

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 2017⁴ 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 2017⁵ 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 Berufsheimnisträgern beschlossen. Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ vom 30.10.2017⁶ 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 Berufsheimnisträger 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 Empfehlungen⁸ abgegeben. Der diesbezügliche Beschluss des Bundesrates vom 19.10.2018⁹ 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.