseudonymisierung nach Art. 4 Nr. 5 DSGVO an, wenn sie zwei Voraussetzungen erfüllen. Sie müssen erstens die Daten so verarbeiten, dass sie „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können". Zweitens müssen die

228 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779 – Breyer.
229 S. hierzu Kap. 3.3.2.

„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".

3.4 Löschung durch Anonymisierung?

Das folgende Kapitel beantwortet die Frage 4.4. Diese lautet:

> *Kann eine wirksame Anonymisierung von Daten als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 EU-DSGVO angesehen werden? Gehen Sie bitte auch darauf ein, ob eine wirksame Anonymisierung ausreichend ist, wenn die Löschung im Rahmen einer Einwilligung vereinbart wurde.*

Art. 17 Abs. 1 DSGVO sieht in sechs Fällen ein Recht und eine Pflicht zur Löschung vor. Um die Daten weiterhin nutzen zu können, stellt sich die Frage, ob in diesen sechs Fällen eine wirksame Anonymisierung von Daten als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 DSGVO angesehen werden kann.

Für die Beantwortung der Frage ist jedoch immer zu beachten, dass eine Löschung personenbezogene Daten voraussetzt und keine Löschung erforderlich ist und eingefordert werden kann, wenn die Daten anonymisiert sind.[230]

3.4.1 Löschung nach der Datenschutz-Grundverordnung

Nach Art. 17 Abs. 1 DSGVO hat

> *„die betroffene Person ... 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.*

230 S. hierzu genauer Kap. 3.4.3.

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.“

Der Begriff des Löschens ist in der Datenschutz-Grundverordnung im Gegensatz zu § 3 Abs. 4 Nr. 5 BDSG a.F. und § 67 Abs. 6 Nr. 5 SGB X a.F. nicht definiert. Er ist in Art. 4 Nr. 2 DSGVO nur als eine Form der Datenverarbeitung erwähnt.

Aus der funktionalen Verwendung des Begriffs „Löschen“ in Art. 17 Abs. 1 DSGVO und aus dem Wortsinn ist abzuleiten, dass „Löschen“ eine Handlungsform beschreibt, die dazu dient, dass Daten nicht mehr verwendet werden können.[231] Dem entsprechend ist „Löschen“ in § 3 Abs. 4 Nr. 5 als „das Unkenntlichmachen gespeicherter personenbezogener Daten“ definiert.[232] In diesem Sinn ist „Löschen“ auch in Art. 4 Nr. 1 DSGVO zu verstehen.[233] Löschen ist nur auf einem elektronischen Datenträger möglich.[234] Das Löschen kann auf unterschiedliche Weise erfolgen. Entscheidend ist, dass es unmöglich ist, die zuvor in den zu löschenden Daten erfassten Informationen wahrzunehmen.[235] Unzureichend ist das schlichte Entfernen eines Verweises auf bestimmte Daten in einem Register oder das Überschreiben der Daten in einer Datei.[236] Notwendig ist, dass die Daten nach dem „Löschen“ nicht wiederhergestellt und in irgendeiner sinnvollen Weise verwendet werden können.[237] Das Löschen ist auf allen Datenträgern des Verantwortlichen vorzunehmen und muss auch alle Sicherungskopien erfassen.[238] Eine „Vernichtung“ der Daten ist nicht gefordert. Diese Handlungsform ist neben dem Löschen in Art. 4 Nr. 2 DSGVO eigens erwähnt. Unter Vernichten ist im Unterschied zum Löschen die physische Beseitigung der Daten zu verstehen.[239] Dies wäre etwa durch Zerstören der Datenträger möglich, wenn man sicher sein kann, dass die Daten nur auf den zerstörten Datenträgern gespeichert waren.

231 S. *Herbst*, in: Kühling/Buchner, Art. 4 Rn. 36; *Reimer*, in: Sydow, Art. 4 Rn. 75: das Datum soll „nicht mehr ausgelesen“ werden können.
232 *Dammann,* in: Simitis, § 3 Rn. 172ff.
233 *Herbst*, in: Kühling/Buchner, Art. 4 Nr. 2 Rn. 36 und Art. 17 Rn. 37; *Reimer*, in: Sydow, Art. 4 Rn. 75.
234 *Ernst*, in: Paal/Pauly, Art. 4 Rn. 34.
235 *Herbst*, in: Kühling/Buchner, Art. 4 Nr. 2 Rn. 36 und Art. 17 Rn. 37.
236 Sie hierzu das in *Dammann*, in: Simitis, § 3 Rn. 179 erwähnte Sonderproblem der Löschung eines zwei Datensätze verbindenden Elements.
237 *Herbst*, in: Kühling/Buchner, Art. 17 Rn. 38f.
238 *Herbst*, in: Kühling/Buchner, Art. 4 Nr. 2 Rn. 36 und Art. 17 Rn. 41f.
239 *Ernst*, in: Paal/Pauly, Art. 4 Rn. 34.

Genau genommen muss jede Anonymisierung auch eine Löschung enthalten, nämlich die der Identifizierungsmerkmale. Denn solange diese noch im Datensatz sind, können die Daten nicht anonym sein. Insofern ist Anonymisieren immer auch ein teilweises Löschen der personenbezogenen Daten (bis sie nicht mehr personenbezogen sind). Insofern ist zu fragen, ob die Löschpflicht bereits mit der Teillöschung durch Anonymisierung erfüllt werden kann.

Löschen soll jedoch dazu führen, dass gespeicherte personenbezogene Daten vollständig unkenntlich gemacht werden, sodass sie nicht mehr verarbeitet, ausgelesen oder wahrgenommen werden können. Dagegen verändert Anonymisieren nur die gespeicherten Daten. Dies erfolgt zwar auf eine Weise, dass die Daten nicht mehr einer betroffenen Person zugeordnet werden können. Die Daten sind aber weiterhin verarbeitbar, auslesbar und wahrnehmbar. Anonymisieren und Löschen führen somit zu unterschiedlichen Ergebnissen. Insofern kann eine Löschpflicht nicht durch Anonymisieren der Daten erfüllt werden.

Soweit der Unionsgesetzgeber für bestimmte Situationen das Löschen als Rechtsfolge vorschreibt, kann dem eine Anonymisierung der Daten nicht genügen. Dies ist auf jeden Fall anzunehmen, wenn nach Art. 17 Abs. 1 lit. e DSGVO die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, der der Verantwortliche unterliegt. Dies gilt aber auch, wenn nach lit. d die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder unrichtig sind.[240] In diesem Fall sollen die Daten vollständig beseitigt werden. Dagegen könnte für Fälle der Zweckerreichung nach lit. a, des Widerrufs einer Einwilligung nach lit. b oder der Einlegung eines Widerspruchs nach lit. c eine Anonymisierung eventuell die Interessen der jeweils betroffenen Person ebenso erfüllen. Allerdings hat der Unionsgesetzgeber auch für diese Fälle eine andere Wertung und Entscheidung getroffen.[241]

Löschen und Anonymisieren sind aber auch in diesen Fällen für die betroffenen Personen nicht gleichwertig, weil sie zu unterschiedlichen Risiken führen. Löschung heißt, dass das Risiko eines Missbrauchs der Daten vollkommen beseitigt ist. Eine faktische Anonymisierung, die nach Art. 4 Abs. 1 DSGVO für eine Aufhebung des Personenbezugs ausreichend ist,[242] bewirkt zwar, dass die Zuordnung der Daten zu einer betroffenen Person nach allgemeinem Ermessen ausgeschlossen ist, führt aber zu einem Restrisiko, das beim Löschen nicht mehr besteht.

Außerdem ist ergänzend zur Löschung in Art. 17 Abs. 2 DSGVO vorgesehen, dass ein zur Löschung verpflichteter Verantwortlicher vertretbare Schritte

240 S. Erwägungsgrund 39 DSGVO.
241 S. Erwägungsgrund 65 Satz 2 und 3 DSGVO.
242 S. Kap. 3.1.5.6 und 3.2.1.

unternehmen muss, um weitere Verantwortliche darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.[243] Diese Informationspflicht geht über die bisherige Löschpflicht hinaus.[244] Diese wird durch eine Anonymisierung nicht erfüllt und ist auch nicht deren notwendige Folge.

Als Ergebnis ist festzuhalten, dass eine wirksame Anonymisierung von Daten nicht als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 DSGVO angesehen werden kann.

3.4.2 Ausnahmen zur Löschpflicht

Nicht eine andere Form des Löschens, sondern Ausnahmen zur Löschpflicht und zum Löschanspruch[245] regelt Art. 17 Abs. 3 DSGVO. Nach lit. d gelten die Absätze 1 und 2 dieser Vorschrift nicht, soweit die Verarbeitung erforderlich ist, „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". Soweit die Ausnahme nach Abs. 3 gilt, beseitigt sie nicht nur Löschungsanspruch und Löschungspflichten, sondern auch die Rechtsgrundlagen für ein Löschen der erfassten Daten als Form der Datenverarbeitung.[246]

Die Ausnahme nach Art. 17 Abs. 3 lit. d DSGVO setzt eine bestimmte Prognose der Folgen der Datenlöschung voraus. Bezogen auf die Forschung muss diese Prognose ergeben, dass durch die Löschung der spezifischen Daten der Zweck der Forschung zumindest ernsthaft gefährdet ist. Dies ist etwa anzunehmen, wenn eine bestimmte Erkenntnis nicht gewonnen, bestimmte Untersuchungen nicht durchgeführt oder die für den Forschungszweck notwendige Vollständigkeit des Datensatzes nicht erreicht werden kann.[247]

Der Bezug auf Art. 89 Abs. 1 DSGVO ist so zu verstehen, dass die Ausnahme nur dann greift, wenn die nach dieser Vorschrift erforderlichen geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person bestehen.[248] Nach Art. 89 Abs. 1 Satz 2 DSGVO muss sichergestellt sein, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen

243 S. Erwägungsgrund 66 DSGVO.
244 S. *Roßnagel/Geminn/Jandt/Richter* 2016, 170.
245 *Herbst*, in: Kühling/Buchner, Art. 17 Rn. 70.
246 *Herbst*, in: Kühling/Buchner, Art. 17 Rn. 70.
247 *Herbst*, in: Kühling/Buchner, Art. 17 Rn. 82; *Peucker*, in: Sydow, Art. 17 Rn. 68; *Nolte/Werkmeister*, in: Gola, Art. 17 Rn. 43.
248 *Herbst*, in: Kühling/Buchner, Art. 17 Rn. 81.

Maßnahmen kann nach Satz 3 die Pseudonymisierung gehören, sofern es möglich ist, die Forschungszwecke auf diese Weise zu erfüllen.[249] Soweit dies möglich ist, sind schließlich nach Art. 89 Abs. 1 Satz 4 DSGVO im Fall einer Weiterverarbeitung der Daten diese zu anonymisieren, soweit der Forschungszweck auch mit anonymisierten Daten erreicht werden kann.[250]

Soweit diese Ausnahme des Art. 17 Abs. 3 lit. d DSGVO greift, kann zwar nicht eine Löschpflicht oder ein Löschanspruch durch Anonymisierung der Daten erfüllt werden. Es kann jedoch die Löschpflicht oder der Löschanspruch entfallen und an seine Stelle kann eine Pflicht und ein Anspruch treten, die Daten zu anonymisieren.

3.4.3 Beseitigung des Personenbezugs durch Anonymisierung

Der Anspruch auf Löschung und die Pflicht zur Löschung gelten allerdings nur für personenbezogene Daten. Zum einen setzt die Anwendung der Datenschutz-Grundverordnung insgesamt nach Art. 3 Abs. 1 DSGVO die Verarbeitung personenbezogener Daten voraus. Zum anderen bestehen im Besonderen der Löschanspruch und die Löschpflicht nur für personenbezogene Daten. Drittens beziehen sich auch die Gründe für einen Löschanspruch und eine Löschpflicht in Art. 17 Abs. 1 lit. a, d und f ausdrücklich auf personenbezogene Daten.

Weder die Datenschutz-Grundverordnung noch Art. 17 Abs. 1 DSGVO gelten für anonyme Daten. Wenn die Daten anonymisiert worden sind, bevor der Löschanspruch oder die Löschpflicht entsteht, kommt die Datenschutz-Grundverordnung nicht zur Anwendung und es kann kein Löschanspruch geltend gemacht werden. Sind die Daten personenbezogen, wenn ein Löschanspruch gerichtlich geltend gemacht wird, kann eine Anonymisierung den entstandenen Löschanspruch nicht erfüllen.

3.4.4 Vereinbarung einer Löschung durch Anonymisierung

Sind der Löschanspruch und die Löschpflicht nicht durch Art. 17 DSGVO begründet, sondern Bedingung einer Einwilligung, kommt es auf den Inhalt der Bedingung in der Einwilligungserklärung an, ob eine Anonymisierung die Löschung ersetzen kann. Wenn die betroffene Person in die Datenverarbeitung nur eingewilligt hat, weil der Verantwortliche ihr ohne weitere Spezifizierung eine Löschung in bestimmten Situationen zugesagt hat, ist davon auszugehen, dass eine Löschung im Sinne des Art. 17 Abs. 1 DSGVO gemeint ist. In diesem Fall kann aus den genannten Gründen[251] die Anonymisierung die Löschung nicht ersetzen.

249 S. z.B. *Peucker*, in: Sydow, Art. 17 Rn. 67; *Nolte/Werkmeister*, in: Gola, Art. 17 Rn. 43.
250 S. Kap. 3.2.2.
251 S. Kap. 3.4.2.

Doch auch in diesem Fall gilt: Soweit die Daten anonymisiert worden sind, bevor der Löschanspruch und die Löschpflicht entstehen, kommen weder die Regelungen in der Datenschutz-Grundverordnung zur Einwilligung noch die Einwilligung in die Verarbeitung personenbezogener Daten selbst zur Anwendung und es kann auch kein Löschanspruch aus der bedingten Einwilligung geltend gemacht werden.

Wenn jedoch im Rahmen von AGB, in deren Geltung die betroffene Person eingewilligt hat, vereinbart wurde, dass eine Löschung auch durch eine Anonymisierung ersetzt werden kann, könnte die Einwilligung zulässig und wirksam sein. Jedenfalls gibt es in der Datenschutz-Grundverordnung keine Regelung mehr wie in § 6 Abs. 1 BDSG a.F. und § 84a SGB X a.F., nach der die Rechte der betroffenen Person unabdingbar sind und daher das Recht etwa auf Löschung nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden kann. Ob eine Einwilligung in die Datenverarbeitung unter Geltung solcher AGBs wirksam ist, hängt von den Voraussetzungen des Art. 4 Nr. 11 DSGVO sowie Art. 7 DSGVO ab, insbesondere davon, dass die betroffene Person nach Art. 7 Abs. 2 DSGVO ausreichend aufgeklärt und die Einwilligung gemäß Art. 7 Abs. 4 DSGVO freiwillig erteilt worden ist.[252]

3.4.5 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Durch die Datenschutz-Grundverordnung ändern sich weder die Anforderungen an eine Löschung noch die Einschätzung des Verhältnisses von Löschung und Anonymisierung. Nach § 3 Abs. 4 Nr. 5 BDSG a.F. und § 67 Abs. 6 Nr. 5 SGB X a.F. ist Löschen „das Unkenntlichmachen gespeicherter personenbezogener Daten". Diesem Verständnis des Löschens wird eine Anonymisierung der Daten nicht gerecht.

Die Gründe für einen Löschanspruch und eine Löschpflicht in Art. 17 Abs. 1 DSGVO haben sich leicht gegenüber den Gründen in §§ 20 und 35 BDSG a.F. und § 84 SGB X verändert. Dies ändert aber nichts an der Grundaussage, dass eine Anonymisierung eine Löschung nicht ersetzen kann.

Neu sind allerdings die Ausnahmen von der Löschpflicht und dem Löschanspruch nach Art. 17 Abs. 3 DSGVO. Dies kann im Fall der medizinischen Forschung dazu führen, dass Löschpflicht und Löschanspruch entfallen und dafür im Fall der Weiterverarbeitung von Forschungsdaten eine Pflicht und ein Anspruch auf Anonymisierung der Daten an deren Stelle treten.[253]

Die Anforderungen an eine Einwilligung in Art. 4 Nr. 11 und Art. 7 DSGVO haben sich gegenüber § 4a BDSG a.F. und § 67b Abs. 2 SGB X a.F. leicht verändert.

252 S. hierzu z.B. *Ernst*, ZD 2017, 110; *Buchner/Kühling*, DuD 2017, 544.
253 S. Kap. 3.4.2.

Aber auch diese Änderungen sind für das Ergebnis irrelevant, dass bei der Vereinbarung einer Löschung, die zur Bedingung einer Einwilligung wird, eine Anonymisierung nicht ausreicht. Lediglich soweit in der bedingten Einwilligung ein gesetzlicher Anspruch auf Löschung durch einen Anspruch auf Anonymisierung ersetzt wird, greift für die Datenverarbeitung nach dem bisherigen deutschen Datenschutzrecht das Dispositionsverbot nach § 6 Abs. 1 BDSG a.F. und § 84a SGB X a.F. Dieses ist in der Datenschutz-Grundverordnung entfallen.

Für alle Erwägungen greift jedoch die Feststellung, dass eine Löschung immer personenbezogene Daten voraussetzt und keine Löschung erforderlich ist und eingefordert werden kann, wenn die Daten zuvor anonymisiert worden sind.

3.4.6 Ergebnis zur Löschung durch Anonymisierung

Eine wirksame Anonymisierung von Daten kann nicht als Umsetzung der Löschpflicht oder des Löschanspruchs nach Art. 17 Abs. 1 DSGVO angesehen werden, da beide unterschiedliche Wirkungen haben. Löschpflicht oder Löschanspruch entfallen jedoch nach Art. 17 Abs. 3 DSGVO. Im Fall der Forschung im öffentlichen Interesse besteht keine Löschpflicht und kein Löschanspruch, soweit voraussichtlich die Verwirklichung der Ziele der Datenverarbeitung unmöglich gemacht oder ernsthaft beeinträchtigt werden. Soweit die Ausnahme des Art. 17 Abs. 3 lit. d DSGVO greift, kann es sein, dass die Löschpflicht oder der Löschanspruch entfallen und an ihre Stelle eine Pflicht und ein Anspruch treten, die Daten zu anonymisieren. Weiterhin ist zu beachten, dass weder die Datenschutz-Grundverordnung noch Art. 17 Abs. 1 DSGVO für anonyme Daten gelten. Wenn die Daten anonymisiert sind, bevor der Löschanspruch oder die Löschpflicht entsteht, kommt die Datenschutz-Grundverordnung nicht zur Anwendung und es besteht weder eine Löschpflicht noch ein Löschanspruch.

3.5 Vereinbarkeit der Ergebnisse mit Art. 8 GRCh und Art. 16 AEUV

Art. 8 GRCh begründet ein Recht auf Schutz personenbezogener Daten. Die Grundrechte-Charta erlangte mit dem Inkrafttreten des Vertrags von Lissabon[254] zum 1. Dezember 2009 Rechtskraft. Sie ist damit Teil des EU-Primärrechts.[255] Nach Art. 8 Abs. 1 GRCh hat „jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten". Art. 8 Abs. 2 Satz 1 GRCh enthält eine Präzisierung des Schutzes, wonach Daten „nur nach Treu und Glauben

254 Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13.12.2007, ABl. C 306, 1.

255 S. auch KOM (2010) 573 endg., 3: „Mit dem Vertrag von Lissabon wurden die in der Charta verankerten Rechte, Freiheiten und Grundsätze anerkannt und dieser dieselbe Rechtsverbindlichkeit wie den Verträgen verliehen."

für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden" dürfen. Art. 8 Abs. 2 Satz 2 GRCh erweitert den Schutz noch um ein Auskunfts- und Berichtigungsrecht. Art. 8 Abs. 3 GRCh garantiert die Überwachung des Grundrechts durch eine unabhängige Stelle.

Art. 8 GRCh stützt sich auf das europäische Sekundärrecht zum Datenschutz, insbesondere die Datenschutz-Richtlinie von 1995.[256] Demnach ist für das Verständnis der Begriffe und die Zulässigkeit eines Eingriffs in das durch Art. 8 Abs. 1 GRCh begründete Recht auf Datenschutz auf das europäische Sekundärrecht zum Datenschutz zu verweisen.[257] Art. 8 GRCh kann als eine Zusammenfassung des geltenden europäischen Datenschutzrechts verstanden werden. Daher orientiert sich auch der Begriff der personenbezogenen Daten an Art. 2 lit. a DSRL.[258] Damit orientiert sich auch Art. 8 Abs. 1 GRCh für die Abgrenzung der personenbezogenen Daten von anonymen Daten und für die rechtliche Einordnung pseudonymer Daten an den Vorgaben der Richtlinie.

Auch Art. 16 Abs. 1 AEUV enthält ein Grundrecht auf Datenschutz. Dieses ist als Wiederholung von Art. 8 GRCh zu verstehen, sodass die Ausführungen zu Art. 8 GRCh auch für Art. 16 AEUV gelten.[259]

Da die Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO identisch mit der Definition in Art. 2 lit. a DSRL ist und die Definition pseudonymer Daten in Art. 4 Nr. 5 DSGVO aus der Rechtsprechung und wissenschaftlichen Diskussion um den Begriff der personenbezogenen Daten in Art. 2 lit. a DSRL hervorgegangen ist, besteht kein Zweifel, dass die beiden Regelungen der Datenschutz-Grundverordnung mit dem Grundrecht auf Datenschutz in Art. 8 GRCh und in Art. 16 Abs. 1 AEUV vereinbar sind. Dies gilt auch für das hier referierte Verständnis der anonymen Daten. Ebenso ist der Begriff des Löschens in Art. 4 Nr. 2 DSGVO identisch mit dem gleichen Begriff des Löschens in Art. 2 lit. b DSRL und damit zusammen mit dem hier referierten Bedeutungsgehalt mit Art. 8 GRCh und Art. 16 Abs. 1 AEUV vereinbar. Wie der Vergleich zwischen der neuen Rechtslage nach der Datenschutz-Grundverordnung und der bisherigen Rechtslage nach der Datenschutz-Richtlinie und ihren deutschen Umsetzungsgesetzen gezeigt hat,[260] sind die Unterschiede sehr gering. Daher stimmen die hier gefundenen Ergebnisse mit der Datenschutzrechtslage vor Erlass des Grundrechts auf Datenschutz in Art. 8 GRCh und in Art. 16 Abs. 1 AEUV überein, die als normativer Bezugsrahmen dem Grundrecht zugrunde liegt.

256 S. Charta-Erläuterungen, EU ABl. C 303 vom 14.12.2007, 20.
257 *Bernsdorff*, in: Meyer 2014, Art. 8 GRCh, Rn. 17; *Kingreen*, in: Callies/Ruffert, Art. 8 GRCh, Rn. 5ff.
258 *EuGH*, Urteil vom 9.11.2010, Rs. C-92/09 und C-93/09, ECLI:EU:C:2010:662, Rn. 52 – Schecke; *Jarass* 2016, Art. 8 Rn. 5; *Kingreen*, in: Callies/Ruffert, Art. 8 GRCh, Rn. 9.
259 *Sobotta*, in: Grabitz/Hilf/Nettesheim 2015, Art. 16 AEUV, Rn. 8; *Kingreen*, in: Callies/Ruffert, Art. 16 AEUV, Rn. 3.
260 S. Kap. 3.1.6, 3.2.4, 3.3.4 und 3.4.5.

4 Regelungen für wissenschaftliche Forschung

Das Kapitel widmet sich der Beantwortung der Forschungsfrage 4.2:

> *Gehen Sie bitte auf den Begriff der „wissenschaftlichen Forschungszwecke" (nach Erwägungsgrund 159 der EU-DSGVO) ein und beschreiben Sie, ob die Inhalte dieses Erwägungsgrundes zu einer anderen Interpretation des Begriffs „wissenschaftliche Forschung" führen, als dies bisher der Fall war. Insbesondere bitten wir um einen Vergleich zu der Rechtsauffassung von Hr. Schneider auf Seite 97/98 (TMF-Veröffentlichung: U.K. Schneider, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, Band 12).*

Im Rahmen wissenschaftlicher Forschung stellen sich nicht selten komplexe ethische und rechtliche Fragen. Wissenschaftliche Forschung endet nicht bereits dort, wo durch die Forschung in Grundrechte Dritter eingegriffen wird. Auch ist die Wissenschaftsfreiheit nicht unter Gesetzesvorbehalt gestellt.[261] Vielmehr ist eine Abwägung mit anderen Grundrechten und Grundwerten mit Verfassungsrang vorzunehmen. Diese privilegierte Stellung beruht auf der „Schlüsselfunktion, die einer freien Wissenschaft sowohl für die Selbstverwirklichung des Einzelnen als auch für die gesamtgesellschaftliche Entwicklung zukommt".[262]

261 *Antoni*, in: Hömig/Wolff, Art. 5 Rn. 35.
262 BVerfGE 35, 79 (113).

Wissenschaftliche Forschung beruht zwar nicht notwendigerweise, aber doch häufig auf der Verarbeitung personenbezogener Daten. Die Forschungsfreiheit aus Art. 5 Abs. 3 Satz 1 GG und das Recht auf informationelle Selbstbestimmung stehen sich dann als eigenständige Grundrechte gegenüber und können in Konflikt geraten. Auf Ebene der Europäischen Union sind es die Forschungsfreiheit aus Art. 13 Satz 1 GRCh und die Rechte aus den Art. 7 und 8 GRCh, die sich gegenüberstehen. Zudem ist das Grundrecht auf körperliche Unversehrtheit nach Art. 3 Abs. 1 GRCh zu beachten. Dieses fordert für medizinische Eingriffe nach Art. 3 Abs. 2 lit. a GRCh eine freie Einwilligung des Betroffenen nach vorheriger Aufklärung. Der Gesetzgeber hat mit seinen Vorgaben zum Datenumgang in der wissenschaftlichen Forschung ein System geschaffen, das diese Grundrechte in einen fairen Ausgleich bringen möchte.

4.1 Die Bedeutung des Datenschutzes für die wissenschaftliche Forschung

Wissenschaftliche Forschung kann an vielen Stellen mit den Grundprinzipien des Datenschutzes in Konflikt geraten. So ist es beispielsweise oft nicht möglich, den Zweck für die Verarbeitung personenbezogener Daten im Rahmen der Forschung bereits zum Zeitpunkt der Datenerhebung vollständig anzugeben.[263] Dennoch ist ein wirksamer Datenschutz auch im Bereich der wissenschaftlichen Forschung zum Schutz der Rechte der betroffenen Personen unverzichtbar.

4.1.1 Wissenschaft und Forschung in Charta und Grundgesetz

Im deutschen Verfassungsrecht gilt die „Wissenschaft" als Oberbegriff zu Forschung und akademischer Lehre.[264] Sie wird sehr weit[265] definiert als „alles, was nach Inhalt und Form als ernsthafter planmäßiger Versucht zur Ermittlung der Wahrheit anzusehen ist".[266]

Die sprachliche Trennung zwischen Forschung und Lehre unter dem Oberbegriff der Wissenschaft findet sich auch in Art. 13 GRCh;[267] der Aspekt der Lehre ist dabei im Begriff der „akademischen Freiheit" enthalten.[268] Dass die Charta

263 Erwägungsgrund 33 DSGVO.

264 S. BVerfGE 35, 79 (112); *Antoni*, in: Hömig/Wolff, Art. 5 Rn. 32; *Scholz*, in: Maunz/Dürig, Art. 5 Abs. 3 Rn. 9.

265 So lasse sich mit der Definition „kaum etwas anfangen"; *Simitis*, in: ders., § 40 Rn. 35. Andererseits kommt der Weite der Definition auch die Funktion zu, offen für Wandel und Neuerung zu sein – s. auch *Schneider* 2015, 97.

266 BVerfGE 47, 327 (367).

267 *Jarass* 2016, Art. 13 Rn. 6; *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 5.

268 *Jarass* 2016, Art. 13 Rn. 8. Nach *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 9 enthält die akademische Freiheit zudem eine Begrenzung des organisatorischen Zugriffs des Unionsgesetzgebers auf Universitäten und außeruniversitäre Forschungsstätten. Eine ähnliche Gewährleistung wird auch für Art. 5 Abs. 3 GG angenommen – s. *Scholz*, in: Maunz/Dürig, Art. 5 Abs. 3 Rn. 81.

in Art. 13 GRCh nicht von „Lehre“ spricht, dient der Abgrenzung zu Art. 14 Abs. 3 GRCh, der die Freiheit zur Gründung von Lehranstalten enthält.[269]

Art. 13 GRCh gilt als vom deutschen Grundgesetz „inspiriert“,[270] was einerseits die Parallelen zwischen Charta und Grundgesetz erklärt, andererseits ermöglicht, die Auslegung zu Art. 5 Abs. 3 GG bis zu einem gewissen Grad auch zur Auslegung von Art. 13 GRCh heranzuziehen. Der Europäische Gerichtshof hat sich bisher nur peripher zur Wissenschaftsfreiheit geäußert.[271] Dennoch kann der Wissenschaftsbegriff des Grundgesetzes nicht einfach auf Art. 13 GRCh übertragen werden.[272] So sei das Element der Wahrheitssuche[273] für die Charta durch ein „methodisch geleitetes Generieren neuen Wissens“ zu ersetzen.[274] Da aber auch Art. 5 Abs. 3 GG die angewandte Forschung miteinschließt, hat diese sprachliche Modifikation der hergebrachten deutschen Definition des Wissenschaftsbegriffs lediglich klarstellenden Charakter, indem sie eine unzulässige idealistische Einschränkung des Begriffs verhindert. Berufen kann sich auf die Wissenschaftsfreiheit nach Art. 13 GRCh „jeder wissenschaftlich Tätige“.[275]

Der Begriff der „Forschung“ wird weder im Primärrecht noch im Sekundärrecht der Union definiert, ist aber nach herrschender Meinung weit zu verstehen.[276] Eine Differenzierung zwischen Grundlagenforschung und angewandter Forschung findet nicht statt.[277]

Das Bundesverfassungsgericht versteht unter Forschung die „geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen“.[278] Eine eigene, klärende Definition findet sich weder im geltenden noch im neuen Bundesdatenschutzgesetz – weder zum Begriff der „Forschung“ noch zu dem der „Wissenschaft“.

Grundrechtliche Vorgaben zu Wissenschaft und Forschung ergeben sich auf Unionsebene insbesondere aus Art. 3 Abs. 2 lit. b GRCh.[279] Dieser fordert „im Rahmen der Medizin und der Biologie“ die Einwilligung des Betroffenen nach vorheriger Aufklärung.

269 *Bernsdorff*, in: Meyer, Art. 13 Rn. 15.
270 *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 1.
271 S. Nachweise in *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 2.
272 *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 6.
273 Dieses fußt auf der Auslegung von Art. 142 der Weimarer Reichsverfassung durch *Smend – Scholz*, in: Maunz/Dürig, Art. 5 Abs. 3 Rn. 91. *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 6 sieht bei *Smend* eine Vorprägung durch den deutschen Idealismus.
274 *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 6.
275 *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 8.
276 S. *Bernsdorff*, in: Meyer, Art. 13 Rn. 15; s. auch Erwägungsgrund 159 Satz 2 DSGVO.
277 *Bernsdorff*, in: Meyer, Art. 13 Rn. 15.
278 BVerfGE 35, 79 (112) unter Verweis auf BT-Drs. V/4335, 4; „Forschung“ i.S.v. Art. 5 Abs. 3 meint damit nur die wissenschaftliche Forschung – *Scholz*, in: Maunz/Dürig, Art. 5 Abs. 3 Rn. 85.
279 „Im Rahmen der Medizin und der Biologie muss insbesondere Folgendes beachtet werden: a) die freie Einwilligung des Betroffenen nach vorheriger Aufklärung entsprechend den gesetzlich festgelegten Einzelheiten“.

4.1.2 Rechtslage nach der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung schützt Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO als besondere Kategorie personenbezogener Daten. Art. 4 Nr. 15 DSGVO definiert Gesundheitsdaten als personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Einen Ausgleich zwischen Art. 7 und 8 GRCh einerseits und Art. 13 und 3 GRCh andererseits bewirkt die Verordnung vornehmlich durch die Regeln zur Einwilligung und durch besondere Garantien gemäß Art. 89 Abs. 1 DSGVO.

Auch für Forschungszwecke bestimmt sich die Zulässigkeit einer Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. a bis f DSGVO. An erster Stelle wird in lit. a die Einwilligung genannt. Da auch Art. 8 Abs. 2 Satz 1 GRCh die Einwilligung vor der gesetzlichen Zulässigkeit nennt, wird sie von manchen als die „vornehmste" Bedingung für die Rechtmäßigkeit der Verarbeitung aufgeführt.[280] Sie muss nach ihrer Definition in Art. 4 Nr. 11 DSGVO unter anderem freiwillig und für den bestimmten Fall, in informierter und unmissverständlicher Weise abgegeben werden. Weitgehend unproblematisch ist auch die Verarbeitung von Gesundheitsdaten, wenn sie sich nach Art. 9 Abs. 2 lit. a DSGVO auf eine wirksame Einwilligung des Betroffenen stützt. Ausnahmen durch nationales Recht sind nach Art. 9 Abs. 2 lit. j DSGVO möglich. Trotz der Vorgabe aus Art. 4 Nr. 11 DSGVO, die Einwilligung müsse „für den bestimmten Fall" abgegeben werden, sind für Zwecke der wissenschaftlichen Forschung ausnahmsweise auch breit formulierte Einwilligungen möglich. Dies stellt Erwägungsgrund 33 DSGVO klar:[281]

> *„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."*

In der Praxis bedeutet dies eine bereichsspezifische Aufweichung der datenschutzrechtlichen Vorgabe, den Zweck der Verarbeitung vorab möglichst präzise anzugeben.[282]

280 S. z.B. *Albers*, in: Wolff/Brink, Art. 6 DSGVO, Rn. 19; *Frenzel*, in: Paal/Pauly, Art. 6 Rn. 10.
281 S. auch *Johannes*, in: Roßnagel 2017, § 4 Rn. 65.
282 S. Art. 5 Abs. 1 lit. b DSGVO: „für festgelegte, eindeutige und legitime Zwecke".

Art. 89 Art. 1 Satz 1 DSGVO enthält die Feststellung, dass die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken „geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung" unterliegt. Der Norm kommt primär eine strukturierende Funktion zu; sie stellt keinen gesonderten Erlaubnistatbestand dar.[283] Indem sie Forschungsinteressen mit dem Schutz personenbezogener Daten in Ausgleich zu bringen sucht, versuche sie eine „Quadratur des Kreises".[284]

Privilegierungen der Datenverarbeitung zu Forschungszwecken finden sich an vielen Stellen der Verordnung. Nach Art. 5 Abs. 1 lit. b DSGVO etwa ist eine Weiterverarbeitung für wissenschaftliche Forschungszwecke nicht unvereinbar mit den ursprünglichen Zwecken. Das hat zur Folge, dass zur Weiterverarbeitung im Verhältnis zur Erstverarbeitung keine neue Rechtsgrundlage notwendig ist, sondern die Verarbeitung auf die Grundlage der Erstverarbeitung gestützt werden kann.[285] Diese Privilegierung der Verarbeitung von personenbezogenen Daten zu Forschungszwecken bezogen auf die Zweckbindung ist von zentraler Bedeutung. Die Bedeutung dieser Vereinbarkeitsvermutung ist allerdings umstritten.[286] Die Formulierung „nicht unvereinbar" indiziert, dass zumindest Ausnahmen von der in Art. 5 Abs. 1 lit. b DSGVO formulierten Regel denkbar sind. In bestimmten Fällen kann also dennoch eine neue Rechtsgrundlage erforderlich sein, wobei primär an besonders schwerwiegende Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person im Sinne von Art. 6 Abs. 4 lit. d DSGVO zu denken ist.[287] Letztlich sollte nicht von einer „faktische[n] Aufhebung des Zweckbindungsgrundsatzes" gesprochen werden,[288] sondern lediglich von einer Flexibilisierung.[289]

Eine weitere Privilegierung bezogen auf die Speicherdauer personenbezogener Daten im Falle einer Verarbeitung für wissenschaftliche Forschungszwecke enthält Art. 5 Abs. 1 lit. e DSGVO. Grundsätzlich dürfen personenbezogene Daten nur so lange gespeichert werden, wie dies für die Verarbeitungszwecke erforderlich ist. Danach sind sie zu löschen oder der Personenbezug ist zu entfernen. Vorbehaltlich geeigneter technischer und organisatorischer Maßnahmen ist eine Speicherung personenbezogener Daten zu wissenschaftlichen Forschungszwecken gemäß Art. 89 Abs. 1 DSGVO aber auch nach Wegfall der Erforderlichkeit erlaubt. Eine Festlegung auf einen konkreten Zeitraum ist der

283 *Hense*, in: Sydow, Art. 89 Rn. 1.
284 So *Hense*, in: Sydow, Art. 89 Rn. 2.
285 S. Erwägungsgrund 50 DSGVO: „Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten."
286 Für den Wegfall des Erfordernisses einer neuen Rechtsgrundlage: *Schulz*, in: Gola, Art. 6 Rn. 185ff.; *Frenzel*, in Paal/Pauly, Art. 5 Rn. 31; *Roßnagel*, in: Simitis/Hornung/Spiecher, Art. 6 Abs. 4 i.E.; *Kühling/Martini u.a.* 2016, 38; differenziert: *Herbst*, in: Kühling/Buchner, Art. 5 Rn. 49; *Heberlein*, in: Ehmann/Selmayr, Art. 5 Rn. 20.
287 So *Johannes/Richter*, DuD 2017, 300 (301).
288 So noch *Johannes*, in: Roßnagel 2017, § 4 Rn. 64.
289 So *Johannes/Richter*, DuD 2017, 300 (301).

Verordnung allerdings nicht zu entnehmen; sie spricht lediglich davon, dass solche Daten „länger" gespeichert werden dürfen. Damit wird auch das Prinzip der Speicherbegrenzung zugunsten wissenschaftlicher Forschungszwecke erweitert. Statt am Primärzweck muss sie sich nun am Sekundärzweck der Forschung ausrichten. Die Speicherung für den Forschungszweck darf nicht zu einer unbegrenzten Vorratsdatenhaltung führen. Der wissenschaftliche Zweck, der die Erhaltung des Personenbezugs erforderlich macht, muss wenigstens lege artis theoretisch nach der konkreten Wissenschaft absehbar sein.[290]

Nach Art. 17 Abs. 3 lit. d DSGVO steht der betroffenen Person kein Recht auf Löschung zu, wenn die Datenverarbeitung für wissenschaftliche Forschungszwecke erforderlich ist und das Recht die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.[291] Der Verantwortliche ist von seiner Informationspflicht nach Art. 14 Abs. 1 bis 4 DSGVO befreit, wenn ihre Erfüllung gemäß Art. 14 Abs. 5 lit. b DSGVO im Rahmen der Verarbeitung für wissenschaftliche Forschungszwecke einen unverhältnismäßigen Aufwand erfordern würde.

Zu beachten sind auch die weitreichenden Öffnungsklauseln der Datenschutz-Grundverordnung für die Verarbeitung von personenbezogenen Daten etwa im öffentlichen Bereich.[292]

4.1.3 Rechtslage nach dem neuen Bundesdatenschutzgesetz

Die Datenschutz-Grundverordnung enthält eine große Zahl von Öffnungsklauseln, die die nationalen Gesetzgeber nutzen können, um abweichende Regelungen zu treffen. Art. 9 Abs. 1 DSGVO verbietet, besondere Kategorien von personenbezogenen Daten zu verarbeiten. Art. 9 Abs. 2 DSGVO gibt dem nationalen Gesetzgeber vielfältige Möglichkeiten, Ausnahmen von diesem Verbot festzulegen[293] – für medizinische Forschung in Art. 9 Abs. 2 lit. j DSGVO. Eine Ausnahme von diesem Verbot befreit jedoch nach Erwägungsgrund 51 DSGVO nicht davon, „die allgemeinen Grundsätze und Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung" zu beachten. Daher gelten auch für besondere Kategorien von personenbezogenen Daten die Bedingungen für die Zulässigkeit der Datenverarbeitung, die sich aus Art. 6 Abs. 1 und 4 DSGVO[294] und Art. 89 Abs. 1 DSGVO ergeben. Allerdings fordern die Öffnungsklauseln in Art. 9 Abs. 2 DSGVO von den mitgliedstaatlichen Regelungen, die spezielleren nationalen

290 *Johannes*, in: Roßnagel 2018, § 7 Rn. 253.
291 S. Kap. 3.4.2.
292 Zu den Öffnungsklauseln s. *Johannes*, in: Roßnagel 2018, § 7 Rn. 276ff.
293 S. *Frenzel*, in: Paal/Pauly, Art. 9 Rn. 1.
294 S. z.B. *Schulz*, in: Gola, Art. 9 Rn. 5f.; *Weichert*, in: Kühling/Buchner, Art. 9 Rn. 4; a.A. *Kampert*, in: Sydow, Art. 9 Rn. 1 und 12: Art. 9 ist abschließend.

Erlaubnistatbestände gegenüber den allgemeinen Erlaubnisregeln in Art. 6 Abs. 1 DSGVO zu verengen.[295] Sie gehen daher diesen vor. Für die allgemeinen Bedingungen ergeben sich außerdem für die Forschung Öffnungsklauseln aus Art. 89 Abs. 2 und im öffentlichen Bereich aus Art. 6 Abs. 2 und 3 DSGVO.[296]

Das neue Bundesdatenschutzgesetz enthält deshalb in § 27 BDSG-neu eigene Regelungen zur Datenverarbeitung zu wissenschaftlichen Forschungszwecken. Diese sind als lex generalis im Verhältnis zum bereichsspezifischen Recht ausgestaltet.[297] Der Wortlaut von § 27 BDSG-neu ist wie folgt:

> *„(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."*

295 *Weichert*, in: Kühling/Buchner, Art. 9 Rn. 4.
296 Zur Kritik an dieser Konstruktion s. *Johannes/Richter*, DuD 2017, 300 (302).
297 BT-Drs. 18/11325, 100.

Eine Verarbeitung besonderer Kategorien personenbezogener Daten soll nach § 27 Abs. 1 Satz 1 BDSG-neu auch ohne Einwilligung zu wissenschaftlichen Forschungszwecken möglich sein, sofern die Interessen des Verantwortlichen „erheblich überwiegen" und der Verantwortliche im Sinn von § 22 Abs. 2 Satz 1 BDSG-neu „angemessene und spezifische Maßnahmen zur Wahrnehmung der Interessen der betroffenen Person" vorsieht. Zudem sind die Vorgaben aus § 27 Abs. 3[298] und 4 BDSG-neu zu beachten.

Die Rechte aus den Art. 15, 16, 18 und 21 DSGVO können nach Maßgabe von § 27 Abs. 2 Satz 1 BDSG-neu beschränkt werden. Eine Beschränkung ist dann möglich, wenn die genannten Rechte die Verwirklichung des Forschungszwecks unmöglich machen oder ernsthaft beeinträchtigen; die Beschränkung muss für die Erfüllung der Forschungszwecke notwendig sein. Ein Fallbeispiel bietet die Gesetzesbegründung: Die Verwirklichung des Forschungszwecks kann dann unmöglich sein, wenn das fragliche Forschungsprojekt andernfalls von der zuständigen Ethikkommission nicht genehmigt werden würde.[299]

§ 27 Abs. 2 Satz 2 BDSG-neu enthält eine weitere Einschränkung des Auskunftsrechts aus Art. 15 DSGVO. Dieses ist dann ganz abdingbar, wenn die Auskunftserteilung zu Forschungsdaten, die zur Erreichung des Forschungszwecks erforderlich sind, einen unverhältnismäßigen Aufwand erfordern würde.

§ 27 Abs. 3 BDSG-neu ergänzt die in § 22 Abs. 2 BDSG-neu genannten Maßnahmen, auf die § 27 Abs. 1 Satz 2 BDSG-neu verweist. So sind nach § 27 Abs. 3 Satz 1 BDSG-neu zu wissenschaftlichen Forschungszwecken verarbeitete besondere Kategorien personenbezogener Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist, sofern nicht berechtigte Interessen der betroffenen Person dem entgegenstehen.[300] § 27 Abs. 3 Satz 2 BDSG-neu enthält eine Vorgabe an die Speicherung der Merkmale, mit denen eine Zuordnung zu einer bestimmten Person möglich ist. Diese Merkmale sind getrennt zu speichern und nur bei konkretem Bedarf mit den Einzelangaben zusammenzuführen. Dies entspricht inhaltlich exakt § 40 Abs. 2 BDSG a.F.

§ 27 Abs. 4 BDSG-neu enthält die Vorgabe, dass personenbezogene Daten abseits von Ereignissen über die Zeitgeschichte nur mit Einwilligung der betroffenen Person veröffentlicht werden dürfen, was § 40 Abs. 3 BDSG a.F. entspricht. Die Regelung kann auf Art. 85 DGSVO gestützt werden.

4.1.4 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Ähnliche Privilegierungen wie in der Datenschutz-Grundverordnung finden sich schon in Art. 6 Abs. 1 lit. b, Art. 11 Abs. 2 und Art. 13 Abs. 2 DSRL. Eine

298 S. zu diesem Kap. 3.2.2.
299 BT-Drs. 18/11325, S. 99.
300 Diese Regelung ist angesichts des Wortlauts von Art. 89 Abs. 1 Satz 4 DSGVO unionsrechtswidrig – s. Kap. 3.2.2.

Art. 89 DSGVO entsprechende „Grundnorm" enthält die Datenschutzrichtlinie aber nicht.[301] Im Vergleich zur Richtlinie wird in der Verordnung aber eine Präzisierung und Eingrenzung des Begriffs der „wissenschaftlichen Zwecke" zu den „wissenschaftlichen Forschungszwecken" versucht.

Regelungen zur wissenschaftlichen Forschung finden sich im geltenden Bundesdatenschutzgesetz etwa in §§ 13 Abs. 2 Nr. 8, 14 Abs. 2 Nr. 9 und Abs. 5 Satz 1 Nr. 2, 28 Abs. 2 Nr. 3 und Abs. 6 Nr. 4 sowie 40 BDSG a.F. Diese wurden unter Nutzung von Öffnungsklauseln teilweise in das neue Bundesdatenschutzgesetz übernommen. § 27 Abs. 2 Satz 2 wie auch die Absätze 3 und 4 BDSG-neu stellen so im Vergleich zum geltenden Bundesdatenschutzgesetz grundsätzlich keine Neuerungen dar. § 27 Abs. 2 Satz 2 BDSG-neu ist vielmehr eine Übertragung von § 33 Abs. 2 Satz 1 Nr. 5 i.V.m. § 34 Abs. 7 sowie § 19a Abs. 2 Nr. 2 BDSG a.F. in das neue Bundesdatenschutzgesetz.[302] § 27 Abs. 3 und 4 BDSG-neu sind weitgehend inhalts- und wortgleich mit § 40 Abs. 2 und 3 BDSG a.F.[303] Die ausdrückliche Ausweitung auf alle Daten in § 40 Abs. 2 BDSG a.F. und die explizite Beschränkung von § 40 Abs. 3 BDSG a.F. auf wissenschaftliche Forschung betreibende Stellen wird jedoch aufgegeben.

Gegenüber §§ 13, 14 und 28 BDSG a.F. fehlt es § 27 Abs. 1 BDSG-neu an den Voraussetzungen „zur Durchführung wissenschaftlicher Forschung erforderlich" und dass „der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann". Hier wird deshalb mit einer Absenkung des bisherigen Datenschutzniveaus gerechnet.[304]

Anforderungen an die Verarbeitung von personenbezogenen Daten zu Forschungszwecken finden sich neben dem Bundesdatenschutzgesetz auch in den Landesdatenschutzgesetzen und in Spezialgesetzen wie dem Krebsregisterdatengesetz und den Landeskrankenhausgesetzen. Eine Anpassung dieser Gesetze an die Datenschutz-Grundverordnung ist bisher nicht erfolgt, vereinzelt liegen jedoch bereits Entwürfe vor.[305]

Der Wegfall des Begriffs der „Forschungseinrichtung" im Sinn von § 40 BDSG a.F. dürfte – abgesehen vom Ende der Exklusion von Einzelforschern – letztlich ohne größere Folgen bleiben. Dieser findet sich im neuen Bundesdatenschutzgesetz nicht mehr und ist auch in der Datenschutz-Grundverordnung nicht

301 *Hense*, in: Sydow, Art. 89 Rn. 3.
302 BT-Drs. 18/11325, 99.
303 BT-Drs. 18/11325, 100.
304 So *Johannes/Richter*, DuD 2017, 300 (302).
305 S. den Gesetzentwurf der Bayerischen Staatsregierung für ein Bayerisches Datenschutzgesetz vom 28.9.2017; Gesetzentwurf der Sächsischen Staatsregierung für ein Gesetz zur Anpassung landesrechtlicher Vorschriften an die Datenschutz-Grundverordnung vom 29.9.2017, LT-Drs. 6/10918; Gesetzentwurf der Fraktionen der CDU und der Fraktion Bündnis 90/DIE GRÜNEN für ein Hessisches Gesetz zur Anpassung des Landesdatenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 5.12.2017, LT-Drs. 19/5728.

enthalten.[306] In den Begriff wird insbesondere die Anforderung der Unabhängigkeit hineingelesen.[307] Diese Anforderung wird aber ohnehin als den Begriffen „Wissenschaft" und „Forschung" immanent angesehen.[308] Auch nach der Datenschutz-Grundverordnung dürfte etwa in einem Unternehmen weiter eine Trennung des Forschungsbereichs vom restlichen Unternehmen gefordert sein. Dies ergibt sich einerseits aus den Vorgaben zur Zweckbindung, andererseits aus den Vorgaben zu Maßnahmen zum Schutz personenbezogener Daten. Die Trennung im Sinn der Datenschutz-Grundverordnung bezieht sich aber auf den Datenumgang, nicht auf die Organisationsstruktur. Unter Verweis auf den Begriff der „Forschungszwecke" eine Restriktion der Privilegierung auf Forschungseinrichtungen im Sinn von § 40 BDSG a.F. anzunehmen, ist nicht zulässig. Vom deutschen Recht kann nicht auf die Auslegung unionsrechtlicher Rechtsbegriffe geschlossen werden.

4.1.5 Vereinbarkeit von § 27 BDSG-neu mit Art. 8 GRCh, Art. 16 AEUV und der Datenschutz-Grundverordnung

Fraglich ist, ob die Regelungen in § 27 BDSG-neu mit den Vorgaben der Art. 8 GRCh und Art. 16 AEUV sowie der Datenschutz-Grundverordnung vereinbar sind.

Art. 8 Abs. 1 GRCh enthält lediglich ein abstraktes Recht auf Schutz personenbezogener Daten. Art. 8 Abs. 2 Satz 1 GRCh enthält die Prinzipien der Zweckbindung und der Rechtmäßigkeit der Verarbeitung. Art. 8 Abs. 2 Satz 2 GRCh garantiert die Rechte auf Auskunft und auf Berichtigung. § 27 BDSG-neu ist mit Art. 8 Abs. 1 und Abs. 2 Satz 1 GRCh vereinbar. § 27 BDSG-neu etabliert eine gesetzlich geregelte Grundlage zur Verarbeitung personenbezogener Daten wie in Art. 8 Abs. 2 Satz 1 GRCh gefordert. Fraglich ist allenfalls ein Verstoß gegen die von Art. 8 Abs. 2 Satz 1 GRCh geforderte Beschränkung auf festgelegte Zwecke. § 27 Abs. 1 BDSG-neu ist restriktiv formuliert und greift nur bei einem erheblichen[309] Überwiegen der Interessen des Verantwortlichen gegenüber denen der betroffenen Person. Zudem errichten § 22 Abs. 2 Satz 2 und § 27 Abs. 3 und 4 BDSG-neu (wenige) zusätzliche Hürden. Ein Verstoß gegen die Beschränkung auf festgelegte Zwecke besteht somit nicht.

306 Zudem enthält auch das geltende Bundesdatenschutzgesetz neben § 40 BDSG a.F. eine Reihe von Privilegierungen für die wissenschaftliche Forschung, die keine Einschränkung auf Forschungseinrichtungen vornehmen wie etwa § 4a Abs. 2 BDSG a.F.

307 S. *Gola/Schomerus*, § 40 Rn. 7; *Simitis*, in: ders., § 40 Rn. 29: Die Institution muss „ihrer Aufgabe und Struktur nach der wissenschaftlichen Forschung gewidmet sein".

308 *Gola/Schomerus*, § 40 Rn. 7ff.; s. auch *Hornung/Hofmann*, ZD-Beilage 4/2017, 1 (5): „Ein solches Unabhängigkeitserfordernis wird man auch für den Begriff der wissenschaftlichen Forschung nach der Datenschutz-Grundverordnung verlangen müssen." S. auch *Schneider* 2015, 97.

309 Diese Vorgabe wurde etwa vom Wirtschaftsausschuss des Bundesrats als unnötig kritisiert. Ein überwiegendes Interesse, verbunden mit dem Verweis auf § 22 Abs. 2 Satz 2 BDSG-neu sei ausreichend; BR-Drs. 110/1/17 (neu), 34. Die Vorgabe war aber indes etwa bereits in § 13 Abs. 2 Nr. 8 BDSG a.F. enthalten.

Da § 27 Abs. 2 BDSG-neu Beschränkungen der Betroffenenrechte der Grundverordnung enthält, insbesondere zum Recht aus Auskunft, kollidiert er mit Art. 8 Abs. 2 Satz 2 GRCh. Das Recht aus Art. 8 GRCh ist jedoch nicht vorbehaltlos gewährleistet; Einschränkungen sind möglich. Diese müssen nach Art. 52 Abs. 1 Satz 1 GRCh gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Diese Voraussetzungen erfüllen sowohl Art. 89 Abs. 2 DSGVO als auch § 27 Abs. 2 BDGS.

An der Vereinbarkeit von § 27 BDSG-neu mit Art. 16 Abs. 1 AEUV[310] bestehen keine Zweifel. Art. 16 Abs. 1 AEUV enthält ein gegenüber Art. 8 Abs. 1 GRCh wortgleiches Recht auf Schutz personenbezogener Daten.[311] Auch mit Blick auf Art. 16 Abs. 2 Satz 2 AEUV bestehen keine Bedenken an der Vereinbarkeit.

Zur Vereinbarkeit von § 27 Abs. 1 BDSG-neu mit der Datenschutz-Grundverordnung ist Folgendes festzuhalten: § 27 Abs. 1 BDSG-neu ist als Ausnahmetatbestand zum Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aus Art. 9 Abs. 1 DSGVO ausgestaltet und gilt deshalb ausschließlich für die Verarbeitung von besonderen Kategorien personenbezogener Daten. Die Vorschrift stützt sich laut Gesetzesbegründung auf Art. 9 Abs. 2 lit. j DSGVO.[312] Dieser fordert, den Wesensgehalt des Rechts auf Datenschutz aus Art. 8 GRCh zu wahren sowie angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte vorzusehen. Der Gesetzgeber will dieser Vorgabe durch den Verweis auf § 22 Abs. 2 Satz 2 BDSG-neu Rechnung tragen.[313] Dabei wird jedoch kritisiert, dass die in § 22 Abs. 2 Satz 2 BDSG-neu geforderten Maßnahmen „weitgehend ohnehin" von der Grundverordnung gefordert werden und der deutsche Gesetzgeber durch Verweis auf einen unverbindlichen Beispielkatalog von Maßnahmen die besonderen Garantien, die Art. 89 Abs. 1 Satz 2 DSGVO fordert, nicht ausreichend erfüllt.[314]

§ 27 Abs. 2 BDSG-neu ist nicht auf besondere Kategorien personenbezogener Daten beschränkt, sondern gilt für alle Datenkategorien. Nach § 27 Abs. 2 Satz 1 BDSG-neu ist eine Einschränkung der Rechte aus Art. 15, 16, 18 und 21 DSGVO möglich, sofern absehbar ist, dass diese die Verwirklichung der Forschungszwecke „unmöglich machen oder ernsthaft beeinträchtigen". Zudem muss die Beschränkung für die Erfüllung der Forschungszwecke „notwendig" sein. Damit hält sich der deutsche Gesetzgeber eng an den Wortlaut des Art. 89 Abs. 2 DSGVO und übernimmt diesen mit nur kleinen Anpassungen.[315]

310 „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten."
311 S. Kap. 3.5.
312 BT-Drs. 18/11325, S. 99.
313 BT-Drs. 18/11325, 99.
314 *Johannes/Richter*, DuD 2017, 300 (302f.).
315 Dies wohl, um die Einhaltung der strengen (s. *Kühling/Martini u.a.* 2016, S. 298) Anforderungen des Art. 89 Abs. 2 DSGVO zu garantieren.

Nach § 27 Abs. 2 Satz 2 BDSG-neu besteht das Auskunftsrecht aus Art. 15 DSGVO zudem nicht, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Die vom Auskunftsrecht ausgenommenen Daten müssen zudem für die Zwecke der wissenschaftlichen Forschung erforderlich sein. Der Gesetzgeber versucht mit dieser Regelung, §§ 33 Abs. 2 Satz 1 Nr. 5 i.V.m. 34 Abs. 7 sowie § 19a Abs. 2 Nr. 2 BDSG a.F. in das neue Bundesdatenschutzgesetz herüber zu retten. Er beruft sich dabei auf Art. 23 Abs. 1 lit. i DSGVO.[316]

§ 27 Abs. 3 und 4 BDSG-neu sind eine Übertragung von § 40 Abs. 2 und 3 BDSG a.F. in das neue Bundesdatenschutzgesetz.[317] § 27 Abs. 3 BDSG-neu ist insoweit unionsrechtswidrig als er die Anforderung der Anonymisierung auf besondere Kategorien personenbezogener Daten beschränkt, statt sie wie Art. 89 Abs. 1 Satz 4 DSGVO auf alle Forschungsdaten zu erstrecken.[318]

4.2 Begriff der „wissenschaftlichen Forschungszwecke"

Die Datenverarbeitung für „wissenschaftliche Forschungszwecke" erfährt in der Datenschutz-Grundverordnung neben den Zwecken der Archivierung im öffentlichen Interesse und den Zwecken der Statistik eine besondere Behandlung, die ihr datenschutzrechtlich einen größeren Handlungsspielraum einräumt. Eine Definition, was unter „wissenschaftlichen Forschungszwecken" zu verstehen ist, fehlt jedoch in der Datenschutz-Grundverordnung. Der Begriff der „Forschungseinrichtung", wie ihn § 40 BDSG a.F. kennt, kommt in der Grundverordnung nicht vor.[319] Eine bestimmte Eigenschaft des Verarbeiters ist damit durch die Grundverordnung nicht gefordert; für eine Inanspruchnahme der Sonderregelungen reicht es aus, dass Daten für wissenschaftliche Forschungszwecke verarbeitet werden.[320] Dem Zweck der Verarbeitung kommt damit eine noch zentralere Rolle zu als bisher.

4.2.1 „Wissenschaftliche Forschungszwecke" in der Datenschutz-Grundverordnung

Anhaltspunkte für die Auslegung des Begriffs „wissenschaftliche Forschungszwecke" gibt Erwägungsgrund 159 DSGVO:

> *„Diese Verordnung sollte auch für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken gelten. Die Verarbeitung personenbezogener*

316 BT-Drs. 18/11325, 99; a.A. *Johannes/Richter*, DuD 2017, 300 (303): § 27 Abs. 2 Satz 2 BDSG-neu genüge den Anforderungen von Art. 23 Abs. 2 DSGVO nicht, könne aber auf Art. 89 Abs. 2 DSGVO gestützt werden.

317 BT-Drs. 18/11325, S. 100.

318 S. Kap. 3.2.2.

319 Damit unterfallen anders als nach § 40 BDSG a.F. – s. *Gola/Schomerus*, § 40 Rn. 7 – auch „Einzelforscher" den entsprechenden Regelungen und Privilegierungen der Datenschutz-Grundverordnung.

320 Kritisch zu diesem Ansatz *Simitis*, in: ders., § 40 Rn. 35.

Daten zu wissenschaftlichen Forschungszwecken im Sinne dieser Verordnung sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Darüber hinaus sollte sie dem in Artikel 179 Absatz 1 AEUV festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen. Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Um den Besonderheiten der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken zu genügen, sollten spezifische Bedingungen insbesondere hinsichtlich der Veröffentlichung oder sonstigen Offenlegung personenbezogener Daten im Kontext wissenschaftlicher Zwecke gelten. Geben die Ergebnisse wissenschaftlicher Forschung insbesondere im Gesundheitsbereich Anlass zu weiteren Maßnahmen im Interesse der betroffenen Person, sollten die allgemeinen Vorschriften dieser Verordnung für diese Maßnahmen gelten.“

4.2.1.1 Merkmale des Begriffs

Der Begriff ist im Einklang mit dem sonstigen europäischen und auch dem deutschen Recht weit auszulegen, womit dem weiten Schutzumfang von Art. 13 GRCh Rechnung getragen wird.[321] Dieser Feststellung in Erwägungsgrund 159 Satz 2 DSGVO folgt ein Beispielkatalog, demzufolge die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken die Verarbeitung für die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließt. Auch im begrifflichen Ansatz des Art. 179 AUEV, auf den Erwägungsgrund 159 DSGVO verweist, ist unerheblich, ob ökonomisch verwertbares Wissen generiert wird oder nicht.[322]

Dennoch bedingt wissenschaftliche Betätigung „wesensgemäß“ sowohl im deutschen[323] wie auch im europäischen[324] Verständnis Unabhängigkeit und Selbstständigkeit. Nach Schneider zeichnet sich wissenschaftliche Forschung durch die „Freiheit von sachfremden Erwägungen“ aus. „Hierunter ist die Unabhängigkeit der Forschung in inhaltlicher Hinsicht zu verstehen.“[325] Eine „scheinwissenschaftliche Begründung vorgegebener Ergebnisse“ ist wie schon im geltenden Datenschutzrecht[326] nicht erfasst. Die Vorgabe des Forschungs-

321 *Buchner/Tinnefeld*, in: Kühling/Buchner, Art. 89 Rn. 13.
322 *Ruffert*, in: Calliess/Ruffert, Art. 179 AEUV, Rn. 1; s. zu Art. 179 AEUV auch *Hornung/Hofmann*, ZD-Beilage 4/2017, 1 (4).
323 *Scholz*, in: Maunz/Dürig, Art. 5 Abs. 3 Rn. 99.
324 *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 7: „[W]issenschaftlicher Fortschritt mit seinem Nutzen für das Gemeinwesen kann nur von freier Wissenschaft erwartet werden“.
325 *Schneider* 2015, 97.
326 *Schneider* 2015, 98.

gegenstands durch einen Auftraggeber ist jedoch unschädlich. Damit sind etwa auch Auftragsforschung, Industrieforschung und gutachterliche Forschung erfasst.[327] Die Reichweite der wissenschaftlichen Forschungszwecke erstreckt sich auch auf vorbereitende und unterstützende Aktivitäten.[328] Zudem sind nach Erwägungsgrund 159 Satz 4 DSGVO auch Studien umfasst, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Damit sind auch Forschungsvorhaben der Krankenkassen und Kassenärztlichen Vereinigungen erfasst, die § 287 SGB V datenschutzrechtlich regelt.[329] Ferner ist zwischen Forschung, die aufgrund von Primärerhebungen, und Forschung, die aufgrund von Sekundärerhebungen durchgeführt wird, zu unterscheiden.[330] Bei letzterer sind die Regeln zur Zweckänderung zu beachten. Nicht dem Begriff der wissenschaftlichen Forschung unterfällt zudem die reine Anwendung bereits gewonnener Erkenntnisse.[331] Werden wissenschaftliche Standards lediglich zu Aufsichts- und Kontrollzwecken verwendet, fällt dies ebenfalls nicht unter den Forschungsbegriff der Verordnung, auch wenn sie nach wissenschaftlichen Methoden durchgeführt werden.[332]

Sachliche Überschneidungen gibt es zwischen „Forschungszwecken" und „statistischen Zwecken".[333] Die Grundverordnung fordert hier aber eine Abgrenzung, denn sie geht „offensichtlich davon aus, dass Forschungszwecke und statistische Zwecke zwei unterschiedliche Dinge sind".[334] Nicht als Forschungszwecke können statistische Verarbeitungen gelten, die „zwar neue, aber keine neuartigen Erkenntnisse liefern".[335] Die kommerzielle Marktforschung ist damit aber nicht per se ausgeschlossen; vielmehr kommt es auf eine Abwägung im Einzelfall an.[336]

4.2.1.2 Veröffentlichungsabsicht

Nicht enthalten ist im Begriff der „wissenschaftlichen Forschungszwecke" eine Pflicht oder Absicht zur Veröffentlichung der erzielten Forschungsergebnisse, wie von Schneider gefordert.[337] Eine derartige Pflicht kann schon vor dem Hintergrund eines möglichen Scheiterns ergebnisoffener Forschung

327 So auch *Schneider* 2015, 98.
328 *Jarass* 2016, Art. 13 Rn. 7; *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 8.
329 S. z.B. *Hornung*, in: Hänlein/Schuler, § 287 Rn. 2ff.
330 So *Raum*, in: Ehmann/Selmayr, Art. 89 Rn. 18.
331 *Johannes*, in: Roßnagel 2018, § 7 Rn. 247.
332 *Johannes*, in: Roßnagel 2018, § 7 Rn. 247.
333 *Johannes/Richter*, DuD 2017, 300 (301).
334 *Johannes/Richter*, DuD 2017, 300 (301).
335 *Johannes/Richter*, DuD 2017, 300 (301).
336 *Grages*, in: Plath, Art. 89 DSGVO, Rn. 6; a.A. *Hornung/Hofmann*, ZD-Beilage 4/2017, 1 (14), die Markt- und Meinungsforschung grundsätzlich als vom Begriff der „wissenschaftlichen Forschung" erfasst ansehen.
337 *Schneider* 2015, 98. Die Veröffentlichung von Forschungsergebnissen zählt aber etwa zu den Dienstpflichten eines Universitätsprofessors – s. BVerfGE 47, 327 (375f.).

nicht gefordert werden.[338] Zu Art. 5 Abs. 3 GG ist zudem anerkannt, dass Wissenschaftler „selbst den Zeitpunkt bestimmen können, wann sie ein bestimmtes Forschungsergebnis oder eine bestimmte Lehrmeinung veröffentlichen".[339] Dies dürfte auch für Art. 13 GRCh gelten. Dieser zählt zwar die Publikation von Forschungsergebnissen zu seinem Schutzbereich, dies verdichtet sich jedoch nicht zu einer Veröffentlichungspflicht. Geschützt ist der individuelle Erkenntnisgewinn des Wissenschaftlers. Dieser muss nicht notwendigerweise geteilt werden. Dennoch sind der Austausch und die Veröffentlichung von Forschungsergebnissen vor dem Hintergrund der gesellschaftlichen Komponente der Wissenschaftsfreiheit unerlässlich. Daraus ergibt sich ein Spannungsfeld, das dem zwischen der Notwendigkeit gelebter Demokratie einerseits und dem Fehlen einer Wahlpflicht sowie einer Pflicht zur Teilnahme am demokratischen Diskurs[340] andererseits gleicht. Auch eine von Beginn an bestehende Veröffentlichungsabsicht ist deshalb nicht erforderlich.[341] Die Veröffentlichungsabsicht kann jedoch eine Rolle bei der Abwägung zwischen den Interessen des Verarbeiters personenbezogener Daten und denen der betroffenen Person spielen.[342] Sie kann nämlich positiv zugunsten des Verarbeiters in Form eines Indizes für die Wissenschaftlichkeit des Verarbeitungszwecks wirken, aber auch negativ, wenn die Veröffentlichung personenbezogene Daten enthalten soll. Dies spielt freilich nur dann eine Rolle, wenn die Veröffentlichung tatsächlich zu Forschungszwecken verarbeitete personenbezogene Daten enthalten soll.

Die Forderung einer Veröffentlichungspflicht oder zumindest einer Veröffentlichungsabsicht ist auch aus datenschutzrechtlicher Sicht wenig praktikabel. Käme es zu keiner Veröffentlichung der durch die Verarbeitung personenbezogener Daten erzielten Forschungsergebnisse, so lägen die Voraussetzungen für die Sonderbehandlung der Datenverarbeitung rückwirkend betrachtet nicht vor. Da aber eine Freiheit bezüglich des Veröffentlichungszeitraums besteht, ergäbe sich die Frage, ab wann davon auszugehen ist, dass die Sonderbehandlung unzulässiger Weise in Anspruch genommen wurde, mithin ab wann Sanktionen verhängt werden können. Zudem würde durch die Forderung etwa ein großer Teil der Forschung im Bereich der Landesverteidigung

338 So letztlich auch *Schneider* 2015, 98: „Ist die Aussagekraft, also das Evidenzniveau, sehr gering, wird man keine Veröffentlichung fordern können. Umgekehrt wird man aber auch keine höchste Evidenz für eine Veröffentlichungspflicht fordern können, denn auch die Wissenschaft ist in der Regel ein iterativer, arbeitsteiliger Prozess."

339 BVerfGE 47, 327 (383). *Schneider* 2015, 98: „Auch einem eventuellen Sponsor der Forschung wird man einen gewissen Spielraum zugestehen können, gerade wenn dies für die vorherige Erlangung von Patentschutz für eine Erfindung notwendig ist."

340 S. *Geminn*, VerwArch 2016, 601 (609, 613).

341 So aber *Schneider* 2015, 98: „Sollen die Ergebnisse der Forschung, unabhängig von ihrer wissenschaftlichen Qualität, ggf. aber unabhängig von ihrem Inhalt, langfristig geheim gehalten werden, so fällt die entsprechende Tätigkeit … nicht in den Schutzbereich der Wissenschaft."

342 So auch *Weichert* 2014, https://www.datenschutzzentrum.de/vortraege/20120328-weichert-medizinische-forschung.html.

von einer Sonderbehandlung ausgeschlossen. Dieser Bereich unterliegt allerdings ohnehin Öffnungsklauseln der Datenschutz-Grundverordnung. Aber auch die kommerzielle Forschung wird oftmals an einer Geheimhaltung von Forschungsergebnissen interessiert sein.

4.2.2 „Wissenschaftliche Forschungszwecke" vs. „wissenschaftliche Zwecke"

Abzugrenzen sind „wissenschaftliche Forschungszwecke" vom Begriff der „wissenschaftlichen Zwecke", wie ihn die Datenschutzrichtlinie verwendet. Der Begriffswechsel wurde bewusst und auf Drängen des Europäischen Parlaments vorgenommen, um eine Einschränkung auf „Forschungszwecke im engeren Sinne" vorzunehmen.[343]

Der Begriff der Richtlinie galt „in Zeiten von Big Data und Data Mining" als zu weit.[344] Daher soll der in der Datenschutz-Grundverordnung der engere Begriff der Forschungszwecke verwendet werden. Allerdings wird auch angezweifelt, ob angesichts des weiten Verständnisses der wissenschaftlichen Forschungszwecke die mit dem Begriffswechsel verbundene „Restriktionserwartung" tatsächlich erfüllt wird.[345] Ein „weiter" Forschungszweck „im engeren Sinne" scheint ein nicht auflösbarer Widerspruch zu sein. Vereinzelt wird die Formulierung gar mit Blick auf den übergeordneten Begriff von „Wissenschaft" im Vergleich zu „Forschung" für „sinnlos" gehalten.[346]

Die Datenschutz-Grundverordnung verwendet in Art. 5 Abs. 1 lit. b und e, in Art. 17 Abs. 3 lit. c, Art. 9 Abs. 2 lit. j, Art. 14 Abs. 5 lit. b, Art. 21 Abs. 6 und Art. 89 Abs. 2 DSGVO den Begriff der wissenschaftlichen Forschungszwecke, verwendet in Art. 85 und Erwägungsgrund 156 DSGVO dagegen die aus der Datenschutzrichtlinie bekannte[347] Formulierung „wissenschaftliche Zwecke".[348] Ebenfalls aus der Datenschutzrichtlinie bekannt ist die Verwendung von „Zwecke der wissenschaftlichen Forschung" in Art. 11 Abs. 2 und 13 Abs. 2 DSRL. Diese findet sich in der Verordnung lediglich in Erwägungsgrund 33 DSGVO.

Diese inkonsequente Begriffsnutzung der Grundverordnung bezogen auf die Verarbeitung personenbezogener Daten im wissenschaftlichen Kontext erschwert eine Festlegung über die von Erwägungsgrund 159 DSGVO genannten Beispiele. Vornehmlich verwendet die Verordnung die Begriffspaarung „wis-

343 *Albrecht/Jotzo*, Teil 3 Rn. 71.
344 *Albrecht/Jotzo*, Teil 3 Rn. 71. So auch *Simitis*, in: ders., § 40 Rn. 35: Weite Definitionen „bieten sich daher als ein ebenso bequemes wie wirksames Umgehungsmittel des Datenschutzes förmlich an"; es sei deshalb eine restriktive Interpretation erforderlich.
345 So *Hense*, in: Sydow, Art. 89 Rn. 15.
346 So *Pötters*, in: Gola, Art. 89 Rn. 13.
347 Art. 6 Abs. 1 UAbs. 1 lit. b und e DSRL. In der englischen Sprachfassung: „scientific purposes" (lit. b) und „scientific use" (lit. e).
348 Dies erscheint wenig einleuchtend – so *Pötters*, in: Gola, Art. 89 Rn. 13.

senschaftliche oder historische Forschungszwecke".[349] Zugleich macht sie durch die getrennte Adressierung von „wissenschaftlichen Forschungszwecken" in Erwägungsgrund 159 DSGVO und „historischen Forschungszwecken" in Erwägungsgrund 160 DSGVO deutlich, dass eine getrennte Behandlung der Begriffe erforderlich ist. Allein verwendet wird das Begriffspaar „wissenschaftliche Forschungszwecke" neben Erwägungsgrund 159 DSGVO auch in den Erwägungsgründen 157 und 162 DSGVO. Der Begriff der „Forschungszwecke" taucht auch ohne Adjektiv auf, namentlich in Erwägungsgrund 26 DSGVO. Es ist davon auszugehen, dass es sich bei letzterem lediglich um eine sprachliche Verkürzung handelt.

Fraglich ist nun zunächst, ob der von der dominierenden Sprachwahl („wissenschaftliche Forschungszwecke" und „wissenschaftliche und historische Forschungszwecke") abweichenden Formulierung in Art. 85 Abs. 2 DSGVO[350] und Erwägungsgrund 156 Satz 7 DSGVO („wissenschaftliche Zwecke") tatsächlich eine Bedeutung zukommt. Wo die deutsche Fassung von „Verarbeitung, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt" spricht, ist die englische Sprachfassung nuancierter und spricht von „processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression". Das im Begriff „expression" enthaltene Element der Meinungsäußerung fehlt in der deutschen Übersetzung, ist aber in anderen Sprachfassungen enthalten.[351] Damit klärt sich auch das „verwirrende"[352] Verhältnis zwischen Art. 85 Abs. 1 und Art. 89 Abs. 2 DSGVO. Des Weiteren erklärt sich so die Weite[353] der Öffnungsklausel des Art. 85 Abs. 2 DSGVO. Sie ist nur vor dem Hintergrund ihrer Einengung im Wissenschaftskontext auf „academic expression" und der Bedeutung der freien Meinungsäußerung in einer demokratischen Gesellschaft verständlich. Die deutsche Übersetzung ist an dieser Stelle schlicht missglückt. Die abweichende Wortwahl in Art. 85 Abs. 2 DSGVO ist damit kein redaktioneller Fehler, sondern ihr kommt eine einengende Wirkung der Öffnungsklausel zu.

Für Erwägungsgrund 156 Satz 7 DSGVO gibt es keine derartigen Abweichungen zwischen den verschiedenen Sprachfassungen der Grundverordnung. Warum Erwägungsgrund 156 DSGVO in den Sätzen 1 bis 6 von „wissenschaftlichen und

349 S. Erwägungsgründe 50, 52, 53, 62, 65, 113 und 156 DSGVO.

350 Dieser ist im Gegensatz zu Art. 89 Abs. 2 DSGVO als Regelungsauftrag, nicht als Regelungsoption ausgestaltet; *Pötters*, in: Gola, Art. 85 Rn. 14; *Kühling/Martini u.a.* 2016, 292f.

351 Z.B. in der französischen, die von „fins d'expression universitaire, artistique ou littéraire" spricht oder in der italienischen: „espressione accademica, artistica o letteraria".

352 *Pötters*, in: Gola, Art. 85 Rn. 13.

353 Auch im Vergleich zu Art. 9 DSRL. Abweichungen und Ausnahmen von weiten Teilen der Vorgaben der Grundverordnung sind durch die Mitgliedstaaten vorzusehen (Regelungsauftrag), „wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen". S. auch *Kühling/Martini u.a.* 2016, S. 292. Relativierend wirkt lediglich Erwägungsgrund 153 DSGVO, der von einer Verarbeitung zu „ausschließlich" wissenschaftlichen Zwecken spricht; s. *Buchner/Tinnefeld*, in: Kühling/Buchner, Art. 85 Rn. 14.

historischen Forschungszwecken" spricht, in Satz 7 dann aber von „wissenschaftlichen Zwecken" verwundert zunächst mit Blick auf den ursprünglichen Kommissionsentwurf[354] zur Grundverordnung wo im dortigen Äquivalent zu Erwägungsgrund 156 Satz 7 DSGVO von „Zwecken der wissenschaftlichen Forschung" gesprochen wird.[355] Im Parlamentsentwurf[356] existiert keine entsprechende Vorschrift; der Ratsentwurf[357] spricht schließlich von „wissenschaftlichen Zwecken".[358] Es ist daher davon auszugehen, dass der sprachlichen Abweichung in diesem Fall keine inhaltliche Bedeutung zukommt.

4.3 Ergebnis zur Regelung wissenschaftlicher Forschungszwecke

Für den Sprachwechsel von „wissenschaftlichen Zwecken" in der Datenschutzrichtlinie hin zu „wissenschaftlichen Forschungszwecken" in der Datenschutz-Grundverordnung wird in der Literatur durchgehend die oben angeführte Erklärung, eine Einschränkung auf „Forschungszwecke im engeren Sinne" vornehmen zu wollen,[359] akzeptiert. Es ist naheliegend, deshalb tatsächlich zunächst von einer im Vergleich zur Datenschutzrichtlinie unterschiedlichen inhaltlichen Reichweite der verwendeten Begriffe auszugehen. Die „wissenschaftlichen Forschungszwecke" sind zwar weit auszulegen, mit Blick auf den Forschungsbegriff der Grundrechtecharta ist aber die bloße Anwendung bereits gewonnener Kenntnisse nicht erfasst.[360] Die angewandte Forschung ist jedoch erfasst. Abzustellen ist auf den Primärzweck der jeweiligen Untersuchung im Einzelfall. Ist die wissenschaftliche Zielsetzung lediglich eine Ergänzung zu anderen Zielsetzungen, so fällt die Untersuchung nicht unter den Begriff der wissenschaftlichen Forschung, auch wenn wissenschaftliche Standards eingehalten werden.[361]

Letztlich ändert sich der rechtliche Status quo durch die sprachliche Veränderung nicht; die genannten Merkmale wurden auch bereits in den Begriff „wissenschaftliche Zwecke" hineingelesen. Vor dem Hintergrund der zunehmenden Verfügbarkeit von Big Data-Analysen, ist die mit der Datenschutz-Grundverordnung vorgenommene Präzisierung dennoch grundsätzlich zu begrüßen. Ob sie tatsächlich tauglicher ist, einer nicht-intendierten Ausweitung des Wissenschaftsbegriffs die Grundlage zu entziehen und eine ungewollte Sonderbehandlung von Big Data zu verhindern, als die Vorgängerformulierung der Datenschutzrichtlinie, bleibt aber fragwürdig. So hält etwa Simitis auch

354 KOM(2012) 11 endgültig.
355 S. Erwägungsgrund 125 DSGVO-E-KOM.
356 Beschluss des Europäischen Parlaments vom 12. März 2014, 7427/1/14, REV 1.
357 Rat der Europäischen Union, 9565/15.
358 Erwägungsgrund 125 DSGVO-E-Rat.
359 *Albrecht/Jotzo*, Teil 3 Rn. 71.
360 *Jarass* 2016, Art. 13 Rn. 6; *Johannes*, in: Roßnagel 2018, § 4 Rn. 247.
361 *Johannes*, in: Roßnagel 2018, § 4 Rn. 247.

den Begriff der „wissenschaftlichen Forschung“ für unpräzise.[362] Aus einer streng dogmatischen und verfassungsrechtlichen Sicht, ist Forschung ohnehin der Teil der Wissenschaft, der nicht Lehre und akademische Freiheit ist.[363] Die „wissenschaftliche Forschung“ wäre damit eine Tautologie und die Begrenzung auf „wissenschaftliche Forschungszwecke“ würde letztlich lediglich „wissenschaftliche Lehrzwecke“ ausschließen.[364] Dies ist jedoch erkennbar nicht die Zielsetzung der Anpassung der Formulierung beim Wechsel von der Datenschutzrichtlinie zur Datenschutz-Grundverordnung.

Immerhin leistet die Formulierung „wissenschaftliche Forschungszwecke“ eine deklaratorische Klarstellung, dass nicht die bloße Anwendung wissenschaftlicher Methoden eine Sonderbehandlung rechtfertigen kann; Forschung muss Primärziel der Verarbeitung personenbezogener Daten sein. Dies war indes aber bereits für die Vorgängerformulierung anerkannt.

Die von Schneider formulierten Kriterien behalten im Wesentlichen auch mit der Datenschutz-Grundverordnung ihre Gültigkeit. Eine Pflicht oder Absicht zur Veröffentlichung ist jedoch nicht zu fordern.

362 *Simitis*, in: ders. 2014, § 40 Rn. 35; a.A. *Schneider* 2015, 97, der in dem Prädikat „wissenschaftlich“ eine Präzisierung des Forschungsbegriffs sieht. Diese Ansicht kann mit Blick auf das Verhältnis der Begriffe „Wissenschaft“ und „Forschung“ zueinander nicht überzeugen.

363 S. *Ruffert*, in: Calliess/Ruffert, Art. 13 GRCh, Rn. 5.

364 S. *Johannes*, in: Roßnagel 2017, § 4 Rn. 59.

5 Ausschluss der Auskunftserteilung zum Wohl der betroffenen Person

Das folgende Kapitel beantwortet die Forschungsfrage 4.5:

> *Der Bundesrat hat in seinem Beschluss zum DSAnpUG-EU (Vgl. Ziff. 27 Lit. d), BR-Drucksache 110/17 v. 10.03.2017) für die Behandlung im weiteren Gesetzgebungsverfahren die Frage aufgeworfen, inwieweit ein Ausschluss der Auskunftserteilung neben den in § 27 BDSG-E genannten Voraussetzungen nach objektiven Kriterien auch aus therapeutischen sowie ethischen Erwägungsgründen zum Wohl der betroffenen Person möglich sein sollte. Prüfen Sie bitte auf welcher verfassungs- und europarechtlichen Grundlage solche Ausnahmen von den Auskunftsrechten für wissenschaftliche Forschungsvorhaben vorgenommen werden können.*

Dem Recht auf Auskunft kommt eine zentrale Rolle im Datenschutzrecht zu. Nur über das Auskunftsrecht kann der Betroffene tatsächlich überprüfen, „wer was wann und bei welcher Gelegenheit" über ihn weiß.[365] Dennoch wird das Auskunftsrecht weder im geltenden noch im neuen Datenschutzrecht schrankenlos gewährt.

365 BVerfGE 65, 1 (43).

5.1 Auskunftserteilung nach Art. 15 DSGVO

Das Recht auf Auskunft in Art. 15 DSGVO ist im Wesentlichen[366] deckungsgleich mit seinem Vorgänger aus der Datenschutzrichtlinie und seiner Umsetzung im bisherigen Bundesdatenschutzgesetz. Das Auskunftsrecht ist zweitstufig aufgebaut. Auf Antrag der betroffenen Person ist der Verantwortliche verpflichtet, diese darüber zu informieren, ob er personenbezogene Daten der betroffenen Person verarbeitet. Ist dies der Fall, so sind der betroffenen Person bestimmte Informationen über die Umstände der Verarbeitung und ihrer Rechte gegenüber dem Verantwortlichen[367] zur Verfügung zu stellen. Hierzu findet sich in Art. 15 Abs. 1 Hs. 2 lit. a bis h DSGVO ein abschließender Katalog. Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, treten nach Art. 15 Abs. 2 DSGVO weitere Informationen zu den geeigneten Garantien nach Art. 46 DSGVO hinzu. Nach Art. 15 Abs. 3 DSGVO ist der betroffenen Person zudem eine Kopie der sie betreffenden personenbezogenen Daten zur Verfügung zu stellen. Die Rechte und Freiheiten anderer Personen dürfen durch das Recht nach Abs. 3 nicht beeinträchtigt werden.[368] Erwägungsgrund 63 DSGVO nennt hier beispielhaft Geschäftsgeheimnisse und Rechte des geistigen Eigentums. Die Feststellung, welche Rechte überwiegen, bedarf einer Abwägung im Einzelfall.

Das Recht auf Auskunft bildet die Basis für die Überprüfung der Rechtmäßigkeit der Verarbeitung durch den Betroffenen.[369] Ohne Auskunftsrecht sind die ihm nachfolgenden Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch oftmals faktisch nicht wahrnehmbar.

Erwägungsgrund 63 DSGVO erläutert, dass die Ausübung des Auskunftsrechts auf angemessene Abstände beschränkt sein soll. Gesundheitsbezogene Daten sind ausdrücklich vom Auskunftsrecht erfasst.

Die Form der Bereitstellung ist in Art. 15 Abs. 3 DSGVO geregelt. Wird der Antrag auf Auskunft elektronisch gestellt, so ist bei der Bereitstellung ein „gängiges elektronisches Format" zu wählen. Dem Antragsteller steht es aber frei,[370] ein anderes Format zu verlangen, sofern in der Wahl des Formats kein Missbrauch des Auskunftsrechts liegt.[371] Erwägungsgrund 63 DSGVO fordert ferner die Einrichtung eines Fernzugangs.

366 S. zu den Abweichungen im Detail *Hohmann/Miedzianowski*, in: Roßnagel 2018, § 4 Rn. 7, 14.
367 Namentlich die Rechte aus Art. 16, 17, 18, 21 und 79 DSGVO.
368 Art. 15 Abs. 4 DSGVO.
369 *Ehmann*, in: Ehmann/Selmayr, Art. 15 Rn. 1.
370 Ob teilweise (so *Bäcker*, in: Kühling/Buchner, Art. 15 Rn. 31) oder vollumfänglich ist dabei umstritten.
371 *Franck*, in: Gola, Art. 15 Rn. 23, 27. Bei exzessiven Anträgen kann der Verantwortliche Nach Art. 12 Abs. 5 Satz 2 DSGVO sich wahlweise weigern, tätig zu werden, oder ein angemessenes Entgelt verlangen.

Die weiteren Modalitäten der Ausübung des Auskunftsrechts finden sich in Art. 12 DSGVO. So hat die Mitteilung gemäß Art. 15 DSGVO durch den Verantwortlichen etwa nach Art. 12 Abs. 1 Satz 1 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu erfolgen.[372] Die Auskunft muss nach Art. 12 Abs. 5 DSGVO unentgeltlich erfolgen.

5.2 Auskunftserteilung nach Art. 8 Abs. 2 Satz 2 GRCh

Das Recht auf Auskunft aus Art. 15 DSGVO ergibt sich unmittelbar aus Art. 8 Abs. 2 Satz 2 GRCh, der ein solches Recht primärrechtlich etabliert.[373] Da die Charta jedoch jünger ist als die Datenschutzrichtlinie, kann Satz 2 auch als primärrechtliche Bestätigung von Art. 12 lit. a DSRL gelesen werden.[374]

Der Europäische Gerichtshof hat festgestellt, dass es zur Wahrung des Auskunftsrechts nach Art. 8 Abs. 2 Satz 2 GRCh genügt, dass der Antragsteller „eine vollständige Übersicht dieser Daten in verständlicher Form erhält, d.h. in einer Form, die es ihm ermöglicht, von diesen Daten Kenntnis zu erlangen und zu prüfen, ob sie richtig sind und der RL gemäß verarbeitet werden, sodass er ggf. die ihm in der RL verliehenen Rechte ausüben kann."[375]

Eine Einschränkung des Auskunftsrechts ist möglich nach der allgemeinen Einschränkungsklausel des Art. 52 Abs. 1 GRCh. Die Einschränkung muss gesetzlich vorgesehen sein und den Wesensgehalt der Rechte und Freiheiten der Charta achten. Sie muss verhältnismäßig und erforderlich bezogen auf die Ziele des Gemeinwohls und den Schutz der Rechte und Freiheiten anderer sein.

Ein Ausschluss des Rechts auf Auskunft kommt aufgrund seiner zentralen Bedeutung „nur bei zwingenden und sehr gewichtigen Gemeinwohlgründen in Betracht".[376]

Solche zwingenden und sehr gewichtigen Gemeinwohlgründe können in Grundrechten Dritter bestehen. Hier geht es aber um den Schutz von Grundrechten der betroffenen Person selbst. Als solche Grundrechte kommen das Grundrecht auf körperliche und geistige Unversehrtheit nach Art. 3 Abs. 1 GRCh[377] und eventuell das Grundrecht auf „Nichtwissen" infrage,[378] wenn man

372 Gebot der Genauigkeit und Verständlichkeit; *Bäcker*, in: Kühling/Buchner, Art. 12 Rn. 11.
373 *Franck*, in: Gola 2017, Art. 15 Rn. 2; *Ehmann*, in: Ehmann/Selmayr, Art. 15 Rn. 2.
374 *Bernsdorff*, in: Meyer 2014, Art. 8 Rn. 23.
375 *EuGH*, Urteil v. 17.7.2014 – C-141/12 und C-372/12, ECLI:EU:C:2014:2081, Rn. 60 – YS.
376 *Jarass* 2016, Art. 8 Rn. 16.
377 S. z.B. *Jarass* 2016, Art. 3 Rn. 5.
378 S. zum deutschen Verfassungsrecht im Kontext genetischer Informationen *Trute*, in: Roßnagel 2003, Kap. 2.5 Rn. 59ff., der dieses Recht der informationellen Selbstbestimmung und dem Persönlichkeitsrecht zuordnet. Ob dieses ohne Weiteres auf die Grundrechtecharta übertragen werden kann, bedürfte ausführlicher Untersuchungen.

dieses als Konkretisierung des Grundrechts auf Menschenwürde in Art. 1 GRCh verstehen wollte.[379] Diese beiden Grundrechte können mit dem Grundrecht auf Datenschutz konkurrieren, das in Art. 8 Abs. 2 Satz 2 GRCh das Grundrecht auf Auskunft über die eigenen, von anderen verarbeiteten Daten gewährleistet. Einen Ausgleich zwischen seinen eigenen Grundrechten herbeizuführen, fällt in die Entscheidungsfreiheit des Einzelnen und lässt eine gesetzliche Regelung nicht zu. Dadurch löst sich der Konflikt zwischen dem Wunsch nach Nichtwissen und dem Wunsch nach Auskunft. Hier kann der Verantwortliche nachfragen, ob die betroffene Person tatsächlich diese Auskunft möchte, die für sie belastend oder schädlich sein könnte. Die grundrechtliche Lösung kann aber nur darin bestehen, die betroffene Person diese Frage entscheiden zu lassen. In einem Konflikt zwischen Auskunft und körperliche Unversehrtheit ist die Lösung grundsätzlich auf die gleiche Weise zu suchen. Dies legt auch Art. 3 Abs. 2 lit. a GRCh nahe, der die Entscheidung in Gesundheitsfragen der betroffenen Person überlässt und die freie Einwilligung des Betroffenen nach vorheriger Aufklärung zur Voraussetzung jedes Heileingriffs macht. Lediglich wenn die betroffene Person objektiv nicht in der Lage ist, diese Entscheidung verständig zu treffen, könnte eine Verweigerung der Auskunft trotz Antrags der betroffenen Person vorgesehen werden. Fraglich ist, ob eine solche Ausnahme des Auskunftsanspruchs bereits dem geltenden Recht entnommen werden kann oder ob ein Gesetzgeber eine solche Ausnahme einführen kann.

5.3 Beschränkung der Auskunft nach § 27 Abs. 2 BDSG

§ 27 Abs. 2 BDSG-neu enthält zwei Möglichkeiten zur Beschränkung des Rechts auf Auskunft nach Art. 15 DSGVO.

Das Auskunftsrecht aus Art. 15 DSGVO ist nach Maßgabe von § 27 Abs. 2 Satz 1 BDSG-neu 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. § 27 Abs. 2 Satz 1 BDSG-neu ist dabei sprachlich eng an Art. 89 Abs. 2 DSGVO angelehnt.

§ 27 Abs. 2 Satz 2 BDSG-neu enthält eine weitere Einschränkung des Auskunftsrechts. Danach besteht das Auskunftsrecht nach Art. 15 DSGVO nicht, „wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde".

379 Dies ist bisher allerdings weder von der Rechtsprechung des EuGH noch von der Kommentarliteratur zur GRCh erfolgt.

Wie bereits oben festgestellt, versucht der Gesetzgeber mit dieser Regelung § 33 Abs. 2 Satz 1 Nr. 5 i.V.m. § 34 Abs. 7 sowie § 19a Abs. 2 Nr. 2 BDSG a.F. in das neue Bundesdatenschutzgesetz zu übertragen.[380] Er beruft sich dabei auf Art. 23 Abs. 1 lit. i DSGVO.[381]

Auf verfassungsrechtlicher Ebene ergibt sich das Recht auf Auskunft aus dem Recht auf informationelle Selbstbestimmung. Bezogen auf Krankenunterlagen etwa hat das Bundesverfassungsgericht festgestellt, dass sich ein Anspruch auf Einsicht aus dem Recht auf Selbstbestimmung und der personalen Würde des Patienten ergibt.[382] Es zählt zu den verfahrensrechtlichen Schutzvorkehrungen des Rechts auf informationelle Selbstbestimmung.[383] Aufgrund der verfassungsrechtlichen Dimension des Auskunftsrechts sind seinen Beschränkungen hohe Hürden gesetzt. Eine Beschränkung ist „allenfalls aus triftigen Gemeinwohlgründen oder zum Schutze Dritter" möglich.[384] Eine Auskunftsbeschränkung zum Wohl der betroffenen Person ist damit aus verfassungsrechtlicher Sicht bei Beachtung der hohen Hürden grundsätzlich möglich.

5.4 Beschränkung der Auskunftserteilung zum Wohl der betroffenen Person

Nach Erwägungsgrund 2 DSGVO soll die Datenschutz-Grundverordnung zum Wohlergehen natürlicher Personen beitragen. Das Wohl des Betroffenen wird sonst an keiner Stelle in der Verordnung explizit angesprochen.

Fraglich ist, ob ein Ausschluss der Auskunftserteilung nach Art. 15 DSGVO auch aus therapeutischen sowie ethischen Erwägungsgründen zum Wohl der betroffenen Person möglich ist. Der Bundesrat hatte im Rahmen des Gesetzgebungsverfahrens zum Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 darum gebeten, zu prüfen, ob ein solcher Ausschluss Aufnahme in das Gesetz finden sollte.[385] Die Bundesregierung hatte angekündigt, „die Vorschläge des Bundesrates im Bereich von Wissenschaft und Forschung im weiteren Verfahren" zu prüfen.[386] Sie hat den Vorschlag aber letztlich nicht übernommen.

380 BT-Drs. 18/11325, S. 99.
381 BT-Drs. 18/11325, S. 99. A.A. *Johannes/Richter*, DuD 2017, 300 (303): § 27 Abs. 2 Satz 2 BDSG-neu genüge den Anforderungen von Art. 23 Abs. 2 DSGVO nicht, könne aber auf Art. 89 Abs. 2 DSGVO gestützt werden.
382 *BVerfG*, NJW 1999, 1777.
383 *Di Fabio*, in: Mainz/Dürig 2016, Art. 2 Rn. 178.
384 *Di Fabio*, in: Mainz/Dürig 2016, Art. 2 Rn. 178.
385 BR-Drs. 110/17 (B) vom 10. März 2017, 25, Nr. 27 lit. d: „Der Bundesrat bittet im weiteren Gesetzgebungsverfahren zu prüfen, inwieweit ein Ausschluss der Auskunftserteilung neben den in § 27 BDSG-E genannten Voraussetzungen nach objektiven Kriterien auch aus therapeutischen sowie ethischen Erwägungsgründen zum Wohl der betroffenen Person aufgenommen werden sollte."
386 Gegenäußerung der Bundesregierung, BT-Drs. 19/11655, 53.

5.4.1 Beschränkung zum Wohl Dritter

Möglich ist ein Ausschluss des Rechts aus Art. 15 Abs. 3 DSGVO auf Bereitstellung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Dieses darf nach Art. 15 Abs. 4 DSGVO die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Damit ist zunächst eine Beschränkung des Auskunftsanspruchs aus therapeutischen und ethischen Erwägungsgründen zum Wohl Dritter möglich.

Darüber hinaus ist eine Beschränkung des Auskunftsrechts nach Art. 23 Abs. 1 lit. i Alt. 2 DSGVO zum Schutz der Rechte und Freiheiten anderer Personen möglich.

5.4.2 Beschränkung zum Wohle des Betroffenen

Direkt aus Art. 15 DSGVO ergibt sich jedoch keine mit Art. 15 Abs. 4 DSGVO vergleichbare Beschränkung zum Wohl der betroffenen Person selbst. Art. 15 DSGVO kann aber nach Maßgabe von Art. 23 Abs. 1 DSGVO durch Rechtsvorschrift der Union oder eines Mitgliedstaats[387] eingeschränkt werden. Jede Beschränkung muss dabei den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellen. Dies entspricht im Wesentlichen Art. 52 Abs. 1 GRCh. Darüber hinaus enthält Art. 23 Abs. 1 DSGVO einen Katalog von Zielen, die eine Beschränkung grundsätzlich rechtfertigen können. Die Voraussetzungen des Art. 23 DSGVO müssen kumulativ vorliegen.[388] Der Katalog der Ziele, die eine Beschränkung rechtfertigen können, ist abschließend.

Zusätzlich sind die Vorgaben zu beachten, die der Europäische Gerichtshof in seiner Rechtsprechung entwickelt hat.[389] Diese entsprechen letztlich dem, was auch die Verordnung selbst fordert:

- Klarheit und Präzision der beschränkenden Vorschrift,
- Garantien für den Schutz der Rechte des Betroffenen,
- Achtung des Wesensgehalts der relevanten Grundrechte und
- Notwendigkeit der Einschränkung.

Bezogen auf die Ausgangsfrage kommt hier primär Art. 23 Abs. 1 lit. i DSGVO in seiner ersten Alternative in Betracht. Danach ist eine Beschränkung unter den genannten Voraussetzungen möglich, sofern diese den Schutz der betroffenen Person sicherstellt. Diese Voraussetzung ist äußerst weit gefasst und entspricht wörtlich der Regelung des Art. 13 Abs. 1 lit. g DSRL. Aber auch die in den Buchstaben a bis h und j genannten Zielen dienen letztlich dem Wohl

387 Bezogen auf die Gesetzgebungsmaßnahme sind zusätzlich die Vorgaben von Art. 23 Abs. 2 DSGVO zu beachten.
388 *Bertermann*, in: Ehmann/Selmayr, Art. 23 Rn. 3.
389 S. insbesondere *EuGH*, Urteil vom 6.10.2015, C-362/14. ECLI:EU:C:2015:650, Schrems.

der betroffenen Person. Auf grundrechtlicher Ebene findet Art. 23 Abs. 1 lit. i DSGVO seine Rechtfertigung unter anderem in Art. 3 Abs. 1 GRCh.

Zur Vorgängerregelung in Art. 13 Abs. 1 lit. g DSRL wurde gefordert, die Beschränkung dürfe nicht dazu führen, dass „unter dem Gesichtspunkt des Betroffenenschutzes dessen grundrechtliche Position ad absurdum geführt wird".[390] Dies ist auch für Art. 23 Abs. 1 lit. i DSGVO zu fordern. Ein auch im Kontext von Art. 23 DSGVO relevantes Beispiel liefert Erwägungsgrund 42 DSRL, wo es heißt, die Mitgliedstaaten können das Auskunftsrecht im Interesse der betroffenen Person in der Art beschränken, dass „Auskunft über medizinische Daten nur über ärztliches Personal erhalten werden kann".

5.4.3 Beschränkung nach § 630g BGB

Ein Beispiel für eine mit Art. 23 Abs. 1 lit. i DSGVO kompatible Beschränkung stellt bereits jetzt § 630g BGB dar. Dieser enthält in § 630g Abs. 1 BGB ein Recht auf unverzügliche Einsichtnahme in die Patientenakte im Kontext von Behandlungsverträgen i.S.v. § 630a BGB. Dieses wird jedoch nur gewährt, „soweit der Einsichtnahme nicht erhebliche therapeutische Gründe entgegenstehen".[391] Die Ablehnung ist zu begründen.[392] Umfasst vom Einsichtsrecht des Patienten sind auch „Niederschriften über persönliche Eindrücke und subjektive Wahrnehmungen des Behandelnden".[393] Erhebliche therapeutische Gründe sollen etwa dann vorliegen, wenn die Ausübung des Rechts auf Einsichtnahme zu einer „erheblichen gesundheitlichen (Selbst-)Schädigung des Patienten" führen könnte.[394] Sie sind sorgfältig für jeden Einzelfall zu ermitteln und auf konkrete und substantiierte Anhaltspunkte zu stützen.[395] Im Zweifel ist für die Auskunft zu entscheiden.[396] Eine paternalistische Bevormundung des Patienten durch den Behandelnden ist ausdrücklich nicht erwünscht.[397]

Nach § 630g Abs. 1 Satz 3 BGB ist § 811 BGB anzuwenden. Dieser besagt, dass die Vorlegung der Patientenakte an dem Ort zu erfolgen hat, an welchem sie sich befindet.[398] Ausnahmen von diesem Grundsatz sind im Einzelfall aber möglich.

390 *Ehmann/Helfrich* 1999, Art. 13 Rn. 76.
391 § 630g Abs. 1 Satz 1 BGB.
392 § 630g Abs. 1 Satz 2 BGB.
393 BT-Drs. 17/10488, 27. Das Persönlichkeitsrecht des Behandelnden soll nur in Ausnahmefällen einen Ausschluss rechtfertigen können; *Wagner*, in: MüKo BGB, § 630g Rn. 8.
394 BT-Drs. 17/10488, 26. Dies soll etwa dann der Fall sein, wenn der Patient durch die Einsichtnahme „zum Selbstmord veranlasst würde"; BVerwGE 82, 45. Die Schwelle ist also hoch angesetzt.
395 BT-Drs. 17/10488, 26f.
396 *Wagner*, in: MüKo BGB, § 630g Rn. 10.
397 BT-Drs. 17/10488, 26; *Wagner*, in: MüKo BGB, § 630g Rn. 11.
398 Ein Ortswechsel kann nur aus „wichtigem Grund" verlangt werden; § 811 Abs. 1 Satz 2 BGB. Ein solcher soll etwa „bei einer nicht unerheblichen Erkrankung des Patienten" oder bei einem Umzug des Behandelnden" vorliegen; BT-Drs. 17/10488, 27.

Anzumerken ist, dass vor einer vollständigen Verweigerung der Einsichtnahme eine partielle Verweigerung als milderes Mittel zu prüfen ist.[399] Zudem kommen die „durch den Behandelnden unterstützte oder auch begleitende Einsichtnahme" oder die Vermittlung durch eine dritte Person ebenfalls als milderes Mittel in Betracht.[400] Ferner ist der Rechtsgedanke des § 603e Abs. 5 BGB zu beachten, wonach auf den Entwicklungsstand und die Verständnismöglichkeit sowie auf das Wohl des Patienten Rücksicht zu nehmen ist.[401] Eine vollständige Verweigerung der Einsichtnahme dürfte damit auf wenige Extremfälle beschränkt sein.[402]

Zu dem Recht auf unverzügliche Einsichtnahme in die Patientenakte aus § 630g Abs. 1 BGB tritt in § 630 Abs. 2 Satz 1 BGB ein Recht auf Erhalt physischer oder elektronischer Abschriften der Patientenakte. Hier gelten dieselben Einschränkungsmöglichkeiten wie im Falle der Einsichtnahme. Der Anspruch auf eine bestimmte Form der Abschriften soll jedoch auf Fälle beschränkt sein, in denen der Patient ein berechtigtes Interesse an dieser hat.[403]

§ 630 Abs. 3 BGB enthält Regelungen zur Wahrnehmung der Rechte aus Abs. 1 und 2 im Falle des Todes des Patienten durch Erben und nächste Angehörige.

Das Auskunftsrecht nach § 630g BGB kann durch individuelle Parteivereinbarung, nicht aber durch allgemeine Geschäftsbedingungen ausgeschlossen werden.[404]

Es zeigt sich mit Blick auf § 630g BGB, dass der Einschränkung der Auskunftserteilung aus therapeutischen und ethischen Erwägungsgründen zum Wohl der betroffenen Person im Falle von Gesundheitsdaten hohe Hürden gesetzt sind. Jedes Ersuchen ist als individueller Einzelfall umfassend zu prüfen, sofern tatsächlich eine Ablehnung in Betracht kommt. Insbesondere kann nicht jede potenzielle Schädigung des Betroffenen durch die Einsichtnahme als Rechtfertigungsgrund dienen; diese muss vielmehr erheblich sein und etwa der Suizid des Betroffenen drohen. Im Extremfall kann sich ein Schädigungspotenzial sogar zu einem Beschränkungsgebot verdichten.

Die verfassungsrechtlichen Grundlagen für § 630g BGB hat das Bundesverfassungsgericht 2006 in einem Beschluss aufgearbeitet.[405] Das Recht aus § 630g BGB dient vornehmlich dem Recht des Patienten auf informationelle Selbstbestimmung.[406] Die vom Gericht aufgearbeiteten Grundlagen lassen sich abstrahieren und auf andere Sachverhalte übertragen. Auf diese Weise wurden

399 So der Umkehrschluss aus BT-Drs. 17/10488, 26.
400 BT-Drs. 17/10488, 27.
401 *Wagner*, in: MüKo BGB, § 630g Rn. 5.
402 Sie ist allenfalls ultima ratio; *Wagner*, in: MüKo BGB, § 630g Rn. 12.
403 *Wagner*, in: MüKo BGB, § 630g Rn. 20.
404 *Wagner*, in: MüKo BGB, § 630g Rn. 30.
405 *BVerfG*, Beschluss vom 9.1.2006 – 2 BvR 443/02, NJW 2006, 1116.
406 BT-Drs. 17/10488, 26; *Wagner*, in: MüKo BGB, § 630g Rn. 4.

bereits auf nationaler Ebene Einsichtsrechte in Pflegeunterlagen[407] und in die im Kontext der Teilnahme an einer Lehranalyse angefertigten Dokumentation[408] anerkannt.[409] Auch eine Übertragung auf das Auskunftsrecht aus Art. 8 GRCh ist möglich, soweit dieses dem aus dem Recht auf informationelle Selbstbestimmung abgeleiteten Recht wesensgleich ist. Insofern kann § 630g BGB als eine mit Art. 23 Abs. 1 lit. i DSGVO vereinbare Ausfüllung der Öffnungsklausel angesehen werden.

5.4.4 Beschränkung im Kontext wissenschaftlicher Forschung

Fraglich ist, ob eine solche Beschränkung auch im Kontext von wissenschaftlichen Forschungsvorhaben möglich wäre.

Die Datenschutz-Grundverordnung will die Verarbeitung von personenbezogenen Daten im wissenschaftlichen Kontext bevorzugen und enthält deshalb mit Art. 85 Abs. 2 DSGVO eine Öffnungsklausel, die im Vergleich zu Art. 23 Abs. 1 DSGVO deutlich weitreichendere[410] Abweichungen und Ausnahmen von den Vorgaben der Verordnung durch die Mitgliedstaaten ermöglicht. Eine Einengung findet aber wiederum durch die Verwendung des Begriffspaars „academic expression" statt.[411] Hier steht die Meinungsäußerung im Vordergrund. Eine Beschränkung des Auskunftsrechts zu wissenschaftlichen Forschungszwecken kann deshalb nicht auf Art. 85 Abs. 2 DSGVO gestützt werden.

Infrage käme aber Art. 89 Abs. 2 DSGVO, der zwar Ausnahmen von den Rechten aus Art. 15 DSGVO ermöglicht, dies aber nur insoweit, „als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind". Dies ist bei einer Beschränkung der Auskunftserteilung aus therapeutischen und ethischen Erwägungsgründen zum Wohl der betroffenen Person nicht der Fall. Eine derartige Beschränkung muss deshalb auf Art. 23 Abs. 1 DSGVO gestützt werden und kann nicht an der Bevorzugung der wissenschaftlichen Forschung teilhaben.

Eine Beschränkung wäre aber nach Art. 23 Abs. 1 lit. i DSGVO möglich, sofern die Hürden entsprechend hoch angesetzt werden und die Beschränkung als Ultima Ratio ausgestaltet wäre.[412] Da auch hier auf erhebliche Schäden des Betroffenen durch die Offenlegung ihm selbst gegenüber abzustellen ist, dürfte eine solche Beschränkung faktisch nur auf Gesundheitsdaten Anwendung

407 BGHZ 185, 74.
408 *BGH*, Urteil vom 7.11.2013 – III ZR 54/13.
409 S. *Wagner*, in: MüKo BGB, § 630g Rn. 31f.
410 *Pötters*, in: Gola 2017, Art. 85 Rn. 16.
411 S. Kap. 4.2.
412 S. auch *Bäcker*, in: Kühling/Buchner, Art, 23 Rn. 30, der Art. 23 Abs. 1 lit. Alt. 1 DSGVO „allenfalls einen äußerst schmalen Anwendungsbereich" zugesteht.

finden. Unabhängig davon kann das Auskunftsrecht aber auch im Kontext wissenschaftlicher Forschung durch Individualvereinbarung ausgeschlossen werden.[413]

Eine Beschränkung der Auskunftserteilung aus therapeutischen und ethischen Erwägungsgründen zum Wohl der betroffenen Person im Kontext von wissenschaftlichen Forschungsvorhaben ist also durchaus denkbar, müsste aber auf einer konkreten Rechtsvorschrift beruhen. Eine solche Rechtsvorschrift enthält das neue Bundesdatenschutzgesetz nicht. Sie könnte mit Blick auf die verfassungsrechtlichen und unionsrechtlichen Vorgaben allerdings geschaffen werden. Da Einschränkungen des Auskunftsrechts nach Art. 23 Abs. 1 DSGVO nur im Wege von Gesetzgebungsmaßnahmen möglich sind, wäre eine entsprechende Rechtsvorschrift auch angezeigt. Der Begriff der Gesetzgebungsmaßnahme ist vor dem Hintergrund von Art. 52 Abs. 1 GRCh[414] jedoch weit auszulegen, sodass er etwa auch Richterrecht umfasst; ein formelles Gesetz ist nicht erforderlich.[415]

Denkbar wäre deshalb auch eine analoge Anwendung von § 630g BGB im Kontext wissenschaftlicher Forschungsvorhaben. Dies gründet darauf, dass § 630g BGB nicht als abschließende Regelung konzipiert ist und nicht auf die Akteneinsicht im Rahmen von Behandlungsverträgen beschränkt ist.[416] Eine analoge Anwendung des § 630g BGB findet etwa bezogen auf die Pflegedokumentation statt. Zudem ist eine analoge Anwendung auf Lehranalysen anerkannt.[417]

5.5 Ergebnis zum Ausschluss der Auskunftserteilung zum Wohl der betroffenen Person

Das Recht auf Auskunft in Art. 8 Abs. 2 Satz 2 GRCh und Art. 15 DSGVO ist im Wesentlichen deckungsgleich mit seinem Vorgänger aus der Datenschutzrichtlinie und seiner Umsetzung im bisherigen Bundesdatenschutzgesetz. Es bildet die Basis für die Überprüfung der Rechtmäßigkeit der Verarbeitung durch den Betroffenen. Beschränkungen des Auskunftsrechts – auch zum Wohl der betroffenen Person – sind nach Art. 52 GRCh und Art. 23 DSGVO möglich, aber in besonderem Maße begründungsbedürftig. Beschränkungsmöglichkeiten für das Recht auf Auskunft enthält etwa § 27 Abs. 2 BDSG-neu, die aber für eine Verweigerung der Auskunftserteilung zum Wohl der betroffenen Person nicht gelten.

413 Zu Einschränkungsmöglichkeiten von Rechten der betroffenen Person s. Kap. 3.4.3.
414 *Borowsky*, in: Meyer, Art. 52 Rn. 20f.
415 S. auch *Kühling/Martini u.a.* 2016, 72; *Bäcker*, in: Kühling/Buchner, Art. 23 Rn. 35.
416 *Wagner*, in: MüKo BGB, § 630g Rn. 31.
417 S. *Mansel*, in: Jauernig, § 630g BGB, Rn. 2. S. auch bereits oben in Kap. 5.4.3.

Ein Ausschluss der Auskunftserteilung zum Wohl der betroffenen Person ist jedoch nach § 630g BGB möglich. Diese Vorschrift ist mit Art. 23 Abs. 1 lit. i DSGVO kompatibel. Dem Ausschluss sind dabei hohe Hürden gesetzt.

Auch im Kontext von wissenschaftlichen Forschungsvorhaben ist eine ähnliche Einschränkung – als Ultima Ratio – grundsätzlich möglich. Diese müsste aber auf einer konkreten Rechtsvorschrift beruhen. Eine solche Rechtsvorschrift existiert derzeit nicht, könnte aber geschaffen werden. Die Beschränkung muss aber auf Art. 23 Abs. 1 DSGVO gestützt werden und kann nicht an der Bevorzugung der wissenschaftlichen Forschung durch die Grundverordnung teilhaben. Unabhängig davon kann das Auskunftsrecht aber auch im Kontext wissenschaftlicher Forschung durch Individualvereinbarung ausgeschlossen werden.

6 Weitergabe von Informationen an „mitwirkende Personen“ im Rahmen der medizinischen Forschung

Das folgende Kapitel beantwortet die Forschungsfrage 4.6:

> *Nach dem Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (BR-Drucksache 163/17) soll § 203 StGB in der Form geändert werden, dass die Weitergabe von Informationen an „mitwirkende Personen“ für einen Berufsgeheimnisträger (z.B. Arzt) straflos sein soll, wenn diese an der „beruflichen Tätigkeit“ des Berufsgeheimnisträgers mitwirken. Prüfen Sie bitte, ob eine Mitwirkung an einer Forschungstätigkeit eines Arztes auch als Mitwirkungshandlung im Sinne der neuen Rechtsvorschrift verstanden werden kann. Gehen Sie bitte darauf ein, wie die „berufliche Tätigkeit“ eines Arztes auch mit Blick auf die EU-DSGVO und den bisherigen Rechtsrahmen definiert wird und ob Unterschiede zwischen der ärztlichen Tätigkeit in einem Universitätskrankenhaus/sonstigem Krankenhaus und einer Arztpraxis besteht.*

Das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen bewirkt in seinem Art. 1 eine wichtige Änderung des § 203 StGB.[418]

418 S. Kap. 1.

6.1 Die Neuregelung des § 203 StGB

Ziel der Änderung des § 203 StGB ist es, „die Möglichkeiten für Berufsgeheimnisträger zu erweitern, sich im Rahmen ihrer beruflichen oder dienstlichen Tätigkeit ohne (straf-)rechtliches Risiko der Mitwirkung dritter Personen zu bedienen".[419]

Strafbar macht sich nach § 203 StGB, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Berufsgeheimnisträger im Sinn von Abs. 1 und 2 anvertraut worden oder sonst bekannt geworden ist. Für diese bestand in der Hinzuziehung von Personen, die nicht ebenfalls der Strafbarkeit von § 203 StGB unterfallen, ein rechtliches Risiko.[420] Die herrschende Meinung ging davon aus, dass nicht einem eng auszulegenden Gehilfenbegriff unterfallende Personen nicht zur Sphäre des Berufsgeheimnisträgers zählen[421] und damit nicht am Vertrauensverhältnis teilnehmen.[422] Andere argumentierten, der Begriff des berufsmäßig tätigen Gehilfen könne weit ausgelegt werden und umfasse etwa auch externe IT-Dienstleister.[423] Die Hinzuziehung insbesondere eines externen Dienstleisters barg mithin das Risiko einer Strafbarkeit nach § 203 StGB.[424] Zudem bestand kein strafrechtlicher Schutz für die externen Personen anvertrauten oder bekannt gewordenen Geheimnisse.

Die zunehmende Nutzung von Informationstechnik macht es häufig aber erforderlich, externe Fachkräfte hinzuzuziehen, die außerhalb der Sphäre des Berufsgeheimnisträgers stehen, beispielsweise zur Wartung der eingesetzten Technik. Dabei können diesen Personen jedoch fremde Geheimnisse offenbart werden. Zudem wird zunehmend die eigene Informationstechnik durch externe Technik ergänzt, beispielsweise in Form des Cloud Computing. Der Weg über eine informierte Einwilligung des Berechtigten führte zwar zu einem Ausschluss der Strafbarkeit nach § 203 StGB,[425] da in diesem Fall eine Befugnis vorliegt.[426] Deren Einholung ist aber nicht immer möglich und mit Aufwand

419 BT-Drs. 18/12940, 1.

420 S. z.B. *Behling u.a.* 2015, 9ff., 15; *Jandt/Roßnagel*, MedR 2011, 140ff.

421 Die Gesetzesbegründung sieht in der Einbindung externer Personen eine Überdehnung des Begriffs „Gehilfe"; BT-Drs. 18/11936, 18. Der Begriff sei der Gedanke eines „geschlossenen Geheimnisträgerkreises immanent". „Externe Personen, die selbständig tätig sind oder die in den Betrieb eines Dritten eingebunden sind, sind deshalb regelmäßig keine Gehilfen".

422 So auch die Gesetzesbegründung, BT-Drs. 18/11936, 18; *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 19b; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 21; *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 54, 56; bezogen auf Cloud-Anbieter *Wicker* 2016, 136ff.

423 S. auch *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 38a, Gehilfe, sofern beim Outsourcing „die organisatorische Anbindung der Datenverwalter an den Auftraggeber gewährleistet" ist. Nach *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 129, Gehilfe, wenn die Aufträge „eine besonders enge Beziehung zum Aufgabenbereich des Schweigepflichtigen aufweisen".

424 S. etwa *LG Flensburg*, Urteil vom 5.7.2013 – 4 O 54/11; s. zum Outsourcing im Gesundheitsbereich *Jandt/Roßnagel/Wilke*, NSR 2011, 641ff.

425 S. z.B. *Jandt/Roßnagel/Wilke*, RDV 2011, 222 (228); *Jandt/Roßnagel/Wilke*, NSR 2011, 641.

426 Man beachte aber den Streit, ob die Einwilligung das Tatbestandsmerkmal „unbefugt" ausschließt oder die Rechtswidrigkeit entfallen lässt, s. hierzu *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 58ff.

verbunden.[427] Zudem würde dieser Weg eine nach vorliegender Einwilligung und verweigerter Einwilligung differenzierte Datenverarbeitung erfordern. Auch die Annahme einer konkludenten Einwilligung[428] barg rechtliche Risiken; die Weitergabe von Geheimnissen zu Forschungszwecken kann sie zudem nicht legitimieren.[429] Zahlreiche Meinungsstreitigkeiten in der strafrechtlichen Fachliteratur zu § 203 StGB und fehlende obergerichtliche Rechtsprechung zum Thema Outsourcing verkomplizierten die Sache weiter und sorgten für Rechtsunsicherheit.[430] In der Praxis wurde teilweise versucht, die Problematik durch den Abschluss von Mehrfach-Arbeitsverhältnissen zu lösen.[431]

Die Novelle des § 203 StGB soll hier nun Rechtsklarheit für alle Beteiligten herstellen und den Schutz von Privatgeheimnissen auch in einer digitalisierten Arbeitswelt garantieren.

6.1.1 Der neue § 203 StGB

In § 203 StGB wurde der bisherige Abs. 2a aufgehoben und durch die neuen Abs. 3 und 4 ersetzt. Diese lauten:

> *„(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.*
>
> *(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer*
>
> *1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung*

427 Die Gesetzesbegründung nennt etwa die Archivierung von Altbeständen von Daten; BT-Drs. 18/11936, 18. Zu den Problemen der Einwilligung s. auch *Behling u.a.* 2015, S. 15; *Pohle/Ghaffari*, CR 2017, 489 (490); *Wicker* 2016, S. 142f.

428 S. hierzu *Altenhain*, in: Matt/Renzikowski 2013, § 203 Rn. 35; *Kargl*, in: Kindhäuser/Neumann/Paeffgen 2017, § 203 Rn. 21a; *Cierniak/Niehaus*, in: MüKo StGB 2012, § 203 Rn. 56; *Wicker* 2016, 143.

429 *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 67.

430 *Pohle/Ghaffari*, CR 2017, 489 (489, 491); *Jandt/Roßnagel/Wilke*, NSR 2011, 641ff.; *Preuß*, DuD 2016, 802ff.

431 *Pohle/Ghaffari*, CR 2017, 489 (491).

verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat."

Tatbestandlich fordern § 203 Abs. 1 und 2 StGB das unbefugte Offenbaren eines fremden Geheimnisses. Täter können die in Abs. 1 und 2 aufgelisteten Personen sein, wenn ihnen das fremde Geheimnis im Rahmen ihrer Tätigkeit nach Abs. 1 und 2 anvertraut oder sonst bekannt geworden ist. Unumstritten war das mündliche Offenbaren. Im Falle verkörperter Geheimnisse war umstritten, ob wie im Falle des mündlichen Offenbarens eine tatsächliche Kenntnisnahme erforderlich ist oder ob die bloße Möglichkeit der Kenntnisnahme ausreicht.[432] Die Gesetzesbegründung enthält nun die Klarstellung, „dass ein Offenbaren bereits dann gegeben ist, wenn die Möglichkeit der Kenntnisnahme von Geheimnissen besteht".[433] Der Streit ist damit zugunsten eines weiten Offenbarungsbegriffs entschieden. Der Einsatz technischer Sicherungsmaßnahmen soll ein Offenbaren ausschließen können.[434] Damit kann letztlich auch das Unterlassen technisch-organisatorischer Sicherungsmaßnahmen ein Offenbaren begründen.

Nach § 203 Abs. 3 Satz 1 StGB n.F. liegt kein Offenbaren vor, wenn den Abs. 1 und 2 unterfallende Personen Geheimnisse berufsmäßig tätigen Gehilfen oder den ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Im medizinischen Kontext ist dabei insbesondere an medizinische Fachangestellte und medizinisch-technische Assistenten zu denken. Die Regelung hat primär eine klarstellende Funktion.[435] So wurde auch für § 203 StGB a.F. als ganz herrschende Meinung angenommen, dass bei der Hinzuziehung von Hilfspersonen im beruflichen Kontext keine Offenbarung vorliegt, da die Hilfsperson „unmittelbar an dem konkreten Vertrauensverhältnis teilnimmt".[436] Dabei wurde auch darauf abgestellt, dass die Hinzuziehung im

432 Zum Streit s. *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 28f.; *Pohle/Ghaffari*, CR 2017, 489 (490).

433 BT-Drs. 18/11936, 28. Das „intellektuelle Verstehen" seitens des Dritten ist nicht erforderlich; *Heger*, in: Lackner/Kühl 2014, § 203 Rn. 17.

434 So *Pohle/Ghaffari*, CR 2017, 489 (491); *Wicker* 2016, S. 133f.; *Hartung*, VersR 2012, 400 (405); *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 19b.

435 BT-Drs. 18/11936, 2.

436 *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 19a; s. auch *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 53; *Wicker* 2016, S. 136.

Rahmen einer ordnungsgemäßen Berufsausübung erforderlich ist.[437] Dieses Merkmal findet sich so nicht im Wortlaut von § 203 Abs. 3 Satz 1 StGB n.F., dürfte jedoch auch in die neue Vorschrift hineinzulesen sein. Eine Erforderlichkeit soll aber bereits dann gegeben sein, wenn der Berufsgeheimnisträger ein wirtschaftliches Interesse geltend machen kann.[438]

§ 203 Abs. 3 Satz 2 Hs. 1 StGB n.F. enthält eine Fallgruppe, in der zwar ein Offenbaren vorliegt, dieses aber erlaubt ist. Dies ist dann der Fall, wenn fremde Geheimnisse sonstigen Personen offenbart werden, die an der Tätigkeit des Offenbarenden mitwirken. Das Offenbaren muss für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Person erforderlich sein.

Nach § 203 Abs. 3 Satz 2 Hs. 2 StGB n.F. ist ein Offenbaren auch dann erlaubt, wenn sonstige mitwirkende Personen sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in Abs. 1 und 2 Genannten mitwirken.

Die mitwirkenden Personen werden durch § 203 Abs. 4 Satz 1 StGB n.F. der Strafbarkeit nach § 203 StGB unterworfen.[439] Strafbar macht sich zudem der Berufsgeheimnisträger, wenn er nicht dafür Sorge trägt, dass die sonstige mitwirkende Person zur Geheimhaltung verpflichtet wird, und diese ein Geheimnis unbefugt offenbart.[440] Gleiches gilt für die mitwirkende Person, wenn sie sich weiterer Personen bedient.[441] Bestraft wird ferner, wer nach dem Tod einer zur Geheimhaltung verpflichteten ein Geheimnis unbefugt offenbart, das er von der verstorbenen Person oder aus deren Nachlass erfahren hat.[442]

Zu beachten ist, dass der Berufsgeheimnisträger bereits durch Berufsrecht zur Verschwiegenheit verpflichtet sein kann.

6.1.2 Verhältnis von § 203 StGB und Datenschutzrecht

§ 203 StGB dient zumindest auch dem Schutz des Rechts auf informationelle Selbstbestimmung.[443]

437 *Lenckner/Eisele*, in: Schönke/Schröder 2014, § 203 Rn. 19a; *Jandt/Roßnagel*, MedR 2011, 140 (142).
438 BT-Drs. 18/11936, 18.
439 Die Gesetzesbegründung spricht von einer „Verlängerung“ des strafrechtlichen Geheimnisschutzes; BT-Drs. 18/11936, 20.
440 § 203 Abs. 4 Satz 2 Nr. 1 StGB n.F. Die Pflicht zur Verpflichtung zur Geheimhaltung entfällt, wenn die sonstige mitwirkende Person selbst Berufsgeheimnisträger ist.
441 § 203 Abs. 4 Satz 2 Nr. 2 StGB n.F.
442 § 203 Abs. 4 Satz 2 Nr. 3 StGB n.F.
443 Zum Streit s. *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 1; *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 3; *Tag*, in: Dölling/Duttge/König/Rössner, § 203 StGB, Rn. 3ff.; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 2; *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 6; *Weidemann*, in: BeckOK StGB, § 203 Rn. 2; *Heger*, in: Lackner/Kühl, § 203 Rn. 1.

Tatobjekt des § 203 Abs. 1 und Abs. 2 StGB ist das fremde Geheimnis.[444] Dabei kann es sich um eine beliebige Tatsache handeln. Voraussetzung ist nach einer Auffassung lediglich, dass der Geheimnisträger an der Geheimhaltung der Tatsache ein sachlich begründetes Interesse hat oder haben würde.[445] Dies wird angenommen für gesundheitliche Verhältnisse, kann aber auch schon anzunehmen sein für die bloße Tatsache, dass sich jemand überhaupt in psychologischer oder ärztlicher Behandlung befindet, was ebenso für die Begleitumstände einer Krankenhausaufnahme gelten kann.[446] Nach anderer Ansicht liegt ein Geheimnis vor, wenn die Tatsache nur einem beschränkten Personenkreis bekannt ist[447] und der Betroffene einen Geheimhaltungswillen hat.[448] Dies wird aber mit dem Erfordernis eines schutzwürdigen[449] Geheimhaltungsinteresses kombiniert.[450]

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies bedeutet, dass nicht jedes personenbezogene Datum ein Geheimnis ist, jedoch handelt es sich bei jedem Geheimnis um ein personenbezogenes Datum.[451] Wird dieses personenbezogene Datum nach Art. 2 Abs. 1 DSGVO ganz oder teilweise automatisiert verarbeitet oder zwar nichtautomatisiert verarbeitet, aber in einem Dateisystem gespeichert oder wird diese Speicherung angestrebt, so ist ab dem 25. Mai 2018 grundsätzlich die Datenschutz-Grundverordnung anwendbar. Eine Verarbeitung ist dann nur unter den Voraussetzungen von Art. 6 Abs. 1 und eventuell Art. 9 Abs. 2 DSGVO rechtmäßig. Gesundheitsdaten, in Art. 4 Nr. 15 DSGVO definiert als personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen, sind dabei nach Art. 9 DSGVO als besondere Kategorie personenbezogener Daten besonders geschützt.

Eine § 1 Abs. 3 Satz 2 BDSG a.F. wortgleiche Entsprechung findet sich in § 1 Abs. 2 Satz 3 BDSG-neu. Danach bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungsvorschriften durch das Bundesdatenschutzgesetz

444 Zusätzlich ist § 203 Abs. 2 Satz 2 StGB zu beachten, der unter bestimmten Umständen Einzelangaben über persönliche und sachliche Verhältnisse dem Geheimnis gleichstellt.

445 *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 5, 7.

446 *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 7.

447 Als „faktisches Begriffselement" *Heger*, in: Lackner/Kühl, § 203 Rn. 14.

448 Nach a.A. ist ein Geheimhaltungswille nicht erforderlich; so *Weidemann*, in: BeckOK StGB, § 203 Rn. 4a; s. auch *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 19f., wonach der Geheimhaltungswille erst auf Ebene der Rechtfertigung relevant ist. S. auch *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 12ff.

449 Im Sinn einer „objektiven Geheimhaltungswürdigkeit" *Heger*, in: Lackner/Kühl, § 203 Rn. 14.

450 S. *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 21; *Weidemann*, in: BeckOK StGB, § 203 Rn. 4a; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 6b ff.

451 So auch *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 17, der einen Personenbezug fordert und diesbezüglich auf § 3 Abs. 1 BDSG a.F. verweist; s. auch *Heger*, in: Lackner/Kühl, § 203 Rn. 14: „Das Geheimnis muss personenbezogen sein."

unberührt. Datenschutzrecht und Strafrecht gelten nebeneinander.[452] Sie haben unterschiedliche Adressaten (Verantwortlicher und Arzt) sowie unterschiedliche Schutzgüter (Patientengeheimnis und informationelle Selbstbestimmung) und Schutzzwecke (Schutz vor Offenbarung und Schutz vor unzulässiger Verarbeitung).[453] Daher besteht keine Kollision zwischen § 203 StGB und datenschutzrechtlichen Vorschriften im Sinne von § 1 Abs. 3 Satz 1 BDSG a.F.

Ist die Verarbeitung nach geltendem Datenschutzrecht rechtmäßig, so folgt daraus deshalb nicht, dass die Offenbarung nicht mehr unbefugt im Sinn von § 203 Abs. 1 und 2 StGB ist, auch wenn die Übermittlung an den Empfänger aus datenschutzrechtlicher Sicht rechtmäßig ist. Es ist vielmehr eine gesonderte Offenbarungsbefugnis erforderlich. „Allgemeine datenschutzrechtliche Übermittlungsbefugnisse genügen grundsätzlich nicht“.[454] Anderes gilt aber im Falle von Übermittlungs- und Offenbarungspflichten, die sich auch aus dem Datenschutzrecht ergeben können. Liegt eine solche Pflicht vor, entfällt das Tatbestandsmerkmal des unbefugten Offenbarens. Zudem sollen auch bereichsspezifische Datenschutzvorschriften für den Bereich der medizinischen Forschung anders als allgemeines Datenschutzrecht eine Befugnis zur Übermittlung im Sinne von § 203 StGB darstellen.[455]

Eine Verschränkung zwischen § 203 StGB und dem Datenschutzrecht ergibt sich aus der Tatsache, dass auch ein Unterlassen geeigneter technisch-organisatorischer Sicherungsmaßnahmen ein Offenbaren darstellen kann. Hier kann auf die Vorgaben des Art. 32 DSGVO zur Datensicherheit abgestellt werden, um Anhaltspunkte dafür zu finden, wo die Schwelle für ein strafbares Unterlassen liegt. Eine Parallele besteht zudem zwischen dem Erfordernis der Erforderlichkeit in § 203 Abs. 3 Satz 2 n.F. und dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO.

Die Befugnisse der Aufsichtsbehörden können nach Art. 90 Abs. 1 DSGVO gegenüber Berufsgeheimnisträgern eingeschränkt werden. Der Gesetzgeber hat diese Möglichkeit durch § 29 Abs. 3 BDSG-neu genutzt. Hier spielt § 203 StGB eine konstituierende Rolle. Den dort genannten Personen gegenüber sind die Befugnisse der Aufsichtsbehörde eingeschränkt, „soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde“. § 203 StGB ist damit letztlich auch Grundlage einer signifikanten datenschutzrechtlichen Bevorzugung.

---

452 *Pöttgen* 2009, 222f.; *Kilian*, NJW 1998, 787 (787f.); s. auch *Wronka*, RDV 2017, 129 (131).

453 *Jandt/Roßnagel/Wilke*, RDV 2011, 222 (228); *Jandt/Roßnagel*, MedR 2013, 17ff.; *Preuß*, DuD 2016, 802 (803).

454 *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 38.

455 *Pöttgen* 2009, 222f.: „Anders stellt sich die Lage jedoch bei den bereichsspezifischen Vorschriften des für den Bereich der medizinischen Forschung relevanten Datenschutzrechts dar, insbesondere bei den Landeskrankenhausgesetzen und den Krebsregistergesetzen. Die in diesen Gesetzen enthaltenen Übermittlungsregeln sind auf die Kollision mit der ärztlichen Schweigepflicht zugeschnitten und können deshalb im Rahmen des § 203 StGB als Rechtsfertigungsgründe herangezogen werden.“

6.2 „Berufliche Tätigkeit" des Berufsgeheimnisträgers und „mitwirkende Personen"

Das fremde Geheimnis muss dem Geheimnisträger in seiner beruflichen Tätigkeit anvertraut oder sonst bekannt geworden sein. Zudem ist fraglich, was unter dem Begriff der „mitwirkenden Personen" zu verstehen ist, den der § 203 StGB neu einführt.

6.2.1 „Berufliche Tätigkeit"

Das Tatobjekt des fremden Geheimnisses muss in beruflicher Eigenschaft erlangt worden sein – „sei es als Zweck oder Nebenfolge seiner Aufgabenerfüllung".[456] Hier differenziert § 203 StGB zwischen dem anvertrauten und dem sonst bekannt gewordenen fremden Geheimnis. Unter Anvertrauen wird „das Einweihen in ein Geheimnis unter ausdrücklicher Auflage des Geheimhaltens oder unter solchen Umständen, aus denen sich eine Verpflichtung zur Verschwiegenheit ergibt"[457] verstanden. Es ist mithin ein Vertrauensakt erforderlich.[458] Erforderlich ist zudem ein innerer Zusammenhang mit der Ausübung seines Berufs. Dies lässt sich aus den Anforderungen an das Wort „als" in § 203 Abs. 1 und 2 StGB ableiten.[459] Ein Vertrag oder eine zivilrechtliche Sonderbeziehung ist nicht erforderlich; das Anvertrauen muss aber „in der Erwartung erfolgen, dass das Mitgeteilte im Sinne der funktionsgerechten Aufgabenstellung des Empfängers genutzt wird".[460]

Auch beim sonst bekannt gewordenen fremden Geheimnis wird ein innerer Zusammenhang zwischen der Aufgabenwahrnehmung des Geheimnisträgers und dem Bekanntwerden verlangt.[461] Es ist jedoch streitig, ob hier ebenso wie beim anvertrauten Geheimnis ein Vertrauensverhältnis erforderlich ist.[462]

Nicht zur beruflichen Tätigkeit des Berufsgeheimnisträgers gehören andersartige Nebentätigkeiten. Was konkret zur beruflichen Tätigkeit gehört, soll sich „aus dem beruflichen Rollenbild des Täters ergeben". Berufsfremd sind damit Tätigkeiten, „die überwiegend von anderen Personen professionell wahrgenommen werden."[463] Nicht erfasst ist beispielsweise die Tätigkeit eines Arztes, der als Pharmareferent tätig wird.[464]

456 *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 23.
457 *Weidemann*, in: BeckOK StGB, § 203 Rn. 12.
458 *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 48.
459 *Lenckner/Eisele*, in: Schönke/Schröder, § 203 Rn. 13; *Tag*, in: Dölling/Duttge/König/Rössner, § 203 StGB, Rn. 40; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 13f.; *Heger*, in: Lackner/Kühl, § 203 Rn. 16.
460 *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 14.
461 *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 15.
462 Zum Streit s. *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 16.
463 *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 13.
464 So *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 23.

6.2.2 „Mitwirkende Personen“

Der Begriff der „mitwirkenden Person“ wird mit der Novelle des § 203 StGB neu in das Strafgesetzbuch eingeführt. Er ist ein Überbegriff und umfasst einerseits den berufsmäßig tätigen Gehilfen und die beim Berufsgeheimnisträger zur Vorbereitung auf den Beruf tätigen Personen und andererseits die sonstigen mitwirkenden Personen.[465]

6.2.2.1 Berufsmäßig tätige Gehilfen

Mit der Novelle des § 203 StGB ist der Streit um die Auslegung des Gehilfenbegriffs bezogen auf externe Personen, die nicht in die Organisation des Berufsgeheimnisträgers eingebunden sind, entschieden: Diese unterfallen nicht dem Gehilfenbegriff. So heißt es in der Gesetzesbegründung: Berufsmäßig tätiger Gehilfe ist, „wer innerhalb des beruflichen Wirkungsbereichs des Berufsgeheimnisträgers eine auf dessen berufliche Tätigkeit bezogene unterstützende Tätigkeit ausübt, welche die Kenntnis bzw. die Möglichkeit der Kenntnisnahme fremder Geheimnisse mit sich bringt“.[466]

Die Auslegung des Gehilfenbegriffs bezogen auf interne Personen war aber ebenfalls umstritten. Nach enger Auslegung sollte beispielsweise auch internes EDV-Personal nicht zu den berufsmäßigen Gehilfen zählen, da anders als etwa bei der Krankenschwester hier kein innerer Zusammenhang zur Tätigkeit des Berufsgeheimnisträgers bestünde.[467] Nach anderer Auffassung ist dies aber der Fall.[468] Der Streit ist auch nach der Novelle des § 203 StGB relevant, da er bestimmt, wann die Bevorzugung des § 203 Abs. 3 Satz 1 StGB n.F. greift und wann auf § 203 Abs. 3 Satz 2 StGB n.F. abzustellen ist. Konsens besteht bei der Notwendigkeit eines inneren Zusammenhangs[469] zwischen der Arbeit des Gehilfen und der „eigentlichen Berufsausübung“[470] des Geheimnisträgers. Reinigungskräfte, Fahrer und ähnliche Mitarbeiter werden deshalb übereinstimmend nicht als berufsmäßig tätige Gehilfen gewertet. Hier werden lediglich die „äußeren Bedingungen für die fragliche Berufstätigkeit“ geschaffen; „ihre eigentliche Aufgabe ist inhaltlich nicht hinreichend durch das Arbeitsgebiet

465 S. BT-Drs. 18/11936, 21.

466 BT-Drs. 18/11936, 18, 22.

467 So *Altenhain*, in: Matt/Renzikowski, § 203 Rn. 11; *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 54, wonach etwa die Krankenhausverwaltung außenstehender Dritter sein soll. Angehörige des „technischen Personals“ sollen grundsätzlich ausgeschlossen sein; *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 124.

468 So zählt etwa *Tag*, in: Dölling/Duttge/König/Rössner, § 203 StGB, Rn. 19 den EDV-Support durchaus zu den berufsmäßig tätigen Gehilfen. Gleiches gilt bei *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 38 für „organisatorisch eingebundene EDV-Betreuer“; s. auch *Weidemann*, in: BeckOK StGB, § 203 Rn. 27. S. auch *BGH*, NJW 1995, 2419 (2420) zum Rechenzentrum eines Krankenhauses.

469 S. aber auch *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 123, die von einem „unmittelbaren Zusammenhang“ sprechen. *Weidemann*, in: BeckOK StGB, § 203 Rn. 27 fordert neben dem inneren Zusammenhang eine mit der Kenntnisnahme von Geheimnissen verbundene Tätigkeit.

470 *Heger*, in: Lackner/Kühl, § 203 Rn. 11b.

der betreffenden Einrichtung geprägt".[471] Ob die Tätigkeit ehrenamtlich oder tatsächlich berufsmäßig ausgeübt wird, soll trotz des Wortlauts keine Rolle spielen.[472] Gefordert wird aber eine organisatorische Anbindung.[473] Dies stellt auch die Gesetzesbegründung klar, wonach „der Gehilfe nicht selbst seinen Beruf ausüben muss".[474]

Die Gesetzesbegründung enthält einen Beispielkatalog von „mitwirkenden Tätigkeiten". Darunter fallen neben Schreibarbeiten und Rechnungswesen auch IT-bezogene Tätigkeiten wie „Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art" sowie die „Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten".[475] Damit dürfte der Streit um die Reichweite des Gehilfenbegriffs bei Personen innerhalb der Sphäre des Berufsgeheimnisträgers in dem Sinn entschieden sein, dass auch interne EDV-Mitarbeiter als Gehilfen zu qualifizieren sind. Dies folgt aus der Tatsache, dass die mitwirkende Person Oberbegriff für den Gehilfen ist. Plausibler ist für die Zukunft also ein (intern) weiter Gehilfenbegriff, dem auch (internes) technisches Personal, Verwaltungsmitarbeiter und Schreibkräfte unterfallen. Ausreichend ist eine Einbindung „in irgendeiner Weise".[476] Reinigungskräfte und Fahrer bleiben aber wohl weiter ausgeschlossen; sie sind nicht „in die Organisation der fraglichen Berufspraxis selbst"[477] eingebunden.

6.2.2.2 Sonstige mitwirkende Personen

Die sonstige mitwirkende Person muss an der beruflichen oder dienstlichen Tätigkeit des Berufsgeheimnisträgers mitwirken.[478] Die Gesetzesbegründung definiert die sonstigen mitwirkenden Personen als solche, „die zwar an der beruflichen oder dienstlichen Tätigkeit der schweigepflichtigen Person mitwirken, also in diese Tätigkeit in irgendeiner Weise eingebunden werden und Beiträge dazu leisten, allerdings ohne in die Sphäre des Berufsgeheimnisträgers eingegliedert zu sein".[479] Der wesentliche Unterschied zum Gehilfen ist also die fehlende Teilhabe an der Sphäre des Berufsgeheimnisträgers. Dafür, wann eine Mitwirkung an der beruflichen oder dienstlichen Tätigkeit des Berufsgeheimnisträgers vorliegt, gibt auch hier der Beispielkatalog in der Geset-

471 *Kargl*, in: Kindhäuser/Neumann/Paeffgen, § 203 Rn. 38; s. auch *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 124; *Weidemann*, in: BeckOK StGB, § 203 Rn. 27.
472 So *Weidemann*, in: BeckOK StGB, § 203 Rn. 27.1; a.A. *Cierniak/Niehaus*, in: MüKo StGB, § 203 Rn. 123; *Heger*, in: Lackner/Kühl, § 203 Rn. 11b.
473 *Heger*, in: Lackner/Kühl, § 203 Rn. 11b.
474 BT-Drs. 18/11936, 21.
475 BT-Drs. 18/11936, 22.
476 BT-Drs. 18/11936, 18, 22.
477 BT-Drs. 18/11936, 18.
478 So der Wortlaut von § 203 Abs. 3 Satz 2 Hs. 1 StGB.
479 BT-Drs. 18/11936, 22.

zesbegründung Anhaltspunkte. Ein externes Schreibbüro kann somit ebenso mitwirkende Person sein wie ein Cloud-Anbieter.

Bezüglich der Grundlage der Mitwirkung heißt es in der Gesetzesbegründung, man wolle „keinen möglichen Rechtsgrund, auf dem eine sonstige Mitwirkung beruhen kann, ausschließen“.[480] Notwendig sind lediglich die Einbindung in die berufliche Tätigkeit und das Einvernehmen mit der schweigepflichtigen Person.

6.3 Forschungstätigkeit eines Arztes als „berufliche Tätigkeit“

Fraglich ist nun einerseits, ob die Forschungstätigkeit des Arztes als berufliche Tätigkeit zu werten ist, und andererseits, ob die Mitwirkung an der Forschungstätigkeit eines Arztes als Mitwirkungshandlung im Sinn des § 203 StGB n.F. verstanden werden kann.

Nach § 1 MBO dienen Ärzte der Gesundheit des einzelnen Menschen und der Bevölkerung.[481] Ihre Aufgabe 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“.

§ 15 Abs. 1 Satz 1 MBO enthält Vorgaben unter anderem für Ärzte, die Forschung mit personenbezogenen Daten durchführen.[482] Dass die Musterberufsordnung in § 15 überhaupt Regelungen für die ärztliche Forschung enthält, darf bereits als starkes Indiz dafür gelten, dass die Forschungstätigkeit des Arztes als berufliche Tätigkeit zu werten ist.

6.3.1 Der Arzt im Universitätskrankenhaus

Das Bundesverfassungsgericht hat festgestellt, dass die Krankenversorgung eine der Universität vom Staat zusätzlich übertragene Aufgabe darstellt: „Ihre Übertragung auf die Universität ist zwar durch die medizinische Forschung und Lehre begründet und bedingt; sie stellt jedoch eine Zusatzaufgabe dar, die in beträchtlichem Maße über den rein wissenschaftlichen Bereich hinausgeht.“[483] Das bedeutet, dass bei Hochschullehrern, die Kranke an Universitätskliniken behandeln, diese Aufgabe neben diejenige tritt, Forschung und Lehre zu betreiben.[484] Die Verpflichtung zu Forschung und Lehre ergibt sich aus

480 BT-Drs. 18/11936, 22f.; s. auch *Pohle/Ghaffari*, CR 2017, 489 (492).
481 So auch § 1 Abs. 1 BÄO.
482 § 15 Abs. 1 Satz 1 MBO: „Ärztinnen und Ärzte, die sich an einem Forschungsvorhaben beteiligen, bei dem … Daten verwendet werden, die sich einem bestimmten Menschen zuordnen lassen …“.
483 *BVerfG*, NJW 1981, 1995 (1996).
484 *Lambrecht/Vollmöller*, in: Huster/Kaltenborn, § 16 Rn. 85.

dem Landeshochschulrecht, z.B. aus § 22 Abs. 2 Satz 2 des Gesetzes für die hessischen Universitätskliniken.

Die wissenschaftliche Forschung gehört damit unzweifelhaft zur beruflichen Tätigkeit des Arztes im Universitätskrankenhaus.

6.3.2 Der Arzt im sonstigen Krankenhaus

Der Arzt im sonstigen Krankenhaus ist zur Forschung nicht verpflichtet. Die Nutzung der im Krankenhaus anfallenden Patientendaten für Forschungszwecke wird durch die Landeskrankenhausgesetze aber ausdrücklich gestattet.[485] Auch die Übermittlung an externe Stellen ist in den Landeskrankenhausgesetzen geregelt und in der Regel an eine Einwilligung des Patienten geknüpft.[486] Bezogen auf psychisch kranke Personen enthält das Landesrecht entsprechende Regelungen.[487]

Die Forschung des Arztes im sonstigen Krankenhaus ist Teil seiner beruflichen Tätigkeit. Dabei ist es unerheblich, ob die Forschungstätigkeit vom Arbeitgeber angeordnet wurde oder fakultativ erfolgt. Entscheidend ist nur, dass der Arzt „als Arzt" forscht. Dabei ist zu beachten, dass der Arzt Arzt bleibt, „auch wenn er seinen Beruf nicht als selbstständig praktizierender Arzt oder in einem herkömmlichen Dienstverhältnis, sondern in spezieller Funktion und Rechtsposition ausübt".[488] Nicht als Teil der beruflichen Tätigkeit kann lediglich Forschung gelten, die eine andersartige Nebentätigkeit darstellt. Davon dürfte bezogen auf wissenschaftliche Forschung nur auszugehen sein, wenn der Arzt nicht im medizinischen Kontext, also letztlich fachfremd forscht. Ob der Arzt parallel zur Forschungstätigkeit auch im Sinn von § 1 MBO tätig wird, ist unerheblich. Keine fachfremde Forschung liegt vor, wenn der Arzt als Teil eines Forschungsverbundes seine medizinische Expertise in ein Forschungsvorhaben einbringt, dieses Forschungsvorhaben aber seinen fachlichen Schwerpunkt außerhalb der Medizin hat.

6.3.3 Der Arzt in der Arztpraxis

Auch niedergelassene Ärzte sind wie der Arzt im sonstigen Krankenhaus nicht zur Forschung verpflichtet. Dass die Forschungstätigkeit auch des Arztes in der Arztpraxis zu seiner beruflichen Tätigkeit gehört, ergibt sich implizit einerseits aus der Tatsache, dass die Verarbeitung personenbezogener Daten in der Forschung dem Gebot der ärztlichen Schweigepflicht unter-

485 S. beispielhaft § 14 Abs. 1 Saarländisches Krankenhausgesetz; § 25 Abs. 1 Satz 1 Landeskrankenhausgesetz Berlin.
486 S. z.B. *Jandt/Roßnagel*, MedR 2013, 17ff.
487 S. beispielhaft § 35 Landesgesetz für psychisch kranke Personen Rheinland-Pfalz.
488 *Schelling*, in: Spickhoff, § 1 BÄO, Rn. 7.

liegt,[489] andererseits aus § 15 MBO. Auch hier ist entscheidend, dass der Arzt „als Arzt“ forscht.[490]

Voraussetzung ist dabei, dass die Forschungstätigkeit fachlich dem Arztberuf zugeordnet werden kann. Ein Indiz, dass dies nicht so ist, ist etwa, dass die fragliche Tätigkeit klassisch einer anderen Berufsgruppe zugeordnet wird. Aufgrund möglicher Überschneidungen ist jedoch stets eine Betrachtung des konkreten Einzelfalls erforderlich. In jedem Fall ist ein Konnex zum Themenkreis „Medizin“ erforderlich. Sofern die Forschungstätigkeit einen Bezug zu den in § 1 MBO genannten Aufgaben des Arztes hat, darf dieser als gegeben gelten.

6.3.4 Forschung als ärztliche Tätigkeit

Für die Anerkennung von Forschung als ärztlicher Tätigkeit gibt es im Ergebnis keine Unterschiede zwischen der Arbeit eines Arztes in einem Universitätskrankenhaus, in einem sonstigen Krankenhaus und in einer Arztpraxis. In allen Fällen ist die Forschungstätigkeit des Arztes seiner beruflichen Tätigkeit zuzurechnen und deshalb tatbestandlich im Sinn von § 203 StGB. Entscheidend ist in allen Fällen, dass der forschende Arzt „als Arzt“ tätig wird. Für diese Beurteilung kann als Richtschnur § 1 MBO dienen. In allen Fällen erfährt der Arzt ebenso wie bei der Heilbehandlung geheimhaltungsbedürftige Informationen über den Patienten und muss diese Geheimnisse bewahren. Wäre dem nicht so, entstünde zudem eine Schutzlücke bezogen auf den Schutz von Patientendaten, die so nicht gewollt sein kann.

6.4 Mitwirkung an der Forschungstätigkeit

Die Mitwirkung an der Forschungstätigkeit eines Arztes ist mithin eine Mitwirkungshandlung im Sinn von § 203 StGB.[491]

Die Mitwirkung an der Forschungstätigkeit des Arztes ist breit zu verstehen und beinhaltet beispielsweise auch die Auswertung von Datenmassen in externen Rechenzentren. Notwendig ist stets der innere Bezug der Tätigkeit der mitwirkenden Person und der Forschungstätigkeit des Arztes. Zudem muss es für die Tätigkeit der mitwirkenden Person erforderlich sein, dass diese das Geheimnis zur Kenntnis nimmt oder zumindest die Möglichkeit zur Kenntnisnahme erhält.

489 Bekanntgabe der Bundesärztekammer, DÄBl 1989, A-2843 (A-2844).

490 Ansonsten gelten die Ausführungen in Kap. 6.3.2.

491 A.A. wohl *Hilgendorf* 2004, 93, der einen engen Bezug zur Heiltätigkeit fordert. Nach dieser Ansicht wäre die Forschungstätigkeit des Arztes grundsätzlich keine berufliche Tätigkeit im Sinn von § 203 StGB, da „sich das Vertrauen des Patienten in erster Linie auf die Heiltätigkeit“ beziehe.

Liegen diese Voraussetzungen vor, so unterliegt die mitwirkende Person selbst der Strafbarkeit nach § 203 StGB. Besteht bereits aufgrund eines Gesetzes eine förmliche Verpflichtung einer Person auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben, so ist die Person zudem direkt über § 203 Abs. 2 Satz 1 Nr. 6 StGB strafbar. Derartige gesetzliche Verpflichtungen finden sich beispielsweise in § 476 und 487 Abs. 4 StPO, aber auch in § 16 Abs. 7 BStatG.

6.5 Ergebnis zur Weitergabe von Informationen an „mitwirkende Personen“

Strafbar macht sich nach § 203 StGB, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Berufsgeheimnisträger im Sinne von Abs. 1 und 2 anvertraut worden oder sonst bekannt geworden ist. Hinsichtlich der Strafbarkeit der Offenbarung von Geheimnissen gegenüber externen Fachkräften, die Ärzte in ihrer medizinischen Tätigkeit unterstützten, bestand aufgrund zahlreicher Meinungsverschiedenheiten in der strafrechtlichen Fachliteratur und fehlender obergerichtlicher Rechtsprechung eine große Rechtsunsicherheit. Die Änderung des § 203 StGB 2017 soll hierzu Rechtsklarheit bringen.

Mit der Novelle des § 203 StGB wird der Begriff der „mitwirkenden Person“ neu in das Strafgesetzbuch eingeführt. Er ist ein Überbegriff und umfasst einerseits den berufsmäßig tätigen Gehilfen und andererseits die sonstigen mitwirkenden Personen. Wesentliches Unterscheidungsmerkmal zwischen dem Gehilfen und der sonstigen mitwirkenden Person ist dabei die fehlende Einbindung in die Sphäre des Berufsgeheimnisträgers. Eine Offenbarung gegenüber mitwirkenden Personen ist nicht strafbar, wenn die Mitwirkung im Rahmen der Berufstätigkeit des Arztes erfolgt.

Die Forschungstätigkeit des Arztes ist als berufliche Tätigkeit im Sinn von § 203 StGB zu werten. Entscheidend ist dabei, dass der Arzt „als Arzt“ forscht. Unterschiede zwischen der ärztlichen Tätigkeit in einem Universitätskrankenhaus, einem sonstigen Krankenhaus und einer Arztpraxis bestehen im Ergebnis nicht. In allen Fällen ist die Forschungstätigkeit des Arztes seiner beruflichen Tätigkeit zuzurechnen und deshalb tatbestandlich im Sinn von § 203 StGB. Nicht als Teil der beruflichen Tätigkeit kann lediglich Forschung gelten, die eine andersartige Nebentätigkeit darstellt. Davon dürfte nur auszugehen sein, wenn der Arzt nicht im medizinischen Kontext forscht. Damit ist die Mitwirkung an der Forschungstätigkeit eines Arztes eine Mitwirkungshandlung im Sinn von § 203 Abs. 3 StGB. Eine Offenbarung von Geheimnissen gegenüber der mitwirkenden Person ist nicht strafbar. Die mitwirkende Person unterliegt allerdings selbst dem Straftatbestand des § 203 StGB.

Literatur

Albrecht, Jan Philipp/Jotzo, Florian: Das neue Datenschutzrecht der EU, Nomos: Baden-Baden 2017.

Arning, Marian A./Forgó, Nikolaus/Krügel, T.: Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DuD 2006, 700.

Art. 29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136.

Art. 29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216.

Behling, Thorsten B./Borges, Georg u.a.: Schweigepflicht bei der Auslagerung von IT-Dienstleistungen, Kompetenzzentrum Trusted Cloud, Thesenpapier Nr. 7, Februar 2015 (zit.: Behling u.a. 2015).

Bergt, Matthias: Die Bestimmbarkeit als Grundproblem des Datenschutzrechts. Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365.

Boehme-Neßler, Volker: Das Ende der Anonymität, DuD 2016, 419.

Breyer, Patrick: Personenbezug von IP-Adressen, ZD 2014, 400.

Brink, Stefan/Eckardt, Jens: Wann ist ein Datum ein personenbezogenes Datum?, Anwendungsbereich des Datenschutzrechts, ZD 2015, 205.

Buchner, Benedikt: Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155.

Buchner, Benedikt/Kühling, Jürgen: Die Einwilligung in der Datenschutzordnung 2018, DuD 2017, 544.

Calliess, Christian/Ruffert, Matthias (Hrsg.): EUV/AEUV, Kommentar, 5. Aufl., C.H. Beck: München 2016 (zit.: Autor, in: Calliess/Ruffert).

Caspar, Johannes: Geoinformationen und Datenschutz am Beispiel des Internetdienstes Google Street View, DÖV 2009, 965.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz – Kompakt-Kommentar zum BDSG, 4. Auflage, Bund: Frankfurt a.M. 2014 (zit.: Autor, in: Däubler u.a.).

Danwitz, Thomas von: Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, DuD 2015, 581.

Dölling, Dieter/Duttge, Gunnar/König, Stefan/Rössner, Dieter (Hrsg.): Gesamtes Strafrecht, Kommentar, 4. Aufl., Nomos: Baden-Baden 2017 (zit.: Autor, in: Dölling/Duttge/König/Rössner).

Düsseldorfer Kreis: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009 in Stralsund in Bezug auf IP-Adressen.

Eckhardt, Jens: IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer, CR 2011, 339.

Eckhardt, Jens: Anmerkung zu BGH vom 28.10.2014, CR 2015, 109, CR 2015, 113.

Ehmann, Eugen/Helfrich, Marcus: EG-Datenschutzrichtlinie, Kurzkommentar, Otto Schmidt Verlag: Köln 1999.

Ehmann, Eugen/Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung, Kommentar, C.H. Beck: München 2017 (zit.: Autor, in: Ehmann/Selmayr).

Ernst, Stefan: Die Einwilligung nach der Datenschutz-Grundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO, ZD 2017, 110.

Geminn, Christian L.: Demokratie zwischen Öffentlichkeit und Privatheit, Verw-Arch 2016, 601–630.

Geminn, Christian L.: Risikoadäquate Regelungen für das Internet der Dienste und Dinge?, DuD 2017, 295.

Geminn, Christian L./Roßnagel, Alexander: „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick, JZ 2015, 703.

Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, Kommentar, C.H. Beck: München 2017 (zit.: Autor, in: Gola)

Gola, Peter/Schomerus, Rudolf: Bundesdatenschutzgesetz, Kommentar, 12. Aufl., C.H. Beck: München 2015.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin M. (Hrsg.): Das Recht der Europäischen Union, Band I EUV/AEUV, Kommentar, Loseblatt, Beck: München 2017 (zit.: Autor, in: Grabitz/Hilf/Nettesheim)

Haase, Martin S.: Datenschutzrechtliche Fragen des Personenbezugs – Eine Untersuchung des sachlichen Anwendungsbereiches des deutschen Datenschutzrechts und seiner europarechtlichen Bezüge, Mohr Siebeck: Tübingen 2015.

Hänlein, Andreas/Schuler, Rolf: Lehr- und Praxiskommentar Sozialgesetzbuch V, Nomos, 5. Aufl., Baden-Baden 2016 (zit.: Autor, in: Hänlein/Schuler).

Härting, Nico: Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065.

Hartung, Jürgen: Datenschutz und Verschwiegenheit bei Auslagerungen durch Versicherungsunternehmen, VersR 2012, 400.

von Heintschel-Heinegg, Bernd (Hrsg.): Beck'scher Online-Kommentar StGB, 37. Edition, C.H. Beck: München 2018 (zit.: Autor, in: BeckOK StGB).

Herbst, Tobias: Rechtliche und ethische Probleme des Umgangs mit Proben und Daten bei großen Biobanken, DuD 2016, 371.

Herbst, Tobias: Was sind personenbezogene Daten?, NVwZ 2016, 902.

Hilgendorf, Eric: Strafrechtliche Probleme beim Outsourcing von Versicherungsdaten, in: Hilgendorf, Eric (Hrsg.), Informationsstrafrecht und Rechtsinformatik, Logos: Berlin 2004.

Hömig, Dieter/Wolff, Heinrich A. (Hrsg.): Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 11. Aufl., Nomos: Baden-Baden 2016 (zit.: Autor, in: Hömig/Wolff).

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblatt, C.H. Beck: München (zit. Autor, in: Hoeren/Sieber/Holznagel).

Hofmann, Johanna M./Johannes, Paul C.: DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs, ZD 2017, 221.

Hornung, Gerrit: Der Personenbezug biometrischer Daten, DuD 2004, 429.

Hornung, Gerrit/Hofmann, Kai: Die Auswirkungen der europäischen Datenschutzreform auf die Markt- und Meinungsforschung, ZD-Beilage 4/2017, 1.

Huster, Stefan/Kaltenborn, Markus (Hrsg.): Krankenhausrecht, 2. Aufl., C.H. Beck: München 2017 (zit.: Autor, in: Huster/Kaltenborn).

Jandt, Silke/Roßnagel, Alexander: Qualitätssicherung im Krankenhaus, MedR 2011, 140.

Jandt, Silke/Roßnagel, Alexander: Factoring von Forderungen aus Behandlungsverträgen der Krankenhäuser – datenschutzrechtlich zulässig?, MedR 2013, 17–23.

Jandt, Silke/Roßnagel, Alexander/Wilke, Daniel: Krankenhausinformationssysteme im Gesundheitskonzern, RDV 2011, 222.

Jandt, Silke/Roßnagel, Alexander/Wilke, Daniel: Outsourcing im Medizinbereich, NSR 2011, 641.

Jarass, Hans D.: Charta der Grundrechte der Union, 3. Aufl., C.H. Beck: München 2016.

Jauernig, Othmar (Begr.): Bürgerliches Gesetzbuch, Kommentar, 16. Aufl., C.H. Beck: München 2015 (zit.: Autor, in: Jauernig).

Joecks, Wolfgang/Miebach, Klaus (Hrsg.): Münchener Kommentar zum StGB, Bd. 4, 3. Aufl., C.H. Beck: München 2017 (zit.: Autor, in: MüKo StGB).

Johannes, Paul C./Richter, Philipp: Privilegierte Verarbeitung im BDSG-E, DuD 2017, 300.

Karg, Moritz: Die Rechtsfigur des personenbezogenen Datums – ein Anachronismus des Datenschutzes?, ZD 2012, 255.

Karg, Moritz: Anonymität, Pseudonymisierung und Personenbezug revisited?, DuD 2015, 520.

Kartheuser, Ingemar/Gilsdorf, Friedrich: EuGH: Dynamische IP-Adressen können personenbezogene Daten sein, MMR-Aktuell 2016, 382533

Kilian, Wolfgang: Medizinische Forschung und Datenschutzrecht, NJW 1998, 787–791.

Kindhäuser, Urs/Neumann, Ulfried/Paeffgen, Hans-Ullrich (Hrsg.): Strafgesetzbuch, Kommentar, 5. Aufl., Nomos: Baden-Baden 2017 (zit.: Autor, in: Kindhäuser/Neumann/Paeffgen).

Klar, Manuel: Datenschutzrecht und die Visualisierungen des öffentlichen Raums, Lit: Münster 2012.

Knopp, Michael: Pseudonym – Grauzone zwischen Anonymisierung und Personenbezug, DuD 2015, 527.

Kroschwald, Steffen: Informationelle Selbstbestimmung in der Cloud, Springer: Berlin u.a. 2015.

Krügel, Tina: Das personenbezogene Datum nach der DS-GVO – Mehr Klarheit und Rechtssicherheit, ZD 2017, 455.

Krüger, Stefan/Maucher, Svenja-Ariane: Ist die IP-Adresse wirklich ein personenbezogenes Datum? – Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, 433.

Kühling, Jürgen/Buchner, Benedikt: Datenschutz-Grundverordnung, Kommentar, 2. Aufl. C.H. Beck: München 2018 (zit.: Autor, in: Kühling/Buchner).

Kühling, Jürgen/Klar, Manuel: Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611.

Kühling, Jürgen/Klar, Manuel: Anmerkung zu EuGH, Urt. v. 19.10.2016, C-582/14, ZD 2017, 24, ZD 2017, 27.

Kühling, Jürgen/Martini, Mario u.a.: Die Datenschutz-Grundverordnung und das nationale Recht, Verlagshaus Monsenstein und Vannerdat: Münster 2016.

Lackner, Karl/Kühl, Kristian (Hrsg.): Strafgesetzbuch, Kommentar, 28. Aufl., C.H. Beck: München 2014 (zit.: Autor, in: Lackner/Kühl).

Laue, Philip/Nink, Judith/Kremer, Sacha: Das neue Datenschutzrecht in der betrieblichen Praxis, Nomos: Baden-Baden 2016.

Marnau, Ninja: Anonymisierung, Pseudonymisierung und Transparenz für Big Data, DuD 2016, 428.

Masing, Johannes: Herausforderungen des Datenschutzes, NJW 2012, 2305.

Matt, Holger/Renzikowski, Joachim (Hrsg.): Strafgesetzbuch, Kommentar, Vahlen: München 2013 (zit.: Autor, in: Matt/Renzikowski).

Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz, Loseblatt, C.H. Beck: München 2016 (zit.: Autor, in: Maunz/Dürig).

Meyer, Jürgen (Hrsg.): Charta der Grundrechte der Europäischen Union, Kommentar, 4. Aufl., Nomos: Baden-Baden 2014 (zit.: Autor, in: Meyer).

Meyerdierks, Per: Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8.

Moos, Flemming/Rothkegel, Tobias: Anmerkung zu EuGH, Urt. v. 19.10.2016, C-582/14, MMR 2016, 842, MMR 2016, 845.

Nink, Judith/Pohle, Jan: Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze, MMR 2015, 563.

Paal, Boris P./Pauly, Daniel (Hrsg.): Datenschutz-Grundverordnung, Kommentar, 2. Aufl., C.H. Beck: München 2018 (zit.: Autor, in: Paal/Pauly).

Pahlen-Brandt, Ingrid: Datenschutz braucht scharfe Instrumente – Beitrag zur Diskussion um „personenbezogene Daten", DuD 2008, 34.

Pahlen-Brandt, Ingrid: Zur Personenbezogenheit von IP-Adressen, K & R 2008, 286.

Plath, Kai-Uwe (Hrsg.): BDSG/DSGVO, Kommentar, 2. Aufl., Dr. Otto Schmidt: Köln 2016 (zit.: Autor, in: Plath).

Pohle, Jan/Ghaffari, Sheila: Die Neufassung des § 203 StGB – der Befreiungsschlag für IT-Outsourcing am Beispiel der Versicherungswirtschaft?!, CR 2017, 489.

Pöttgen, Nicole: Medizinische Forschung und Datenschutz, Peter Lang: Frankfurt am Main 2009.

Preuß, Tamina: Die Strafbarkeit von Berufsgeheimnisträgern nach § 203 StGB beim Cloud Computing, DuD 2016, 802.

Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung C.H. Beck: München 2003 (zit.: Autor, in: Roßnagel 2003).

Roßnagel, Alexander: Datenschutz in einem informatisierten Alltag – Gutachten, Friedrich Ebert Stiftung: Berlin 2007.

Roßnagel, Alexander: Modernisierung des Datenschutzes – Nicht die Definition von Personendaten muss geändert werden, sondern die Anforderungen an ihren Schutz, digma 2011, 160.

Roßnagel, Alexander (Hrsg.): Beck'scher Kommentar zum Recht der Telemediendienste – Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr, C.H. Beck: München 2013 (zit.: Autor, in: Roßnagel 2013).

Roßnagel, Alexander (Hrsg.): Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, Nomos: Baden-Baden 2017 (zit.: Autor, in: Roßnagel 2017).

Roßnagel, Alexander: Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, Springer Verlag, Wiesbaden 2017.

Roßnagel, Alexander: Gesetzgebung im Rahmen der Datenschutz-Grundverordnung – Aufgaben und Spielräume des deutschen Gesetzgebers?, DuD 2017, 277.

Roßnagel, Alexander (Hrsg.): Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Nomos: Baden-Baden 2018 (zit.: Autor, in: Roßnagel 2018).

Roßnagel, Alexander/Banzhaf, Jürgen/Grimm, Rüdiger: Datenschutz im Electronic Commerce, Recht und Wirtschaft: Heidelberg 2003.

Roßnagel, Alexander/Geminn, Christian L./Jandt, Silke/Richter, Philipp: Datenschutzrecht 2016 – „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts, kassel university press, Kassel 2016.

Roßnagel, Alexander/Kroschwald, Steffen: Was wird aus der Datenschutzgrundverordnung? Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, ZD 2014, 495.

Roßnagel, Alexander/Nebel, Maxi: (Verlorene) Selbstbestimmung im Datenmeer – Privatheit im Zeitalter von Big Data, DuD 2015, 455.

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2002.

Roßnagel, Alexander/Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Sachs, Ulrich: Datenschutzrechtliche Bestimmbarkeit von IP-Adressen, CR 2010, 547.

Säcker, Franz J./Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 4, 7. Aufl., C.H. Beck: München 2016 (zit.: Autor, in: MüKo BGB).

Schaar, Katrin: DS-GVO: Geänderte Vorgaben für die Wissenschaft. Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen?, ZD 2016, 224.

Schaar, Peter: Datenschutz im Internet – Die Grundlagen, C.H. Beck: München 2002.

Schaffland, Hans-Jürgen/Wiltfang, Noeme: Bundesdatenschutzgesetz – BDSG – Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Loseblatt, Berlin.

Schantz, Peter: Datenschutz-Grundverordnung, NJW 2016, 1841.

Schantz, Peter/Wolff, Heinrich A.: Das neue Datenschutzrecht – Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, C.H. Beck: München 2017 (zit.: Autor, in: Schantz/Wolff).

Schneider, Uwe K.: Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, Schriftenreihe der TMF Bd. 12, Medizinisch Wissenschaftliche Verlagsgesellschaft: Berlin 2015.

Schönke, Adolf/Schröder, Horst (Hrsg.): Strafgesetzbuch, Kommentar, 29. Aufl., C.H. Beck: München 2014 (zit.: Autor, in: Schönke/Schröder).

Schulze, Reiner (Hrsg.): Bürgerliches Gesetzbuch, Kommentar, 9. Aufl., Nomos: Baden-Baden 2017 (zit.: Autor, in: Schulze).

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, Kommentar, 8. Aufl., Nomos: Baden-Baden 2014 (zit.: Autor, in: Simitis).

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, Nomos, Baden-Baden 2018.

Spickhoff, Andreas (Hrsg.): Medizinrecht, 2. Aufl., C.H. Beck: München 2014 (zit.: Autor, in: Spickhoff).

Stiemerling, Oliver/Hartung, Jürgen: Datenschutz und Verschlüsselung – Wie belastbar ist Verschlüsselung gegenüber dem Anwendungsbereich des Datenschutzrechts?, CR 2012, 60.

Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung, Kommentar, Nomos: Baden-Baden 2017 (zit.: Autor, in: Sydow).

Taeger, Jürgen/Gabel, D. (Hrsg.): Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl., Frankfurt a.M. 2013 (zit.: Autor, in: Taeger/Gabel)

Voigt, Paul: Datenschutz bei Google, MMR 2009, 377.

Weichert, Thilo: Cloud Computing und Datenschutz, DuD 2010, 679.

Wicker, Magda: Cloud Computing und staatlicher Strafanspruch, Nomos: Baden-Baden 2016.

Wolff, Heinrich A./Brink, Stefan (Hrsg.): Datenschutzrecht, Kommentar, 23. Edition, C.H. Beck: München 2018 (zit.: Autor, in: Wolff/Brink).

Wronka, Georg: Datenschutzrechtliche Aspekte des „neuen" § 203 StGB, RDV 2017, 129.

Ziebarth, Wolfgang: Automatisierte Erfassung und Verarbeitung von Kfz-Kennzeichen zu Fahndungszwecken, CR 2015; 687.

III

Anhang

Auszug aus dem Pflichtenheft zum Rechtsgutachten zur Nutzung von Sozial- und Gesundheitsdaten im SAHRA-Projekt – in Auftrag gegeben durch TMF e.V.

Version 1.0

1 Einleitung

Die Vergabe des zu erstellenden Rechtsgutachtens zur „Nutzung von Sozial- und Gesundheitsdaten“ erfolgt im Rahmen des vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Smart-Data-Projekts Smart Analysis – Health Research Access (SAHRA). Hauptziel des SAHRA-Projekts ist es, Sozialdaten der AOK Nordost über eine hochsichere webbasierte Datenplattform (SAHRA-Plattform) mit weiteren Datenquellen des Gesundheitswesens zu verbinden. Die Datenplattform soll datenschutzkonforme Möglichkeiten bieten, Abrechnungs-, Behandlungs-, Struktur- sowie Register- und/oder Studiendaten aus verschiedenen Quellen zu kombinieren, zu referenzieren und zu validieren. Die potenziellen Nutzer der SAHRA-Plattform sollen aus der Wissenschaft, der Versorgung und der Industrie stammen.

2 Fragenkatalog

Beschreibung von drei verschiedenen Szenarien:

1. Die Datennutzung geschieht im Rahmen eines Kooperationsprojekts einer gesetzlichen Krankenversicherung mit einer externen Einrichtung. Die Fragestellung für die Datenauswertung wird gemeinsam entwickelt oder von der externen Einrichtung vorgegeben. Die Sozialdaten bleiben in der Einrichtung der gesetzlichen Krankenversicherung und werden hier ausgewertet. Lediglich anonyme Auswertungsergebnisse werden an den externen Partner übermittelt, es verlassen keine Sozialdaten die Einrichtung der gesetzlichen Krankenversicherung.
2. Auch hier kooperieren eine gesetzliche Krankenversicherung und eine externe Einrichtung. Die Sozialdaten werden für ein bestimmtes Vorhaben an die externe Einrichtung übermittelt, die diese im Sinne des Vorhabens verarbeitet und auswertet.
3. In diesem Szenario werden Sozialdaten von einer oder mehreren Einrichtungen der gesetzlichen Krankenversicherung zu übergeordneten Zwecken (z.B. medizinische Forschung oder übergeordnete Qualitätssicherungsaspekte) an eine externe Einrichtung (Datenplattform) übermittelt. Die externe Einrichtung wiederum stellt diese Sozialdaten für bestimmte Vorhaben Dritten zur Verfügung, entweder in Form einer weiteren Übermittlung oder indem anonyme Auswertungsergebnisse zu konkreten Fragestellungen herausgegeben werden.

I Bewertung der aktuellen Rechtslage nach Sozialgesetzbuch (SGB) I –X und weiterer heranzuziehender Gesetze[1]

Bitte beantworten Sie zu jedem Szenario folgende Fragen: Beschreiben Sie, auf welcher Rechtsgrundlage das jeweilige Szenario umgesetzt werden kann. Wenn eine uneingeschränkte Umsetzung auf Basis der aktuellen Rechtslage nicht möglich erscheint, gehen Sie bitte auf die bestehenden Einschränkungen ein. Berücksichtigen Sie bei der Einschätzung auch jeweils die folgenden Aspekte:

I.I Bitte beschreiben Sie, zu welchen Zwecken (wissenschaftliche Forschung, Planung im Sozialleistungsbereich, Qualitätssicherung) jedes Szenario umgesetzt werden darf?

I.II Bitte gehen Sie für jedes Vorhaben auf die Frage ein, ob eine Einwilligung der betroffenen Personen nach SGB X oder anderen Gesetzen einzuholen ist. Legen Sie die wichtigsten Punkte dar die die Einwilligungserklärung erfassen muss. Bitte führen Sie aus, in welchen Fällen, die Einholung von Einwilligungen für die Datennutzung entbehrlich ist. Gehen Sie bitte auch auf die Frage ein, ob bei Vorliegen einer Einwilligung die Herausgabe der Sozialdaten von der gesetzlichen Krankenversicherung verweigert werden kann.

I.III Bitte legen Sie dar, welche Anforderungen hinsichtlich Trägerschaft und Rechtsform an die externe Einrichtung nach Szenario 2 und 3 zu stellen sind.

I.IV Gehen Sie bitte auf die Frage ein, ob eine datenschutzrechtliche Genehmigung für das jeweilige Szenario erforderlich ist, welche Genehmigungsunterlagen vorzulegen wären und welche datenschutzrechtliche Aufsicht zuständig ist.

I.V Bitte gehen Sie bei jedem Szenario auf die Frage ein, ob und ggf. unter welchen Voraussetzungen dieses mit direkt personenbeziehbaren, pseudonymen oder anonymen Daten durchgeführt werden kann und welche technisch-organisatorischen Maßnahmen grundsätzlich für den Schutz der betroffenen Personen zu ergreifen sind.

I.VI Unter welchen Bedingungen können die Sozialdaten für Auswertungen in den Szenarien 2 und 3 auch mit weiteren Patientendaten – z.B. aus der ambulanten oder stationären Versorgung bzw. aus Studien oder Registern – personenbezogen zusammengeführt werden? Beschreiben Sie lediglich die sozialrechtlichen Voraussetzungen und Einschränkungen. Die Voraussetzungen und Einschränkungen für

1 Der Fragenkatalog wurde noch vor dem 25.5.2018 entwickelt und abgestimmt, sodass sich der Begriff der „aktuellen Rechtslage" auf den Zeitraum vor der Anwendbarkeit der DSGVO und entsprechender nationaler Gesetze bezieht. In dem Gutachtenteil von Prof. Dierks, der sich auf die hier wiedergegebenen Abschnitte I bis III bezieht, wurde aufgrund der besseren späteren Lesbarkeit der Bezugsrahmen der Abschnitte I und II umgedreht, so dass die Fragen im Abschnitt I vor dem Hintergrund der neuen Rechtslage und die Fragen im Abschnitt II vor dem Hintergrund der Rechtslage vor dem 25.5.2018 beantwortet wurden.

die Daten, die mit den Sozialdaten zusammengeführt werden, sind hier nicht zu berücksichtigen. Gehen Sie bitte auch auf die Frage ein, ob und in welcher Weise eine Zusammenführung der Daten mithilfe eines Treuhänders bzw. einer Vertrauensstelle zu einer anderen rechtlichen Bewertung führt. Bitte prüfen Sie auch, ob sich eine sozialrechtlich begründete behördliche Genehmigung auch auf die Rechtmäßigkeit der Verwendung der weiteren Gesundheitsdaten erstreckt.

I.VII Stellen Sie bitte dar, zu welchem Zeitpunkt eine Löschung der für die Vorhaben verwendeten Sozialdaten in den Szenarien vorzunehmen ist. Bitte gehen Sie dabei auch auf die Frage ein, wie lange die Daten zu dem Zweck aufbewahrt werden können, die Nachvollziehbarkeit der Auswertungen abzusichern. Im wissenschaftlichen Umfeld gibt es hierzu Regelungen, wie z.B. in der Denkschrift der Deutschen Forschungsgemeinschaft (DFG) zur Sicherung der guten wissenschaftlichen Praxis, die eine Datenaufbewahrung für 10 Jahre vorschreibt. Bitte prüfen Sie dabei auch, ob die Vorschrift des § 304 SGB V analog/entsprechend auf externe Einrichtungen anzuwenden sein könnte.

I.VIII Stellen Sie bitte dar, unter welchen rechtlichen und technischen Gesichtspunkten ein wirksames Anonymisieren von Sozialdaten einer Löschung der Sozialdaten gleichkommen könnte.

I.IX Bitte prüfen Sie abschließend, welchem Rechtsrahmen die übermittelten Sozialdaten bei den externen Einrichtungen in den Szenarien 2 und 3 unterliegen. Hierbei steht v.a. die Frage im Vordergrund, ob und wenn ja, unter welchen Bedingungen, Bestimmungen des SGB X und das Sozialgeheimnis nach § 35 SGB I auch für die externe Einrichtung gelten.

I.X Stellen Sie bitte dar, nach welchen gesetzlichen Vorschriften die externe Einrichtung zur Übermittlung von Sozialdaten an weitere Sozialleistungsträger (vgl. §§ 18-29 SGB I) nach SGB X, I und V verpflichtet werden kann, wenn hierfür keine Einwilligung des Betroffenen vorliegt. Ist der Betroffene vor der Datenübermittlung zu informieren bzw. hat er eine Möglichkeit, die Datenweitergabe zu verhindern?

I.XI Gehen Sie bitte bei Szenario 2 und 3 auf die Frage ein, ob der gesetzlich Versicherte gegenüber der gesetzlichen Krankenversicherung oder der externen Einrichtung einen Auskunftsanspruch dahingehend hat, ob und in welcher Form seine Daten für weitere Zwecke (z.B. wissenschaftliche Forschung, Planung oder Qualitätssicherung) verwendet werden. Stellen Sie bitte dar, welche konkreten Informationen im Rahmen des Auskunftsersuchens mitgeteilt werden müssen. Stellen Sie bitte auch dar, ob es für die rechtliche Würdigung entscheidend ist, ob die Datennutzung der externen Einrichtung auf Grundlage einer Einwilligung oder einer gesetzlichen Übermittlungsnorm stattgefunden hat.

II Bewertung der zukünftigen Rechtslage

II.I Bitte werten Sie die für die Beantwortung dieser Fragen relevanten Vorschriften der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) und die in der Entstehung befindlichen Gesetzentwürfe des Bundes zur Anpassung an die EU-DSGVO aus und prüfen Sie, welche Änderungen in Bezug auf die vorher beschriebenen drei Szenarien und die jeweils in den Fragen genannten Aspekte entstehen.

II.II Wie bewerten Sie die Konformität der aktuell vorliegenden Gesetzentwürfe mit den Vorgaben der EU-DSGVO? Sehen Sie Risiken, dass vor diesem Hintergrund weitere gesetzliche Anpassungen notwendig werden, die Auswirkungen auf die oben beschriebenen Szenarien haben werden?

III Über die aktuellen Gesetzesentwürfe hinausgehende Reformüberlegungen

Bei den folgenden Fragestellungen berücksichtigen Sie bitte auch, welche wesentlichen Grundsätze aus der EU-DSGVO, dem europäischen und deutschen Verfassungsrecht zu beachten sind.

III.I Wie müsste eine Rechtsgrundlage gestaltet sein, die die Errichtung und Nutzung einer (von den gesetzlichen Krankenversicherungen unabhängigen) Datenplattform ermöglicht, auf der unterschiedliche Sozial- und Gesundheitsdatensätze extern gespeichert werden (vgl. Szenario 3)? Eine solche Plattform sollte für Zwecke der wissenschaftlichen Forschung, Planung im Sozialleistungsbereich und Qualitätssicherung offen sein. Dies schließt auch eine langfristige Speicherung der Daten ein, die eine Nachvollziehbarkeit der Auswertungen für übliche Zeiträume (in der Forschung z.B. 10 Jahre) ermöglicht. Um repräsentative Auswertungen zu ermöglichen, sollte die Einholung von Einwilligungen der betroffenen Personen verzichtbar sein. Mit welchen technisch-organisatorischen oder sonstigen Maßnahmen kann sichergestellt werden, dass ein fairer Ausgleich zwischen dem Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen und dem Grundrecht auf Forschungsfreiheit bzw. anderen gesellschaftlichen Interessen sichergestellt wird?

III.II Wie könnte eine gesetzliche Grundlage aussehen, die es dem Betroffenen ermöglicht, auch eine Einwilligung mit einer breiteren Zweckbestimmung (z.B. medizinische Forschung) rechtswirksam abzugeben? Gehen Sie bitte dabei auch darauf ein, inwieweit Aufsichtsbehörden und gesetzliche Krankenversicherungen an den Inhalt der abgegebenen Einwilligungserklärung der betroffenen Person gebunden sind. Prüfen Sie bitte auch, ob eine solche Einwilligung auch für künftig erhobene Sozialdaten gelten kann, oder ob es rechtlich erforderlich erscheint, die Einwilligungserklärung in Bezug auf Sozial-

daten nach Ablauf einer bestimmten Zeit erneut einzuholen (z.B. nach fünf Jahren), oder ob sie auch mit einer breiten Zweckbestimmung auch für einen längeren Zeitraum (z.B. 10-20 Jahre bzw. bis zum Tod des Versicherten) gelten kann. Gibt es Ihrer Auffassung nach bei solchen „breiten Einwilligungserklärungen" besondere Informationsrechte des Betroffenen?

IV Weitergehende Fragen zu den rechtlichen Grundlagen des Datenschutzes[2]

Bitte bewerten Sie im Folgenden die zukünftige Rechtslage nach EU-DSGVO und EU-Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG) und stellen Sie in Bezug auf das Umsetzungsgesetz jeweils dar, ob aus Ihrer Sicht die Vorgaben aus dem europäischen/deutschen Verfassungsrecht bzw. aus der EU-DSGVO eingehalten wurden:

IV.I Vergleichen Sie bitte den Pseudonymisierungsbegriff aus den bisherigen Vorschriften des Bundesdatenschutzgesetzes (BDSG) mit jenen aus der EU-Datenschutzgrundverordnung. Sind diese gleichbedeutend oder ergeben sich unterschiedliche Anforderungen an den Pseudonymisierungsprozess? Gehen Sie in Bezug auf die bisherige Rechtslage bei der Nutzung pseudonymer Daten auch auf das Urteil des Europäischen Gerichtshofs (EuGH) vom 19.10.2016 (Patrick Breyer gegen Bundesrepublik Deutschland, Aktz. C – 582/14) ein. Von Interesse ist hier, ob die EU-DSGVO eher das Konzept eines „absoluten" oder eines „relativen Personenbezugs" unterstützt.

IV.II Gehen Sie bitte auf den Begriff der „wissenschaftlichen Forschungszwecke" (nach Erwägungsgrund 159 der EU-DSGVO) ein und beschreiben Sie, ob die Inhalte dieses Erwägungsgrundes zu einer anderen Interpretation des Begriffs „wissenschaftliche Forschung" führen, als dies bisher der Fall war. Insbesondere bitten wir um einen Vergleich zu der Rechtsauffassung von Herrn Dr. Schneider auf Seite 97/98 (TMF-Veröffentlichung: U.K. Schneider, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, Band 12).

IV.III Bitte vergleichen Sie die bisherige Definition des Anonymisierens nach BDSG mit dem Erwägungsgrund 26 der EU-DSGVO und führen Sie aus, wo aus Ihrer Sicht Unterschiede im Vergleich zur bisherigen Rechtslage bei der Nutzung anonymer Daten für die wissenschaftliche Forschung bestehen.

IV.IV Kann eine wirksame Anonymisierung von Daten als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 EU-DSGVO angesehen werden? Gehen Sie bitte auch darauf ein, ob eine wirksame Anonymisierung ausrei-

2 Die Fragen aus diesem Abschnitt IV werden von dem Gutachtenteil von Prof. Roßnagel im vorliegenden Band beantwortet.

chend ist, wenn die Löschung im Rahmen einer Einwilligung vereinbart wurde.

IV.V Der Bundesrat hat in seinem Beschluss zum DSAnpUG-EU (vgl. Ziff. 27 Lit. d), BR-Drucksache 110/17 v. 10.03.2017) für die Behandlung im weiteren Gesetzgebungsverfahren die Frage aufgeworfen, inwieweit ein Ausschluss der Auskunftserteilung neben den in § 27 BDSG-E genannten Voraussetzungen nach objektiven Kriterien auch aus therapeutischen sowie ethischen Erwägungsgründen zum Wohl der betroffenen Person möglich sein sollte. Prüfen Sie bitte, auf welcher verfassungs- und europarechtlichen Grundlage solche Ausnahmen von den Auskunftsrechten für wissenschaftliche Forschungsvorhaben vorgenommen werden können.

IV.VI Nach dem Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (BR-Drucksache 163/17) soll § 203 Straf-Gesetzbuch (StGB) in der Form geändert werden, dass die Weitergabe von Informationen an „mitwirkende Personen" für einen Berufsgeheimnisträger (z.B. Arzt) straflos sein soll, wenn diese an der „beruflichen Tätigkeit" des Berufsgeheimnisträgers mitwirken. Prüfen Sie bitte, ob eine Mitwirkung an einer Forschungstätigkeit eines Arztes auch als Mitwirkungshandlung im Sinne der neuen Rechtsvorschrift verstanden werden kann. Gehen Sie bitte darauf ein, wie die „berufliche Tätigkeit" eines Arztes auch mit Blick auf die EU-DSGVO und den bisherigen Rechtsrahmen definiert wird und ob Unterschiede zwischen der ärztlichen Tätigkeit in einem Universitätskrankenhaus/sonstigem Krankenhaus und einer Arztpraxis bestehen.

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 in den vergangenen Jahren 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 werden. 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.

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),
- Zoonosen-Forschungsverbünde,
- zentralisierte Biomaterialbanken (Nationale Biobanken-Initiative)
- 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 neun Arbeitsgruppen:

- Arbeitsgruppe Biomaterialbanken
- Arbeitsgruppe Datenschutz
- 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 – aktuell insbesondere zum Thema Versorgungsforschung – 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“. Die Publikation dieser weiteren Rechtsgutachten in der TMF-Schriftenreihe wird sukzessive folgen.

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 beachtet 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.

Der vorliegende Band 17 bietet einen Überblick über den aktuellen Rechtsrahmen zur Nutzung von Sozial- und Gesundheitsdaten für die Forschung.

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

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