RECHTSGUTACHTEN

ÜBER DEN

**SOZIALDATENSCHUTZRECHTLICHEN WEITERENTWICKLUNGSBEDARF
IM SGB V UND SGB X IM HINBLICK AUF BIG-DATA-ANWENDUNGEN**

ERSTELLT IM AUFTRAG DES

BUNDESMINISTERIUM FÜR GESUNDHEIT

VON

PROF. DR. IUR. JÜRGEN KÜHLING, LL.M. (BRÜSSEL)

UNIVERSITÄTSPROFESSOR, REGENSBURG

UNTER MITWIRKUNG VON

FLORIAN SACKMANN UND ROMAN SCHILDBACH

REGENSBURG

- ENDFASSUNG -

STAND: 4. SEPTEMBER 2019

GLIEDERUNG

A.	EINFÜHRUNG UND EINGRENZUNGEN	6
I.	HINTERGRUND DER UNTERSUCHUNG: BIG-DATA-ANWENDUNGEN IM GESUNDHEITSWESEN... 6	6
	1. <i>Definition von „Big Data“</i>	6
	2. <i>Sozialdaten verarbeitende Big-Data-Anwendungen in der Realwelt</i>	8
II.	REFORMVORSCHLÄGE DES DEUTSCHEN ETHIKRATES	10
	1. <i>Grundansatz der Stellungnahme des Deutschen Ethikrates zum Thema „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung“</i>	10
	2. <i>Abkehr von den allgemeinen Grundsätzen der Datenminimierung und der Zweckbindung</i>	11
	3. <i>Die Möglichkeit einer zweckungebundenen Datenspende im Besonderen.....</i>	14
	4. <i>Konzept der Datensouveränität.....</i>	14
III.	GESUNDHEITS-, SOZIAL- UND LEISTUNGSDATEN SOWIE REGELUNGSSYSTEMATIK VON SGB V UND SGB X	15
	1. <i>Gesundheits-, Sozial- und Leistungsdaten.....</i>	15
	a) Gesundheitsdaten.....	16
	b) Sozialdaten	17
	c) Leistungsdaten.....	18
	2. <i>Verantwortliche und Betroffene im Gesundheitswesen im Allgemeinen und im SGB V und SGB X im Besonderen</i>	19
	a) <i>Trias: „Versicherter – Leistungserbringer – Leistungsträger“</i>	19
	b) <i>Akteure in der Sphäre des Patienten/Versicherten.....</i>	20
	c) <i>Akteure auf Leistungserbringerseite</i>	20
	d) <i>Akteure auf Leistungsträgerseite</i>	21
	3. <i>Struktur und Zusammenspiel der gesetzlichen Regelungen im Gesundheitswesen, insbesondere im SGB V und SGB X</i>	22
	a) <i>DS-GVO: Ausgangspunkt mit weiten Öffnungsklauseln</i>	23
	b) <i>Regelungsstruktur des allgemeinen Datenschutzrechts</i>	23
	c) <i>Subsidiarität des allgemeinen Datenschutzrechts: das Sozialdatenschutzrecht in SGB V und SGB X als bereichsspezifischer Gesundheitsdatenschutz des Bundes.....</i>	24
	d) <i>Abrechnung der Leistungserbringer als datenschutzrechtliches Kernstrukturelement im SGB V</i>	25
	e) <i>Das Sozialdatenschutzrecht der Leistungsträger in den SGB I, X und V</i>	26
IV.	KONSEQUENZEN FÜR DEN FORTGANG DER UNTERSUCHUNG.....	27
B.	HANDLUNGSMÖGLICHKEITEN IM RAHMEN DES GELTENDEN RECHTS.....	28
I.	VORGABEN UND STEUERUNGSWIRKUNG DER DS-GVO FÜR DAS GESUNDHEITSWESEN	28
	1. <i>Harmonisierungsanspruch und Öffnungsklauseln in der DS-GVO im Detail.....</i>	28
	a) <i>Begrenzte Harmonisierungswirkung angesichts zahlreicher Öffnungsklauseln</i>	28
	b) <i>Art. 9 DS-GVO mit umfassenden Öffnungsklauseln für das Gesundheitswesen.....</i>	29
	c) <i>Besonderheiten mit Blick auf die Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO</i>	30
	d) <i>Öffnungsklausel für die Datenverarbeitung im Gesundheitswesen insbesondere in Art. 9 Abs. 2 lit. h DS-GVO</i>	31
	e) <i>Zwischenfazit: nationaler Flickenteppich statt unionaler Vollharmonisierung.....</i>	33
	2. <i>Sachlicher Anwendungsbereich der Datenschutzordnung</i>	33
	a) <i>Personenbezogene Daten</i>	34
	b) <i>Anonyme und pseudonyme Daten</i>	37

aa)	Anonyme Informationen	37
bb)	Pseudonymisierung	38
3.	<i>Zentrale Steuerungskonzepte</i>	40
a)	Datensparsamkeit bzw. Datenminimierung	41
b)	Zweckbestimmung bzw. -begrenzung	41
c)	Die Erforderlichkeit der Datenverarbeitung	46
d)	Reichweite und Grenzen der Einwilligung	47
aa)	Allgemeine Voraussetzungen der Einwilligung	47
bb)	Besondere Voraussetzungen der Einwilligung bei der Verarbeitung von Gesundheitsdaten	48
II.	REGELUNGSSYSTEMATIK DER §§ 303A FF. SGB V ALS SCHWERPUNKT DER BETRACHTUNG	49
1.	<i>Normzweck: Datentransparenz und Datenschutz</i>	49
2.	<i>Herkunft und Art der Daten im Dateisystem</i>	50
3.	<i>Akteure und Verfahren der Datenübermittlung</i>	51
a)	Bundesversicherungsamt (BVA)	52
b)	Bundesministerium für Gesundheit (BMG).....	52
c)	Vertrauensstelle nach § 303c SGB V, Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)	52
d)	Datenaufbereitungsstelle nach § 303d SGB V, Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)	54
4.	<i>Bereitstellung der Daten und Zweckbindung</i>	54
a)	Nutzungsberechtigte Stellen	54
b)	Zweckbindungsgrundsatz des § 303e Abs. 2 SGB V.....	55
c)	Art der Bereitstellung	56
5.	<i>Verhältnis zur DS-GVO</i>	57
a)	Grundsätzliche Anwendbarkeit.....	57
b)	Umfassende Öffnungsklauseln im Gesundheitswesen.....	58
III.	PROBLEMATISCHE EINZELFRAGEN	59
1.	<i>Anonymität und Reidentifikation</i>	59
a)	Fallgruppen der Reidentifikation	60
aa)	Fallzahlproblem.....	61
bb)	Randsummenproblem.....	61
b)	Arten von nutzbaren Daten im Versorgungssystem	61
aa)	Aggregierte Daten	62
bb)	Einzeldatensätze	63
c)	Verbot der Reidentifikation	65
2.	<i>Forschungsprivileg und Erforderlichkeit</i>	65
3.	<i>Reichweite der Zweckbindung im Bereich der Wissenschaft</i>	67
4.	<i>Prozedurale Ausdifferenzierung des Antragsverfahrens und Möglichkeit zur Risikoabwägung</i>	69
5.	<i>Auskunftsansprüche von Versicherten</i>	70
6.	<i>Regelungsebene datenschutzrechtlicher Zulässigkeitstatbestände</i>	71
a)	Parlamentsvorbehalt und Bestimmtheitsgebot.....	71
b)	Bedeutung für die Regelungen der Datentransparenz.....	72
7.	<i>Weitere Problemstellungen aus SGB V und X</i>	73
a)	§ 76 SGB X	73
b)	§ 78 SGB X i.V.m. § 305 Abs. 1 SGB V.....	74

IV.	KONSEQUENZEN FÜR DIE REFORMVORSCHLÄGE DES DEUTSCHEN ETHIKRATES	75
1.	<i>Die Möglichkeit einer zweckungebundenen Datenspende de lege lata</i>	75
a)	Allgemeine Anforderungen an eine Einwilligung im Forschungskontext	76
b)	Rechtsunsicherheit als Hemmnis für eine effektive Forschung	76
2.	<i>Konzept der Datensouveränität</i>	77
C.	MÖGLICHE REFORMEN DE LEGE FERENDA	78
I.	GRUNDRECHTLICHE STEUERUNGSVORGABEN	78
1.	<i>Vorgaben aus dem Datenschutzgrundrecht des Art. 8 GrCh (und Art 7 GrCh)</i>	78
2.	<i>Vorgaben aus dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG</i>	81
II.	DIE DS-GVO ALS REFORMOBJEKT UND RAHMEN NATIONALER REFORMEN	84
III.	REFORMEN IM SGB V UND SGB X	85
1.	<i>Datentransparenz gemäß den §§ 303a ff. SGB V</i>	85
a)	Referenten- und Kabinettsentwurf	86
aa)	Referentenentwurf	86
bb)	Kabinettsentwurf	89
b)	Regelungsebene des Datenumfangs	90
c)	Integration von Institutionskennzeichen, Betriebsgeheimnis	91
d)	Fragen der Zweckbindung und Öffnung für die Forschung	93
e)	Erforderlichkeitsprüfung	95
f)	Risikoabwägung und prozedurale Ausdifferenzierung	96
g)	Zur Verwendung der Begriffe „anonymisiert“ und „pseudonymisiert“	97
h)	Verbot der Reidentifikation und Sanktionen	102
i)	Verknüpfung mit weiteren Sozialdaten oder Behandlungsdaten	102
j)	Zwischenfazit	104
2.	<i>Gesetzgeberischer Klarstellungs- und Anpassungsbedarf im SGB X</i>	105
a)	§ 76 Abs. 2 SGB X	105
b)	§ 78 SGB X	107
IV.	BEWERTUNG DER REFORMVORSCHLÄGE DES DEUTSCHEN ETHIKRATES DE LEGE FERENDA	107
1.	<i>Abkehr vom Grundsatz der Datensparsamkeit bzw. der Datenminimierung?</i>	107
2.	<i>Abkehr vom Grundsatz der Zweckbindung im Allgemeinen?</i>	108
3.	<i>Die Möglichkeit einer zweckungebundenen Datenspende im Besonderen</i>	109
a)	Unionsrechtlicher Rahmen	109
b)	Verfassungsrechtlicher Rahmen	110
c)	Berücksichtigung der Rechte Dritter	111
d)	Handlungsempfehlung	111
4.	<i>Ergänzende Einführung eines Konzepts der Datensouveränität?</i>	113
D.	ZUSAMMENFASSUNG DER ERGEBNISSE; HANDLUNGSEMPFEHLUNGEN MIT KONKRETEN VORSCHLÄGEN FÜR GESETZESÄNDERUNGEN	115
I.	HINTERGRUND, STÖBRICHTUNG UND EINGRENZUNG DER UNTERSUCHUNG	115
1.	<i>Zunehmende Big-Data-Anwendungen; Reformvorschläge des Deutschen Ethikrates</i> ..	115
2.	<i>Stoßrichtung der Untersuchung</i>	115
3.	<i>Definition von „Big Data“</i>	116
4.	<i>Big-Data-Anwendungen in der Realwelt von SGB V und SGB X</i>	116

II.	DER RECHTLICHE HANDLUNGSRAHMEN IM GELTENDEN RECHT	117
1.	<i>Der Anwendungsbereich des Datenschutzrechts</i>	117
a)	Begriff des personenbezogenen Datums in Abgrenzung zu anonymen Daten.....	117
b)	Pseudonymisieren	118
2.	<i>Zentrale Datenschutzgrundsätze</i>	118
III.	BEWERTUNG DER REFORMVORSCHLÄGE DES DEUTSCHEN ETHIKRATES	118
1.	<i>Ergänzende Einführung eines Konzepts der Datensouveränität?</i>	118
2.	<i>Abkehr vom Grundsatz der Datensparsamkeit bzw. der Datenminimierung?</i>	119
3.	<i>Abkehr vom Grundsatz der Zweckbindung im Allgemeinen?</i>	119
4.	<i>Die Möglichkeit einer zweckgebundenen Datenspende im Besonderen</i>	120
IV.	KONKRETE GESETZGEBUNGSEMPFEHLUNGEN HINSICHTLICH DER DATENTRANSPARENZ GEMÄß DEN §§ 303A FF. SGB V UND IM § 76 SGB X	120
1.	<i>Datenumfang auf der Ebene eines formellen Gesetzes</i>	120
2.	<i>Schutz der Betriebs- und Geschäftsgeheimnisse</i>	121
3.	<i>Zweckbindung und Öffnung für die Forschung</i>	122
a)	Klarstellung hinsichtlich des Katalogs des § 303e Abs. 2 SGB V	122
b)	Klarstellung bezüglich des Umfangs der Zweckbindung in der Wissenschaft	122
4.	<i>Erforderlichkeitsprüfung</i>	122
5.	<i>Risikoabwägung und prozedurale Ausdifferenzierung</i>	123
6.	<i>Zur Verwendung der Begriffe „anonymisiert“ und „pseudonymisiert“</i>	124
7.	<i>Normierung eines Verbots der Reidentifikation</i>	125
8.	<i>Sanktionen für Datenschutzrechtsverstöße</i>	125
a)	Sperren von nutzungsberechtigten Stellen nach § 303e Abs. 6 S. 2 SGB V-E	125
b)	Straftatbestand für die vorsätzliche Reidentifikation von Versicherten	125
c)	Protokollierung der Datenzugriffe	126
9.	<i>Gesetzgeberischer Klarstellungs- und Anpassungsbedarf im SGB X</i>	126
a)	§ 76 Abs. 2 SGB X	126
b)	§ 78 SGB X	126

A. Einführung und Eingrenzungen

In einem ersten Schritt sollen zunächst die Hintergründe des vorliegenden Rechtsgutachtens erläutert sowie der Untersuchungsgegenstand angesichts der Fülle (gesundheits-)datenschutzrechtlicher Probleme in einer Welt der Big-Data-Anwendungen näher eingegrenzt werden. Dabei ist Hauptanlass der folgenden Untersuchung die zunehmende Verwendung von Big-Data-Analysen im Gesundheitswesen (dazu I.), die zu einer Vielzahl datenschutzrechtlicher Herausforderungen führt. Leitfrage der gesamten Studie ist, ob das geltende Regelungsregime, das im nächsten Teil B. näher betrachtet wird, diesen Herausforderungen gerecht wird, oder ob es Anpassungen des normativen Rahmens bedarf. Letzteres wird im dritten Teil C. ausführlich untersucht. Im abschließenden vierten Teil (dazu D.) können dann die Ergebnisse zusammengetragen werden und es kann ein Ausblick erfolgen. Dabei fokussiert die vorliegende Untersuchung auf die Regelungen im SGB V und SGB X und dabei auf die Verwendung von Sozialdaten im Rahmen der Versorgung durch gesetzliche Krankenkassen (und nicht durch die privaten Krankenversicherungen).

Weiterer Anlass der Studie sind im Übrigen die Reformvorschläge, die der Deutsche Ethikrat für die Fortentwicklung des Datenschutzrechts Ende 2017 unterbreitet hat. Diese sind im Rahmen der Einführung ebenfalls knapp zu skizzieren (dazu II.). Sodann werden grundlegende Hinweise zur Eingrenzung des Gesundheitswesens als Betrachtungsgegenstand der vorliegenden Untersuchung gegeben sowie zur Definition der hier primär relevanten Kategorien der Sozial- und Leistungsdaten, bei denen es sich regelmäßig um besonders sensible Gesundheitsdaten handelt. Auch die komplexe Regelungssystematik von SGB V und SGB X ist zu skizzieren (dazu III.).

Aus diesen grundlegenden Ausführungen folgen die Prüfungsrichtung und der nähere Prüfungsgegenstand des vorliegenden Rechtsgutachtens (dazu IV.).

I. Hintergrund der Untersuchung: Big-Data-Anwendungen im Gesundheitswesen

Den Kerngegenstand der Untersuchung bilden Big-Data-Analysen im Gesundheitswesen. Vor diesem Hintergrund ist zunächst der Begriff „Big Data“ näher einzugrenzen (dazu 1.), bevor typische Anwendungsfälle skizziert werden sollen (dazu 2.).

1. Definition von „Big Data“

Unter „Big Data“ als Sammel- oder Oberbegriff fasst man grundsätzlich solche Anwendungen, Applikationen oder Analyseprogramme, die eine außerordentlich große und gegebenenfalls

heterogene Datenmenge innerhalb kurzer Zeit (oder in Echtzeit) auswerten. Als Kernmerkmale werden häufig die „drei Vs“ genannt: volume (Menge), velocity (Geschwindigkeit/Echtzeit) und variety (unterschiedliche Daten).¹ Hinzu kommen teilweise noch validity (Richtigkeit bzw. Wahrheitsgehalt der Daten) oder alternativ veracity (Genauigkeit) und value (wirtschaftlicher Wert), so dass man auch von „fünf Vs“ sprechen kann.² Eine außergewöhnlich hohe Trennschärfe bietet der Begriff damit nicht und kann schon gar nicht als rechtliche Definition verstanden werden. Jedoch treten im Rahmen von Big-Data-Anwendungen in der Regel eine Reihe von Besonderheiten auf, die sodann (datenschutz-)rechtliche Fragestellungen aufwerfen. Hierzu zählt vor allem, dass – anders als bei vielen herkömmlichen Analysetechniken – nicht gezielt nach der Antwort auf eine bestimmte Fragestellung gesucht wird, sondern die Anwendung ergebnisoffen nach Mustern und Zusammenhängen sucht, woraus sich gänzlich neue Erkenntnisse ergeben können.³ Durch das Aufzeigen von Korrelationen kann die Big-Data-Anwendung so oftmals dazu beitragen, die richtigen Fragen überhaupt erst zu stellen. Dementsprechend groß sind die Hoffnungen, die in verschiedensten Lebensbereichen – insbesondere auch im Gesundheitssektor – in Big-Data-Techniken gesetzt werden. Demgegenüber stehen jedoch die Risiken, die mit der systematischen Auswertung solch großer Datenmengen einhergehen.⁴ Die Persönlichkeitsrechtsverletzungen bei einer Big-Data-Anwendung werden in der Regel Folgen für eine große Zahl von Betroffenen entfalten. Werden darüber hinaus auch noch sensible Daten (wie Gesundheitsdaten) verarbeitet, können Datenschutzrechtsverstöße besonders schwer wiegen. Letztlich ist zu befürchten, dass ein unkontrolliertes Sammeln großer Mengen von personenbezogenen Daten in Verbindung mit einer detaillierten und intelligenten Auswertung dieser den Menschen zum vielbeschworenen „gläsernen Bürger“ macht.

¹ Vgl. die Definition der Unternehmensgruppe *Gartner*, abrufbar unter <https://www.gartner.com/en/conferences/na/data-analytics-us>, abgerufen am 24.6.2019; siehe auch *Rüping*, Bundesgesundheitsblatt 2015, 794; *Spindler*, MedR 2016, 691.

² *Culik/Döpke*, ZD 2017, 226, 227; *Hoffmann-Riem*, in: Hoffmann-Riem (Hrsg.), Big-Data – Regulative Herausforderungen, S. 19 f.; *Weichert*, Big-Data im Gesundheitsbereich, Gutachten 2019, S. 16, abrufbar unter: <http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf>, abgerufen am 16.4.2019.

³ *Boehme-Neßler*, DuD 2016, 419, 421 f.

⁴ Siehe zu den Risiken bereits *Weichert*, ZD 2013, 251.

2. Sozialdaten verarbeitende Big-Data-Anwendungen in der Realwelt

Im Fokus der vorliegenden Betrachtung stehen rechtssystematisch die SGB V und X und inhaltlich die von den gesetzlichen Krankenkassen erhobenen Sozialdaten als Grundlage für Big-Data-Anwendungen. Die Sozialdaten werden zunächst zu Abrechnungszwecken im weiteren Sinn erhoben. Bei mehr als 72 Mio. Versicherten in den gesetzlichen Krankenkassen⁵ sind diese Datensätze von erheblichem Ausmaß.⁶ Über die bloße Abrechnung hinausgehend weisen diese Daten damit Potentiale für die Auswertung mithilfe von Big-Data-Anwendungen auf.⁷ Beschäftigt man sich mit der Frage, inwieweit dieser Datenpool mithilfe von Big-Data-Techniken analysiert wird, so stößt man im Wesentlichen auf zwei Bereiche. Erstens nutzen viele gesetzliche Krankenkassen bereits heute die Sozialdaten ihrer Versicherten zur internen Prozessoptimierung.⁸ Bei der Verwendung von Big-Data nahmen die Krankenkassen bislang gegenüber anderen Wirtschaftszweigen sogar eine Vorreiterrolle ein.⁹ Zweitens wecken die Daten der Krankenkassen ein erhebliches Interesse der medizinischen und pharmakologischen Forschung¹⁰ und schließlich vor allem in der sogenannten Versorgungsforschung. Wichtig sind die Daten in diesem letzten Zusammenhang vor allem für die Bedarfsplanung, denn sie geben Auskunft über regional durchaus unterschiedliche Bedarfe hinsichtlich der einzelnen Facharztgruppen.

⁵ GKV-Spitzenverband, Kennzahlen der gesetzlichen Krankenversicherung, abrufbar unter: https://www.gkv-spitzenverband.de/gkv_spitzenverband/presse/zahlen_und_grafiken/zahlen_und_grafiken.jsp#, abgerufen am 24.6.2019.

⁶ Deutsche Aktuarvereinigung, Ergebnisbericht des Ausschusses Krankenversicherung, Nutzung von Big-Data in der Krankenversicherung, 2017, S. 5, abrufbar unter: https://aktuar.de/unsere-themen/fachgrundsaetze-oeffentlich/2017-10-12_Ergebnisbericht_Nutzung_von_Big_Data_in_der_Krankenversicherung.pdf, abgerufen am 24.6.2019.

⁷ Vgl. *Spindler*, MedR 2016, 691, 691 f.

⁸ *Radic et al.*, Big Data im Krankenversicherungsmarkt, Studie des Fraunhofer-Zentrums für internationales Management und Wissensökonomie, 2016, S. 2, 14, abrufbar unter: https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Studien/Studie_Big%20Data%20im%20Krankenversicherungsmarkt.pdf, abgerufen am 24.6.2019.

⁹ *Weichert*, Big Data im Gesundheitsbereich, Gutachten 2019, S. 37, abrufbar unter: <http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf>, abgerufen am 24.6.2019.

¹⁰ Vgl. *Spindler*, MedR 2016, 691, 691 f.; *Ludwig*, SZ vom 10.11.2017, abrufbar unter: <https://www.sueddeutsche.de/wirtschaft/gesundheitsministerium-datenschutz-der-krankenkassen-weckt-begehrlichkeiten-1.3740473>, abgerufen am 24.6.2019.

Big-Data-Anwendungen kommen innerhalb der gesetzlichen Krankenkassen in verschiedenen Anwendungsgebieten zum Einsatz. Relevante Zielsetzungen entspringen vor allem den Bereichen der Finanzen, der Steuerung oder teils des Marketings und des Vertriebs.¹¹ Dabei kommen Big-Data-Anwendungen in den Anwendungsfeldern Versorgung und Marktanalyse deutlich stärker zum Einsatz als in den Bereichen des Personals, des Rechts und der Finanzen.¹² Die größten Datenquellen stellen neben den Stamm- und Abrechnungsdaten auch gesetzliche Quellen wie amtliche Statistiken und die im Zuge der Datentransparenz i.S.d. §§ 303a ff. SGB V zugänglichen Datensätze dar.¹³

Das andere große Anwendungsfeld bilden die medizinische und pharmakologische Forschung sowie die Versorgungsforschung mit den Sozialdaten. Die Wissenschaft verspricht sich durch die Forschung mit Big-Data-Analysen Erkenntnisgewinne und ein verbessertes Verständnis von Zusammenhängen.¹⁴ Die umfangreichen Datenmengen der gesetzlichen Krankenkassen bergen hierzu ein erhebliches Potenzial.¹⁵ Positive Ergebnisse können beispielsweise die Aufdeckung von schädlichen Neben-¹⁶ und Wechselwirkungen¹⁷ von Medikamenten sein. Dementsprechend ist es sinnvoll, die Daten unter bestimmten Voraussetzungen der Wissenschaft

¹¹ Radic et al., Big Data im Krankenversicherungsmarkt, Studie des Fraunhofer-Zentrums für internationales Management und Wissensökonomie, 2016, S. 2, 11, abrufbar unter: https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Studien/Studie_Big%20Data%20im%20Krankenversicherungsmarkt.pdf, abgerufen am 24.6.2019.

¹² Radic et al., Big Data im Krankenversicherungsmarkt, Studie des Fraunhofer-Zentrums für internationales Management und Wissensökonomie, 2016, S. 2, 11, abrufbar unter: https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Studien/Studie_Big%20Data%20im%20Krankenversicherungsmarkt.pdf, abgerufen am 24.6.2019.

¹³ Radic et al., Big Data im Krankenversicherungsmarkt, Studie des Fraunhofer-Zentrums für internationales Management und Wissensökonomie, 2016, S. 15 f., abrufbar unter: https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Studien/Studie_Big%20Data%20im%20Krankenversicherungsmarkt.pdf, abgerufen am 24.6.2019.

¹⁴ Ludwig, SZ vom 10.11.2017, abrufbar unter: <https://www.sueddeutsche.de/wirtschaft/gesundheitsministerium-datenschutz-der-krankenkassen-weckt-begehrlichkeiten-1.3740473>, abgerufen am 24.6.2019; Weichert, Big-Data im Gesundheitsbereich, Gutachten 2019, S. 51, abrufbar unter: <http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf>, abgerufen am 24.6.2019.

¹⁵ Vgl. Spindler, MedR 2016, 691, 691 f.

¹⁶ Siehe exemplarisch zur Gesundheitsschädlichkeit des Medikaments „Vioxx“ Ladeur, DuD 2016, 360, 363 m.w.N. (Fn. 32).

¹⁷ Siehe exemplarisch zu den Wechselwirkungen des Anti-Depressivums „Paxil“ und des Cholesterinsenkers „Pravastin“ Grötter, Handelsblatt v. 25.11.2014, abrufbar unter <https://www.handelsblatt.com/technik/medizin/der-glaeserne-patient-big-data-ersetzt-klinische-studien/11030186-2.html?ticket=ST-4213414-0p4u0agd1EYkxPtlL4Xd-ap5>, abgerufen am 24.6.2019.

als sekundäre Nutzung zur Verfügung zu stellen.¹⁸ Als Datenquelle können insoweit die Datensätze im Rahmen der Anwendung der Datentransparenz i.S.d. §§ 303a ff. SGB V relevant sein. Daneben eröffnet § 287 SGB V in Ergänzung zu den Vorschriften der §§ 67c Abs. 5 sowie 75 SGB X den Zugriff auch für die Entwicklung eigener Forschungsprojekte der Krankenkassen.¹⁹

II. Reformvorschläge des Deutschen Ethikrates

Der Deutsche Ethikrat hat für die Fortentwicklung des (Gesundheits-)Datenschutzrechts einige kontrovers diskutierte Reformvorschläge unterbreitet, die nachfolgend als zusätzlicher Anlass der vorliegenden Untersuchung kurz dargestellt und in die Diskussion um die Reform des (Gesundheits-)Datenschutzrechts eingeordnet werden sollen.

1. Grundansatz der Stellungnahme des Deutschen Ethikrates zum Thema „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung“

Ende 2017 hat der Deutsche Ethikrat eine umfassende Stellungnahme zum Thema „Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung“ vorgelegt. In diesem Dokument hat der Deutsche Ethikrat Vorschläge entwickelt, wie die Balance zwischen den Chancen und Risiken beim Einsatz von Big-Data-Anwendungen verbessert werden kann und welcher rechtlichen Anpassungen es insoweit bedarf. Die Stellungnahme betrachtet dabei eine große Bandbreite von Datenverarbeitungsprozessen im Gesundheitssektor, die über den vorliegend relevanten Kernbereich der Sozialdaten im Kontext gesetzlicher Krankenversicherungen weit hinausgeht. So werden etwa neben den im Gutachten ebenfalls zu beachtenden „benachbarten“ Anwendungsfeldern der Forschung und Gesundheitsversorgung die Verarbeitung durch Arbeitgeber oder global agierende IT- und Internetunternehmen mit in den Blick genommen. Dementsprechend vielfältig sind die adressierten Regelungsbereiche und Verbesserungspotenziale. Die Stellungnahme entwickelt jedoch auch einige vorliegend relevante spezifische sowie allgemeine Vorschläge, die im Gutachten in Bezug auf etwaige Reformbedürfnisse des SGB V und SGB X auf ihre Belastbarkeit und Umsetzbarkeit hin geprüft werden sollen.

¹⁸ Vgl. *Weichert*, DuD 2014, 831, 833.

¹⁹ Vgl. *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018, § 287 Rn. 1.

Zum Teil setzt die Stellungnahme sehr grundsätzlich an und betrachtet Fundamentalkategorien des geltenden Datenschutzrechts sehr kritisch. So heißt es skeptisch in der Ergebniszusammenfassung²⁰:

„Grundlegende Annahmen, zentrale Prinzipien und Zielvorgaben des überkommenen Datenschutzrechts sind mit den Besonderheiten von Big-Data-Anwendungen kaum in Einklang zu bringen. Die traditionellen datenschutzrechtlichen Grundsätze des Personenbezugs, der Zweckbindung und Erforderlichkeit der Datenerhebung, der Datensparsamkeit, der Einwilligung und Transparenz stehen der spezifischen Eigenlogik von Big-Data entgegen. Will man weder den Einsatz von Big-Data grundsätzlich untersagen noch relevante Einbußen am Schutzniveau hinnehmen, müssen neue Gestaltungsoptionen und Regelungsmechanismen entwickelt werden.“

Insgesamt geht die Stellungnahme davon aus, dass trotz der jüngsten Novelle des unionalen und des nationalen Rechtsrahmens (DS-GVO und BDSG) keine Regulationsstruktur geschaffen wurde, die den Herausforderungen durch Big-Data-Anwendungen gerecht wird.²¹

Im vorliegenden Gutachten sollen drei miteinander verknüpfte Aspekte näher betrachtet werden, nämlich:

1. eine – sehr grundlegende – mögliche Abkehr von den datenschutzrechtlichen Grundsätzen der Datensparsamkeit bzw. Datenminimierung einerseits und der Zweckbindung andererseits (dazu 2.);
2. damit eng verknüpft die Möglichkeit einer zweckungebundenen Datenspende für jegliche medizinische (und pharmakologische) Forschung (dazu 3.) und schließlich
3. das Konzept einer „Datensouveränität“ (dazu 4.).

2. Abkehr von den allgemeinen Grundsätzen der Datenminimierung und der Zweckbindung

Bei den Grundsätzen der Datensparsamkeit und der Zweckbindung handelt es sich um zwei Fundamentalprinzipien, die prägend sind für die Datenschutztradition im deutschen wie im

²⁰ *Deutscher Ethikrat*, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 22 f.

²¹ Ebenda und passim.

europäischen Recht. Sie haben dementsprechend auch prominent Eingang gefunden in die Regelungen der „Grundsätze für die Verarbeitung personenbezogener Daten“ in Art. 5 Abs. 1 lit. b („Zweckbindung“) und lit. c („Datenminimierung“) der DS-GVO. Grundgedanke der Zweckbindung ist die Idee, dass schon bei der Datenerhebung der künftige Zweck der Datenverarbeitung feststehen soll. Die Zweckbindung steht damit in unmittelbarem Zusammenhang mit der Datenminimierung, die dafür Sorge tragen soll, dass bei der Datenverarbeitung auch tatsächlich eine Beschränkung auf das für die Verfolgung des Zwecks Erforderliche gewährleistet ist.²² In der bisherigen Terminologie des BDSG a.F. sprach § 3a noch vom Grundsatz der „Datensparsamkeit“. Gleichwohl sind die Ansätze vergleichbar, auch wenn Art. 5 Abs. 1 lit. c DS-GVO dem Wortlaut nach primär auf die Zweckbindung rekurriert, während § 3a BDSG a.F. spezifischer auf die Möglichkeiten der Anonymisierung und Pseudonymisierung als Datenvermeidungs- bzw. Reduktionsstrategien verwies.²³

Der Deutsche Ethikrat sieht ein grundsätzliches Spannungsverhältnis zwischen „Big Data“-Anwendungen und den Grundsätzen der Zweckbindung und der Datensparsamkeit. Wörtlich heißt es insoweit in der Stellungnahme zum Grundsatz der Zweckbindung:²⁴

„Das geltende Datenschutzrecht (...) legt besonderen Wert auf die damit einhergehenden spezifischen Zweckbindungen. Für Big-Data ist demgegenüber entscheidend, dass bei der Erfassung der Daten die künftigen Anwendungen nicht vorhersehbar sind (...). Daten, die zu anderen Zwecken gespeichert wurden, werden oft für neue Zwecke ausgewertet oder es werden Daten für noch unbestimmte Zwecke erhoben.“

Hinsichtlich der Datenminimierung führt der Ethikrat aus:²⁵

„In augenfälligem Widerspruch zu Big-Data steht ferner der Grundsatz der Datensparsamkeit bzw. Datenminimierung, nach dem so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sollen. Das führt leicht zu einem weitgehenden Ausschluss der Möglichkeiten von Big-Data. Weil aber mit der Menge

²² Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 21.

²³ Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 55.

²⁴ Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 23.

²⁵ Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 23.

an gespeicherten Daten zugleich das Gefährdungspotenzial für das Recht auf informationelle Selbstbestimmung wächst, bedarf es wirksamer alternativer Schutzmechanismen.“

Offensichtlich schwebt dem Ethikrat demnach vor, den Grundsatz der Datenminimierung (und wohl auch der Zweckbindung) zugunsten anderweitiger Schutzkonzepte zurückzudrängen. Während die Problemanalyse insoweit recht deutlich ist, bleiben die substituierenden neuen Instrumente wesentlich unklarer. Sehr vage ist insoweit die folgende Aussage in Bezug auf die Einschränkung des Grundsatzes der Datenminimierung:²⁶

„Dieser Spannung kann im Rahmen der vom Verfassungsrecht gewährten Handlungsspielräume mit flexiblen, innovationsoffenen Regelungen Rechnung getragen werden, die auch die Verwendung komplexerer, privatrechtlicher wie privat-staatlich kooperativer Steuerungsbeiträge mitberücksichtigen.“

Offensichtlich besteht insoweit die Hoffnung, materiell-rechtliche Anforderungen durch prozedurale zu kompensieren. In diese Richtung deutet die folgende Ergebnisthese, die allerdings auch nur als Prüfauftrag formuliert ist:²⁷

„Insbesondere wäre zu prüfen, ob der Mangel an Konkretheit von gesundheitsrelevanten Big-Data-Anwendungen durch zusätzliche technisch-organisatorische sowie materiell- und verfahrensrechtliche Sicherungen kompensiert werden kann.“

Insoweit wird im Folgenden zu prüfen sein, ob eine Einschränkung der Grundsätze der Datenminimierung und der Zweckbindung im Allgemeinen geboten und rechtlich möglich ist und welche kompensatorischen Maßnahmen insoweit gegebenenfalls indiziert wären.

²⁶ Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 26.

²⁷ Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 26.

3. Die Möglichkeit einer zweckungebundenen Datenspende im Besonderen

Die Probleme der Zweckbindung im Allgemeinen zeigen sich auch mit Blick auf die Idee einer Datenspende im Besonderen. Insoweit heißt es in der Stellungnahme des Ethikrates stichwortartig auf der Empfehlungsliste²⁸:

„Rechtliche Möglichkeit für Individuen schaffen, die umfassende Nutzung ihrer Daten für die medizinische Forschung zu erlauben (,Datenspende‘)“

An anderer Stelle wird näher erläutert, dass es darum geht, insoweit auch im Bereich der Einwilligung zu Forschungszwecken eine Lockerung der Zweckbindung zu eröffnen und es dem Betroffenen zu ermöglichen, seine Daten „ohne enge Zweckbindung zugunsten der klinischen und medizinbezogenen Grundlagenforschung zu erlauben“²⁹. Kompensatorisch sind insoweit umfassende Informationspflichten vorgesehen, die sich interessanter Weise auch „auf die Rechte anderer, etwa mitbetroffener Familienmitglieder“ beziehen sollen. Kombiniert werden soll dies mit der Errichtung einer entsprechenden Infrastruktur, die unter wissenschaftlicher Begleitung eine „Erfassung, Speicherung, Pflege, Verarbeitung und Weitergabe von gespendeten Daten“ eröffnet.

4. Konzept der Datensouveränität

Auf grundlegender konzeptioneller Ebene wird schließlich eine Ausrichtung an einem Prinzip der „Datensouveränität“ für sinnvoll erachtet, das eine Fortentwicklung des Konzepts der informationellen Selbstbestimmung darstellen, aber den Chancen von Big-Data-Anwendungen stärker zur Entfaltung verhelfen soll.³⁰ Letztlich wird damit wohl weniger ein neuer Grundansatz verfolgt als vielmehr ein neuer Begriff ins Spiel gebracht. Dieser soll eine Akzentverschiebung markieren, die einer die informationelle Selbstbestimmung wahrende, gleichwohl aber die Entwicklungsmöglichkeiten von Big-Data-Anwendungen eher gerecht werdende Lesart des geltenden Rechts, aber auch einer stärker auf Letzteres ausgerichtete normative Fortentwicklung des Rechtsrahmens einschließlich seiner ethischen Fundierung bezeichnet. Zudem

²⁸ *Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 44.*

²⁹ Hierzu und zum Folgenden *Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 267.*

³⁰ Hierzu und zum Folgenden *Deutscher Ethikrat, Big-Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 39 ff.*

zielt die neue Chiffre darauf ab, zwei als wesentlich angesehene Sphären besser aufeinander abzustimmen, namentlich der Sphäre „der bislang schon durch vergleichsweise klare und strikte Datenschutz-, Qualitäts- und Sicherheitsstandards gekennzeichneten Datennutzung in der medizinbezogenen Forschung und klinischen Praxis“ mit der als zunehmend relevant identifizierten Sphäre der „sehr heterogenen Angebote des freien Marktes“ im Gesundheitssektor.³¹ Hier bleiben die konkreten Konsequenzen unklar und es erfolgen eher vage Hinweise auf die Notwendigkeit, sich auf „ständige Rekombinationen und Rekontextualisierungen“ einzurichten³² bzw. „über eine gleichermaßen kontextsensible wie falladäquate Regulierung und Institutionengestaltung diese Subjekte, aber auch die mit ihnen in Verbindung stehenden Organisationen zu einem souveränen Umgang mit ihren Daten zu befähigen. Vereinfachende Pauschalösungen sollten aufgegeben werden zugunsten komplexerer, aber auch flexiblerer und problemadäquater, institutionell diversifizierter Kombinationsmodelle.“³³ Schließlich wird für die zweite Sphäre des Marktes die Regel aufgestellt:³⁴

„Je näher einzelne Anwendungen an die erste Sphäre heranreichen, desto mehr besteht ethisch und rechtlich die Aufgabe, ihre Gestaltung multiakteursbezogen in die Richtung der dort generell vorherrschenden Qualitäts-, Schutz- und Vertraulichkeitsstandards zu entwickeln.“

III. Gesundheits-, Sozial- und Leistungsdaten sowie Regelungssystematik von SGB V und SGB X

1. Gesundheits-, Sozial- und Leistungsdaten

Zentrale Datenkategorien im Gesundheitswesen sind das Gesundheitsdatum (dazu a) sowie die Sozialdaten (dazu b) und die Leistungsdaten (dazu c). Unter dem Gesundheitswesen wird dabei allgemein – und auch im Folgenden – die Organisation der Gesundheitsversorgung durch die

³¹ *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 41.

³² *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 42.

³³ *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 42.

³⁴ *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 42.

gesetzliche und private Krankenversicherung verstanden.³⁵ Damit geht es vor allem um Datenströme, die bei der Behandlung von Patienten durch die Leistungserbringer und deren anschließender Abrechnung durch die Leistungsträger entstehen. Um die normative Steuerung der diesbezüglichen Zulässigkeit der Datenverarbeitung geht es im vorliegenden Gutachten. Ein besonderer Fokus liegt dabei auf dem SGB V und dem SGB X und die Sozialdaten, so dass die Datenflüsse ausschließlich mit Blick auf die gesetzlichen Krankenkassen und nicht hinsichtlich der privaten Krankenversicherung betrachtet werden. Demnach wird vorliegend nur ein Ausschnitt des Gesundheitswesens betrachtet.

a) Gesundheitsdaten

Das Datenschutzrecht im Gesundheitswesen betrifft damit nur ein Teilgebiet des weiter gefassten Gesundheitsdatenschutzrechts. Gleichwohl kann als klärender Ausgangspunkt die Legaldefinition von Gesundheitsdaten in Art. 4 Nr. 15 DS-GVO zugrunde gelegt werden. Gesundheitsdaten sind demnach „personenbezogene Daten, die sich auf den körperlichen oder geistigen Gesundheitszustand einer natürlichen Person, einschließlich der Erbringung von Gesundheitsleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.“ Der Begriff ist grundsätzlich weit auszulegen.³⁶ Zudem stellen nach Erwägungsgrund 35 der DS-GVO „Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren“ sowie „Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person“ Gesundheitsdaten dar. Irrelevant ist dabei, ob die Daten „von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum“ herrühren.

³⁵ Siehe zum Folgenden bereits *Kühling/Seidel*, in: Kingreen/Kühling (Hrsg.), *Gesundheitsdatenschutzrecht*, 2015, S. 30 ff. sowie *Kühling*, *MedR* 2019 (im Erscheinen).

³⁶ Siehe *Kühling/Klar/Sackmann*, *Datenschutzrecht*, 4. Aufl. 2018, Rn. 279; *Weichert*, in: *Kühling/Buchner* (Hrsg.), *DS-GVO/BDSG*, 2. Aufl. 2018, Art. 4 Nr. 15 Rn. 1; *Ernst*, in: *Paal/Pauly* (Hrsg.), *DS-GVO*, 2. Aufl. 2018, Art. 4 Rn. 109.

Anders als noch im Kommissionsentwurf³⁷ und dem Entwurf des Parlaments³⁸ genügt gemäß dem Wortlaut des Art. 4 Nr. 15 DS-GVO nicht mehr der bloße Bezug zur Erbringung von Gesundheitsleistungen. Als kumulative Voraussetzung hinzugekommen ist vielmehr das Erfordernis, dass sich Informationen über den Gesundheitszustand der betroffenen Person ableiten lassen müssen. Dies stellt zumindest eine geringfügige Einengung des Begriffs dar.³⁹ Für ein dennoch umfassendes Verständnis des Begriffs des Gesundheitsdatums spricht jedoch der Erwägungsgrund 35 der DS-GVO, der zunächst „Informationen über die natürliche Person, die im Zuge der *Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen* im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden“ mit einschließt.⁴⁰

b) Sozialdaten

Unter Sozialdaten sind gemäß § 67 Abs. 2 SGB X sämtliche personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO zu verstehen, allerdings nur, soweit sie von den in § 35 SGB I aufgezählten Stellen, insbesondere den Leistungsträgern, erhoben, verarbeitet und genutzt werden. Aufgrund der generell hohen Sensibilität besteht ein bereichsspezifisches Regelungssystem, das die Öffnungsklauseln in Art. 9 DS-GVO auf nationaler Ebene ausfüllt.⁴¹ Das Sozialgeheimnis als Rechtsanspruch des Bürgers aus § 35 SGB I i.V.m. den §§ 67 – 85a SGB X, die Zulässigkeitstatbestände für die Datenverarbeitung schaffen und zudem Öffnungsklauseln (§§ 67a – c SGB X) für Einzelregelungen in den einzelnen Sozialgesetzbüchern enthalten, bilden ein prinzipiell abgeschlossenes, dichtes Regelungsnetzwerk. Soweit Gesundheitsdaten gleichzeitig Sozialdaten sind, gilt für diese grundsätzlich der bereichsspezifische Regelungsmechanismus, mit der Konsequenz, dass andere Normen und gegebenenfalls andere Rechtsfolgen greifen.

³⁷ KOM/2012/011 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012PC0011>, Zugriff am 21.5.2019.

³⁸ Parlamentsdokument P7_TA(2014)0212, abrufbar unter <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014AP0212>, Zugriff am 21.5.2019.

³⁹ Vgl. noch zum offener formulierten Art. 4 Nr. 12 DS-GVO-E Kühling/Seidel, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 45 ff.

⁴⁰ Im Original nicht kursiv.

⁴¹ Vgl. zur Ausfüllung der Öffnungsklausel Weichert, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 60; zum bereichsspezifischen Regelungssystem vor der DS-GVO Krahrmer, in: Krahrmer (Hrsg.), Sozialdatenschutz nach SGB I und X, 3. Aufl. 2011, Einführung, Rn. 16, 20, § 35 SGB I, Rn. 5.

c) Leistungsdaten

Leistungsdaten nennt man die Daten, die die Leistungserbringer (z.B. Vertragsärzte) zu Abrechnungszwecken, also aufgrund der durch sie erbrachten Leistungen gemäß den §§ 294 ff. SGB V den damit beauftragten Stellen⁴² übermitteln. Dem liegt der Umstand zugrunde, dass die Krankenkassen ihrer Leistungsverpflichtung gegenüber den Versicherten grundsätzlich nicht selbst, sondern durch den Abschluss von Verträgen mit Leistungserbringern nachkommen, die dann die vertraglich vereinbarten Leistungen bewirken.⁴³ Um den dann daraus resultierenden Honoraranspruch zu erfüllen, bedarf es der Abrechnung und der Übermittlung der dazu benötigten leistungsbezogenen Daten.⁴⁴ Aus § 294 SGB V ergibt sich für die Leistungserbringer daher die grundsätzliche Aufzeichnungspflicht und die damit korrespondierende datenschutzrechtliche Befugnis zur Speicherung und Offenbarung der von § 294 SGB V erfassten Daten.⁴⁵ Die Details der Übermittlung zur Abrechnung, etwa welche Angaben genau zu übermitteln sind, ist in den §§ 294a ff. SGB V und den Richtlinien der Gemeinsamen Selbstverwaltung für den Datenaustausch geregelt.⁴⁶

Leistungsdaten sind also die Daten, die von den Leistungserbringern aufgrund der durch sie erbrachten Leistungen an die Krankenkassen, Kassenärztlichen Vereinigungen und andere übermittelt werden.⁴⁷ § 294 SGB V ist dabei die Befugnisnorm zur Datenspeicherung durch die Leistungserbringer,⁴⁸ während sich aus den §§ 294a – 303 SGB V die damit korrespondierenden Befugnisse und Pflichten ergeben, diese Daten zu Abrechnungszwecken weiterzuleiten. Richtigerweise sind Leistungsdaten nicht identisch mit Sozialdaten. Zu Sozialdaten „werden“ Leistungsdaten, ganz i.S.d. Legaldefinition von § 67 Abs. 2 S. 1 SGB X, erst im Moment der Erhebung, Verarbeitung oder Nutzung durch die Leistungsträger, also in der Regel durch die Krankenkassen. Während die Leistungsdaten zunächst nur jene sind, die der Arzt aufzeichnet, um sie *später* zu Abrechnungszwecken zu übermitteln, werden diese Daten erst in dem Moment zu Sozialdaten, wenn sie von den Leistungsträgern auch erhoben werden.

⁴² In der Regel sind dies die Krankenkassen und die Kassenärztlichen Vereinigungen, vgl. § 294 SGB V.

⁴³ *Becker/Kingreen*, in: *Becker/Kingreen* (Hrsg.), *SGB V. Gesetzliche Krankenversicherung*, 6. Aufl. 2018, § 69 Rn. 9 ff.

⁴⁴ *Fischinger/Monsch*, in: *Spickhoff* (Hrsg.), *Medizinrecht*, 3. Aufl. 2018, § 294 SGB V Rn. 1.

⁴⁵ *Michels*, in: *Becker/Kingreen* (Hrsg.), *SGB V*, 6. Aufl. 2018, § 294 Rn. 1 ff.

⁴⁶ *Michels*, in: *Becker/Kingreen* (Hrsg.), *SGB V*, 6. Aufl. 2018, § 294 Rn. 3.

⁴⁷ *Kühling/Seidel*, in: *Kingreen/Kühling* (Hrsg.), *Gesundheitsdatenschutzrecht*, 2015, S. 42 f. m.w.N.

⁴⁸ *Michels*, in: *Becker/Kingreen* (Hrsg.), *SGB V*, 6. Aufl. 2018, § 294 Rn. 1 ff.

Mit der Übermittlung (bzw. „Offenlegung durch Übermittlung“ in der Terminologie der DSGVO⁴⁹) vom Leistungserbringer an den Leistungsträger werden also aus Leistungsdaten Sozialdaten.⁵⁰ Dies ist beispielsweise der Fall, wenn ein niedergelassener Vertragsarzt personenbezogene Daten an den Leistungsträger weitergegeben hat oder dieser die Daten einsieht bzw. abrufen. Somit ist es konsequent, von Sozialdaten ab dem Zeitpunkt der Offenlegung durch Übermittlung zu sprechen, von dem an die entsprechenden Rechtsfolgen des bereichsspezifischen Sozialdatenschutzes greifen. Aufgrund der sehr speziellen Regelungssystematik im Sozialdatenschutzrecht ist diese präzise Unterscheidung keineswegs entbehrlich.

So handelt es sich auch bei den „Leistungsdaten“, von denen § 304 Abs. 1 S. 4 SGB V spricht, um solche, die bei den Krankenkassen aufbewahrt werden, und damit (bereits) um Sozialdaten. § 304 Abs. 1, Abs. 3 SGB V ist eine spezialgesetzliche Ergänzung zu § 84 Abs. 2 SGB X, der Fristen zur Aufbewahrung von Sozialdaten u.a. bei den Krankenkassen regelt.⁵¹

Auf dieser Basis sollte nur (aber auch immer) dann von Sozialdaten gesprochen, wenn auch tatsächlich (bereits) solche i.S.v. § 67 Abs. 2 S. 1 SGB X vorliegen. Äquivalent sollte der Begriff der Leistungsdaten nur für diejenigen Daten Anwendung finden, die von den Leistungserbringern für die spätere Übermittlung an die Leistungsträger zum Zwecke der Abrechnung verwendet werden.

2. Verantwortliche und Betroffene im Gesundheitswesen im Allgemeinen und im SGB V und SGB X im Besonderen

a) Trias: „Versicherter – Leistungserbringer – Leistungsträger“

Die Ausführungen zu den verschiedenen Datenbegriffen im Gesundheitsdatenschutzrecht im Allgemeinen und im Gesundheitswesen im Besonderen haben bereits das komplexe Zusammenspiel verschiedener Akteure deutlich werden lassen.⁵²

Das öffentliche Gesundheitswesen ist geprägt durch die Akteurstrias „Versicherter – Leistungserbringer – Leistungsträger“. Die gesetzlichen Krankenkassen schließen mit den Leis-

⁴⁹ Vgl. zur Terminologie *Herbst*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 2 Rn. 30 f.

⁵⁰ Zu den rechtlichen Konsequenzen siehe *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 233 ff.

⁵¹ *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, 6. Aufl. 2018, § 304 Rn. 1.

⁵² Die folgenden Ausführungen basieren auf *Kühling/Seidel*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 50 ff.; siehe auch *Kühling MedR 2019*, (im Erscheinen).

tungserbringern (Ärzte etc.) oder ihren Verbänden (Kassenärztliche Vereinigungen, Krankenhausgesellschaften etc.) Verträge, um ihre Leistungsverpflichtung gegenüber den Versicherten zu erfüllen (§ 2 Abs. 2 S. 3 SGB V) geprägt. Auf der Ebene der Abrechnung können dann weitere Akteure einbezogen sein, insbesondere private Abrechnungsunternehmen, die für bestimmte Leistungserbringer die Abrechnung mit den Leistungsträgern durchführen.

b) Akteure in der Sphäre des Patienten/Versicherten

Besonders relevant ist vorliegend natürlich zunächst der Betroffene selbst in seiner Eigenschaft als Versicherter bzw. Empfänger von Gesundheitsleistungen, der sich von seinem Hausarzt untersuchen lässt, ein verschreibungspflichtiges Arzneimittel per ärztlicher Verordnung in einer Apotheke abholt oder sich als untersuchungswillige Person auf genetische Dispositionen testen lassen möchte.

Daneben existiert aber eine Reihe von Akteuren, die nicht in das System der gesetzlichen Krankenversicherung integriert sind, aber dennoch Zugang zu gesundheitsrelevanten personenbezogenen Daten erhalten. Das können beispielsweise Sachverständige sein, die (im Sinne des § 79 SGB XI) die Wirtschaftlichkeit und Wirksamkeit ambulanter, teilstationärer und vollstationärer Pflegeleistungen prüfen oder Vertreter von nicht einwilligungsfähigen Personen (z.B. bei Minderjährigen im Rahmen eines Vaterschaftstests). Es kann sich aber auch um Behörden oder Einrichtungen handeln, deren Tätigkeitsfelder unmittelbar gesundheitsbezogen sind, etwa Gesundheitsämter oder das Robert-Koch-Institut (RKI), das insbesondere mit Krankheitsüberwachung und -prävention betraut ist, beispielsweise auf dem Gebiet des Infektionsschutzes, oder die Gendiagnostik-Kommission, die ihre Geschäftsstelle ebenfalls am RKI hat.

c) Akteure auf Leistungserbringerseite

Auch die Akteure, die Gesundheitsleistungen erbringen, sind vielfältig. Zu ihnen zählen zunächst die niedergelassenen Vertragsärzte der verschiedenen Fachrichtungen unter Einschluss der medizinischen Versorgungszentren (§ 95 SGB V), ferner Krankenhäuser (§ 108 SGB V) sowie diverse nichtärztliche Leistungserbringer (§§ 124 ff. SGB V) wie etwa Heilmittelerbringer (z. B. Physiotherapeuten, Logopäden), Hilfsmittelerbringer (etwa Augenoptiker, Hörgeräteakustiker), Apotheken und Dienste der häuslichen Krankenpflege. Hinzu kommen außerhalb des SGB V etwa Pflegeheime und ambulante Pflegedienste und genetische Labors, in denen genetische Untersuchungen zur Abstammungsklä rung vorgenommen werden.

In den Umgang mit gesundheitsrelevanten personenbezogenen Daten können aber auch Entitäten einbezogen sein, die als Verbände oder andere Zusammenschlüsse von einzelnen Leistungserbringern agieren. Bedeutsam sind in diesem Zusammenhang vor allem die 17 Kassen(zahn)ärztlichen Vereinigungen der einzelnen Bezirke⁵³ bzw. die Kassen(zahn)ärztliche Bundesvereinigungen als deren Dachorganisationen, §§ 77 ff. SGB V. Die Kassenärztlichen Vereinigungen kommen neben der Abrechnung (§ 295 SGB V) insbesondere im Rahmen ihres Prüfrechts hinsichtlich der Wirtschaftlichkeit der vertragsärztlichen Versorgung (§§ 106 f. SGB V) in Kontakt mit personenbezogenen Gesundheitsdaten.

Zu erwähnen sind ferner Ärztenetzwerke bzw. Gesundheitsnetze, die durch gezielte Optimierung und Kooperation von Leistungserbringern die Qualität und Wirtschaftlichkeit von Gesundheitsleistungen zu steigern anstreben.

Weiterhin ist zu beachten, dass personenbezogene Daten, gerade im Gesundheitswesen, häufig einen multipolaren (Personen-)Bezug aufweisen. So sind etwa diagnostische Einschätzungen und Protokollierungen eines behandelnden Arztes (Leistungserbringer) in einer bestimmten Patientenakte, die ihm (dem Arzt) zugeordnet werden können, auch personenbezogene Daten des Arztes selbst, weil sie Aussagen über ihn und seine Arbeitsweise enthalten, denen gegebenenfalls sogar haftungs- und strafrechtliche Relevanz zukommen kann.

d) Akteure auf Leistungsträgerseite

Die im vorliegenden Zusammenhang wichtigsten Leistungsträger sind zunächst die Träger der Krankenversicherung, also die Krankenkassen. Hier ist zu unterscheiden zwischen den – vorliegend relevanten – öffentlich-rechtlich organisierten gesetzlichen Krankenkassen (§ 4 SGB V) auf der einen Seite und den privaten Krankenkassen auf der anderen Seite.

Aber auch außerhalb des Bereichs der Krankenversicherung im engeren Sinne existieren zahlreiche öffentlich-rechtliche Leistungsträger wie die Berufsgenossenschaften als Träger der gesetzlichen Unfallversicherung (§ 114 SGB VII), ferner die für die Administration der Pflegeversicherung zuständigen Pflegekassen (§ 46 SGB XI) oder auch beispielsweise die Agenturen für Arbeit sowie die Gemeinden als kommunale Träger, soweit sie als Träger der Sozialhilfe gesundheitsrelevante Leistungen erbringen.

⁵³ Dies sind im Wesentlichen die einzelnen Bundesländer mit Ausnahme von Nordrhein-Westfalen, wo mit der Kassenärztlichen Vereinigung Nordrhein und der Kassenärztlichen Vereinigung Westfalen-Lippe zwei KVen bestehen.

Wie bei den Leistungserbringern bestehen auch auf Leistungsträgerseite zahlreiche Verbände auf regionaler wie auf Bundesebene, etwa die Landesverbände der Pflegekassen oder der Spitzenverband Bund der Krankenkassen.

Aus alledem wird deutlich, dass die im vorliegenden Zusammenhang potentiell beteiligten Akteure nicht nur äußerst vielfältig sind, sondern auch völlig unterschiedlichen Rechtsregimen unterfallen können, auch und gerade was ihren Umgang mit personenbezogenen Daten betrifft. Dies führt zu einer erheblichen rechtlichen Komplexität, die sorgfältige Abgrenzungs- und Strukturierungsarbeit erfordert.

3. Struktur und Zusammenspiel der gesetzlichen Regelungen im Gesundheitswesen, insbesondere im SGB V und SGB X

Das einfachgesetzliche Datenschutzrecht im Gesundheitswesen ist geprägt durch das Zusammenspiel einer Vielzahl von Gesetzen auf unterschiedlichen Ebenen.⁵⁴ Die Identifizierung der richtigen Rechtsgrundlage war bereits vor Einführung der DS-GVO teils keine leichte Aufgabe.⁵⁵ Denn neben verschiedenen allgemeinen und speziellen bundes- und landesrechtlichen Regelungen waren auch bisher schon immer Kirchen-, Straf- und Berufsrecht zu beachten. Durch das Hinzukommen einer zusätzlichen, unmittelbar geltenden unionalen Ebene hat sich diese Situation jedenfalls nicht verbessert, sondern die Komplexität ist tendenziell nochmals gestiegen.⁵⁶

⁵⁴ Vgl. ausführlich zum nachfolgenden Abschnitt *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 196 ff. sowie *Kühling*, MedR 2019, (im Erscheinen).

⁵⁵ Zur Kritik an der Komplexität siehe *Kingreen/Kühling*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 443; ebenso *Buchner*, in: Buchner (Hrsg.), Datenschutz im Gesundheitswesen (2018), Kap. A/2.4, S. 26.

⁵⁶ Vgl. *Buchner*, in: Buchner (Hrsg.), Datenschutz im Gesundheitswesen (2018), Kap. A/2, S. 1; *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 171.

a) DS-GVO: Ausgangspunkt mit weiten Öffnungsklauseln

Der DS-GVO kommt aufgrund ihres Ordnungscharakters nach Art. 288 Abs. 2 AEUV unmittelbare Geltung zu, weshalb sie den normativen Ausgangspunkt jeder datenschutzrechtlichen Betrachtung darstellt.⁵⁷ Dies gilt auch für den Gesundheitssektor und das Gesundheitswesen, weshalb der Rechtsanwender den ersten Blick stets in die DS-GVO werfen muss.⁵⁸ Die Besonderheit des gesamten Gesundheitssektors und damit auch des Gesundheitswesens stellen jedoch die unten noch näher zu erläuternden (dazu B. I. 1.), außerordentlich weit gefassten Öffnungsklauseln der DS-GVO für diesen Bereich dar, die einen großen mitgliedstaatlichen Spielraum eröffnen. Insofern gleicht die als hybride Handlungsform ausgestaltete DS-GVO im Gesundheitsbereich mehr einer Richtlinie und weniger einer Verordnung.⁵⁹ Die besonders umfassenden Öffnungsklauseln führen im Ergebnis zum Ausbleiben der materiellen Harmonisierungswirkung für das Datenschutzrecht des Gesundheitswesens, so dass größtenteils die ursprüngliche nationale Rechtslage aufrechterhalten wird (vertiefend dazu B. I. 1.).⁶⁰

b) Regelungsstruktur des allgemeinen Datenschutzrechts

Grundsätzlich beansprucht demnach im Gesundheitswesen auch nach dem Hinzutreten der DS-GVO das allgemeine nationale Datenschutzrecht Geltung. Dieses besteht in Deutschland wegen der zersplitterten Gesetzgebungskompetenz⁶¹ aus dem BDSG und den 16 Landesdatenschutzgesetzen (LDSG) der Länder, die jeweils im Zusammenhang mit der DS-GVO zu lesen sind und nur im Bereich der Öffnungsklauseln Wirkung entfalten können. Welches Gesetz einschlägig ist, richtet sich gemäß § 1 Abs. 1 BDSG nach der Art der datenverarbeitenden Stelle. Dabei wurde die – in der DS-GVO nicht angelegte – Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen aus dem „alten“ deutschen Datenschutzrecht beibehalten. Das BDSG ist nach § 1 Abs. 1 S. 2 anwendbar auf nicht-öffentliche Stellen, soweit diese automati-

⁵⁷ Vgl. Jülicher, *Medizininformationsrecht*, 2018, S. 82.

⁵⁸ Vgl. Kühling/Klar/Sackmann, *Datenschutzrecht*, 4. Aufl. 2018, Rn. 199; Kühling, *NJW* 2017, 1985, 1986; ebenso Buchner, in: Buchner (Hrsg.), *Datenschutz im Gesundheitswesen*, 2018, Kap. A/2.4.1, S. 26.

⁵⁹ Vgl. Kühling/Martini, *EuZW* 2016, 448, 454; Buchner/Schwichtenberg, *GuP* 2016, 218, 224; ebenso Kühnl/Rohrer/Schneider, *DuD* 2018, 735, 736.

⁶⁰ Vgl. auch Kühnl/Rohrer/Schneider, *DuD* 2018, 735, 737; Buchner, in: Buchner (Hrsg.), *Datenschutz im Gesundheitswesen* (2018), Kap. A/2.4.1, S. 26.

⁶¹ Vgl. hierzu Kircher, in: Kingreen/Kühling (Hrsg.), *Gesundheitsdatenschutzrecht*, 2015, S. 190 ff.; Kühling/Klar/Sackmann, *Datenschutzrecht*, 4. Aufl. 2018, Rn. 55 ff.

siert personenbezogene Daten verarbeiten oder in Dateisystemen speichern. Hierzu zählen beispielsweise privatrechtlich organisierte Leistungserbringer wie niedergelassene Ärzte.⁶² Daneben kommt das BDSG zur Anwendung auf öffentliche Stellen des Bundes. Die Verarbeitung von Gesundheitsdaten richtet sich hier grundlegend nach § 22 Abs. 1 BDSG, der die Öffnungsklauseln des Art. 9 DS-GVO ausfüllt. Im Umkehrschluss sind die LDSGe einschlägig bei einer Datenverarbeitung durch öffentliche Stellen der Länder.⁶³ Hier wird die Öffnungsklausel zur Verarbeitung von Gesundheitsdaten aus Art. 9 DS-GVO beispielsweise von Art. 8 BayDSG genutzt.

c) Subsidiarität des allgemeinen Datenschutzrechts: das Sozialdatenschutzrecht in SGB V und SGB X als bereichsspezifischer Gesundheitsdatenschutz des Bundes

Auf Bundesebene gibt es bereichsspezifische Datenschutznormen, die dem BDSG nach § 1 Abs. 2 S. 1 BDSG vorgehen. Hierunter fallen zunächst Regelungen wie das Transplantationsgesetz, das Gendiagnostikgesetz oder das Infektionsschutzgesetz, auch wenn es sich insoweit nicht mehr um Regelungen zum Gesundheitswesen im engeren Sinne handelt. Einen wichtigen Spezialfall im Gesundheitswesen bildet jedoch vor allem das vorliegend relevante Sozialdatenschutzrecht. Das allgemeine Sozialdatenschutzrecht ist geregelt in § 35 SGB I und in den §§ 67 bis 85a SGB X und gilt für alle Stellen, die in § 35 SGB V genannt sind. Rückgriffe auf das allgemeine Datenschutzrecht sollen insoweit nicht möglich sein, wie § 35 Abs. 2 S. 1 SGB I klarstellt.

Speziell für die gesetzlichen Krankenkassen gibt es bereichsspezifische sozialdatenschutzrechtliche Vorschriften in den §§ 284 ff. SGB V. § 284 Abs. 1 S. 1 Nrn. 1 bis 17 SGB V regelt dabei, für welche Zwecke die gesetzlichen Krankenkassen Sozialdaten erheben dürfen. Den abschließenden Charakter wird das Sozialdatenschutzrecht zumindest gegenüber dem nationalen allgemeinen Datenschutzrecht im BDSG dank der umfangreichen Öffnungsklauseln wohl

⁶² Diese sind auch soweit sie innerhalb der gesetzlichen Krankenkassen als Leistungserbringer tätig werden keinesfalls als öffentliche Stellen zu qualifizieren, so zutreffenden *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 200.

⁶³ Siehe exemplarisch Art. 1 Abs. 1 S. 1 BayDSG.

weitestgehend auch unter der DS-GVO fortführen.⁶⁴ Einzig die Regelungen der DS-GVO selbst gehen dem Sozialdatenschutzrecht wegen des Anwendungsvorrangs des EU-Rechts (und dem klarstellenden Verweis hierauf in § 35 Abs. 2 S. 1 SGB I) vor.

d) Abrechnung der Leistungserbringer als datenschutzrechtliches Kernstrukturelement im SGB V

Im Gesundheitswesen ist – wie soeben skizziert (siehe A. III. 2. a)) – zwischen den Leistungserbringern auf der einen und den Leistungsträgern auf der anderen Seite zu differenzieren.⁶⁵ Für die Leistungserbringer in der Behandlungssituation gilt grundsätzlich das allgemeine Datenschutzrecht. Für die Leistungsträger bildet das Sozialdatenschutzrecht den Ausgangspunkt. Weitere bereichsspezifische Sonderregelungen können in beiden Rechtsgebieten vorrangig sein.

Für die Leistungserbringer (vgl. oben III. 2. c)) – allen voran die Ärzte – ist das allgemeine Sozialdatenschutzrecht aus SGB I und SGB X in der Behandlungssituation grundsätzlich nicht anwendbar. Ob das BDSG, ein LDSG oder eine bereichsspezifische Norm jeweils i.V.m. der DS-GVO einschlägig ist, richtet sich im Wesentlichen nach der Identität des Leistungserbringers. Auch die konkrete Verarbeitungssituation oder der Zweck können eine Rolle spielen.

So gibt es etwa für die Kommunikation innerhalb der kassenärztlichen Versorgung, z.B. zwischen Hausarzt und Facharzt, mit § 73 Abs. 1b SGB V eine spezielle Regelung, die jedoch auch eine Einwilligung fordert. Für die Aufzeichnung und Weitergabe von Leistungsdaten an die Krankenkassen zur Abrechnung ergeben sich aus den §§ 295 f. SGB V besondere Befugnisse.⁶⁶ Innerhalb der Regelversorgung übermitteln die Ärzte nach § 295 Abs. 1 SGB V die Leistungsdaten an die jeweilige Kassenärztliche Vereinigung. Diese wiederum übermitteln auf Grundlage von § 295 Abs. 2 SGB V die dort aufgezählten Leistungsdaten an die Krankenkassen.

⁶⁴ So auch *Buchner/Schwichtenberg*, GuP 2016, 218, 223; *Kühnl/Rohrer/Schneider*, DuD 2018, 735, 738; differenzierend *Weichert*, DuD 2017, 538, 542, der danach unterscheidet, ob materiell-rechtliche Zulässigkeitsvoraussetzungen oder bereichsspezifische Garantien vorliegen. Nur bei letzteren soll das Sozialdatenschutzrecht dem BDSG vorgehen.

⁶⁵ Vgl. hierzu und zum nachfolgenden Abschnitt ausführlich *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 216 ff.

⁶⁶ Siehe hierzu *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 233 ff.

Für sonstige Leistungserbringer ist ebenfalls auf die DS-GVO und das BDSG abzustellen, soweit nicht bei der Abrechnung speziellere Normen aus dem SGB V greifen. Für die Abrechnung bei Apothekern folgen beispielsweise aus § 300 SGB V einige spezielle Vorgaben,⁶⁷ bei Hebammen greift § 301a SGB V und schreibt vor, welche Daten an die Krankenkassen zu übermitteln sind.⁶⁸

Spezielle Regelungen für die im Rahmen der Abrechnung an die Krankenkassen zu übertragenden Daten ergeben sich für die Krankenhäuser aus § 301 SGB V für den Regelfall der stationären Behandlung oder aus § 295a Abs. 3 SGB V für im Notfall erbrachte ambulante Leistungen.⁶⁹

e) Das Sozialdatenschutzrecht der Leistungsträger in den SGB I, X und V

Das allgemeine Sozialdatenschutzrecht nach § 35 SGB I und den §§ 67 bis 85a SGB X entfaltet seine Wirkung im Bereich der Öffnungsklausel der DS-GVO für alle Leistungsträger und Stellen i.S.d. § 35 Abs. 1 SGB I. Relevant ist dies im Bereich des Gesundheitswesens insbesondere für Unfallversicherungsträger oder Pflegekassen. Zulässigkeitstatbestände für Verarbeitung von Sozialdaten ergeben sich im allgemeinen Sozialdatenschutzrecht aus den §§ 67a ff. SGB X.

Für die gesetzlichen Krankenkassen gilt das bereichsspezifische Sozialdatenschutzrecht der §§ 284 ff. SGB V i.V.m. der DS-GVO.⁷⁰ § 284 Abs. 1 und Abs. 2 SGB V regeln dabei, für welche Zwecke Sozialdaten erhoben werden dürfen. Eine weitergehende Verarbeitung darf gemäß § 284 Abs. 3 SGB V grundsätzlich nur zu eben diesem Zweck und im Rahmen der Erforderlichkeit erfolgen.⁷¹ Zweckänderungen sind nach dem ausdrücklichen Wortlaut des § 284 Abs. 3 SGB V nur aufgrund ausdrücklicher gesetzlicher Ermächtigungen im SGB möglich.

Für private Krankenversicherungsunternehmen gilt das Sozialdatenschutzrecht dagegen nicht. Es kommt stattdessen das allgemeine Datenschutzrecht zur Anwendung, ergänzt durch einige

⁶⁷ Vgl. hierzu *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 245 ff.

⁶⁸ Vgl. hierzu *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 248.

⁶⁹ *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 249 f.

⁷⁰ Vgl. *Buchner*, in: Buchner (Hrsg.), Datenschutz im Gesundheitswesen, 2018, Kap. A/2.2.1, S. 11.

⁷¹ Vgl. *Kircher*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 260.

spezialgesetzliche Bestimmungen im VVG oder GenDG⁷², was nicht Gegenstand der vorliegenden Untersuchung ist.

IV. Konsequenzen für den Fortgang der Untersuchung

Vor diesem Hintergrund untersucht das vorliegende Rechtsgutachten den Regelungsrahmen für Big-Data-Anwendungen auf verschiedenen Ebenen: Insbesondere anlässlich der Vorschläge des Deutschen Ethikrates wird auf einer sehr prinzipiellen „Meta-Ebene“ danach gefragt, ob es einer fundamentalen Neuausrichtung des (Gesundheits-)Datenschutzrechts im Zeitalter von Big-Data-Anwendungen bedarf. Konkret wird dies mit Blick auf die Datenminimierung (dazu B. I. 3. a), C. IV. 1. und D. III. 2.) und Zweckbindung (dazu B. I. 3. b), C. IV. 2. und D. III. 3.) als zentralen Kategorien des Datenschutzrechts sowie dem Vorschlag einer stärkeren Orientierung an einer „Datensouveränität“ (dazu C. IV. 4. und D. III. 1.) durchgespielt. Auf einer deutlich spezifischeren normativen Ebene werden einzelne für den Datenschutz und Big-Data-Anwendungen im Gesundheitswesen zentrale Paragraphen des SGB V und SGB X auf ihre Zweckmäßigkeit hin betrachtet. Schließlich werden, gleichsam auf einer „Micro-Ebene“, dabei auch sehr genaue Untersuchungen zur spezifischen Funktionsweise der Normen angestellt (zu beidem siehe B. II. und III.). Daraus werden sodann auch jeweils mögliche Änderungsvorschläge *de lege ferenda* entwickelt (dazu C. III. und D. IV.). Auf der Detailebene wird auch umfassend die Idee einer Datenspende geprüft und normativ verortet (dazu B. IV. 1., C. IV. 3. und D. III. 4.). Nicht weiter nachgegangen werden gleichsam auf einer „Mezzo-Ebene“ angesiedelte systematische Fragen, ob und wie das Datenschutzrecht im Gesundheitswesen durch eine grundlegende Neustrukturierung der relevanten Normen im SGB V und SGB X verbessert werden könnte bzw. ob und inwiefern gegebenenfalls der Detaillierungsgrad der Regelungen zurückgefahren werden sollte.

⁷² Vgl. Washausen, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 406.

B. Handlungsmöglichkeiten im Rahmen des geltenden Rechts

Im Folgenden sollen die Handlungsmöglichkeiten analysiert und dargestellt werden, die der gegenwärtige Rechtsrahmen ohne legislative Anpassungen für Big-Data-Anwendungen im Gesundheitswesen bietet. Dazu sind zunächst die Steuerungsvorgaben der DS-GVO als zentrale Regelungsordnung des Datenschutzrechts für das Gesundheitswesen zu erläutern (dazu I.), bevor auf der Ebene des nationalen Rechts, die jene normative Vorgaben ausfüllenden Bestimmungen in den §§ 303a ff. SGB V als Schwerpunkt der vorliegenden Untersuchung zu betrachten sind (dazu II.). In einem dritten Schritt können eine Reihe gegenwärtig besonders problematischer Einzelfragen vertieft werden (dazu III.). Schließlich sind vor diesem Hintergrund die Konsequenzen für die Kritikpunkte des Deutschen Ethikrates de lege lata zu ziehen (dazu IV.).

I. Vorgaben und Steuerungswirkung der DS-GVO für das Gesundheitswesen

Die DS-GVO als zentrales Normenwerk im Datenschutzrecht setzt auch für den Gesundheitssektor die wesentlichen Leitplanken. Der Harmonisierungsanspruch der Verordnung wird aber durch die zahlreichen Öffnungsklauseln gerade für das Gesundheitswesen deutlich relativiert (dazu 1.). Von allgemeiner Bedeutung für alle datenschutzrechtlichen Felder und damit auch für das Gesundheitswesen sind jedoch die Regelung des Anwendungsbereichs des Datenschutzrechts (personenbezogene Daten einschließlich pseudonymer, nicht aber anonymer Daten; dazu 2.) und der zentralen Steuerungskonzepte wie der Datensparsamkeit bzw. Datenminimierung, der Zweckbestimmung bzw. -begrenzung, der Erforderlichkeit der Datenverarbeitung und der Möglichkeiten und Grenzen einer Einwilligung (dazu 3.).

1. Harmonisierungsanspruch und Öffnungsklauseln in der DS-GVO im Detail

a) Begrenzte Harmonisierungswirkung angesichts zahlreicher Öffnungsklauseln

Fast die Hälfte der Bestimmungen der DS-GVO verfügen über Öffnungsklauseln, die eine Konkretisierung oder Ergänzung auf nationaler Ebene eröffnen (fakultative Öffnungsklauseln) oder gar erfordern (obligatorische Öffnungsklauseln). Teilweise beziehen sich diese Klauseln nicht bloß auf einzelne Bestimmungen der DS-GVO, sondern wirken gleichsam horizontal wie

die weit gefassten Klauseln in der Kernbestimmung zur Rechtmäßigkeit der Verarbeitung in Art. 6 DS-GVO.⁷³

b) Art. 9 DS-GVO mit umfassenden Öffnungsklauseln für das Gesundheitswesen

Gerade im Gesundheitswesen, in dem es um die Verarbeitung von Gesundheitsdaten und damit um eine besondere Kategorie personenbezogener Daten geht, greifen Öffnungsklauseln mit weit reichenden Konkretisierungs- und Ausdifferenzierungsmöglichkeiten auf nationaler Ebene. Besonders wichtig sind dabei die Öffnungsklauseln in Art. 9 DS-GVO.⁷⁴ Diese normieren einen strengeren Rechtfertigungsstandard für die Verarbeitung einzelner Datenkategorien, die als besonders sensibel eingestuft werden.⁷⁵ Das sind u.a. Daten, die sich auf die Gesundheit beziehen (s.o. A. III. 1. a)). In Ergänzung zu den bisherigen Kategorien der Richtlinie 95/46/EG (DSRL) sind zusätzlich die Fälle der genetischen Daten und der biometrischen Daten, die eine spezifische Person identifizieren können, aufgenommen worden. Die letztgenannte Kategorie ist erst im Rahmen des Parlamentsbeschlusses vom 12. März 2014 in den Text eingefügt worden.⁷⁶ Für all jene Daten gilt im Grundsatz, dass jegliche Datenverarbeitung verboten ist, Art. 9 Abs. 1 DS-GVO, selbst wenn ein allgemeiner Rechtfertigungstatbestand vorliegt. Dieses Verbot gilt nach Art. 9 Abs. 2 DS-GVO nicht, sofern verschiedene Voraussetzungen vorliegen. Diese sind vollharmonisiert, eröffnen aber Abweichungsmöglichkeiten. Sie betreffen neben dem für das Gesundheitswesen durchaus bedeutsamen Fall der Einwilligung der betroffenen Person (lit. a) vorliegend relevant vor allem den Bereich des Gesundheitsschutzes im weitesten Sinne (lit. h, i). Ergänzend sind auch die Öffnungsklauseln bei Datenverarbeitungen zur Erfüllung bestimmter Pflichten im Bereich der sozialen Sicherheit und des Sozialschutzes (lit. b), aus Gründen eines gewichtigen öffentlichen Interesses (lit. g) sowie im Forschungs- und Statistikbereich (lit. j i.V.m. Art. 89 DS-GVO) zu beachten. Eine besonders weit gefasste Öffnungsklausel für die Verarbeitung von genetischen, biometrischen und Gesundheitsdaten bildet zudem Art. 9 Abs. 4 DS-GVO.

⁷³ Zu diesen Unterscheidungen *Kühling/Martini*, EuZW 2016, 448; zum Folgenden bereits ausführlich *Kühling*, Datenschutz im Gesundheitswesen, MedR 2019 (im Erscheinen) .

⁷⁴ Die Ausführungen im folgenden Abschnitt gehen zurück auf *Kühling/Martini u.a.*, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, S. 47 ff.

⁷⁵ Vgl. dazu *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 7.

⁷⁶ *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 9 DS-GVO, Rn. 9.

Die bedeutsamste Änderung dieser Norm im Vergleich zum Kommissionsentwurf ist gerade hier erfolgt, da im Kommissionsentwurf der dortige Art. 81 DS-GVO-E noch eine strenge Überformung des nationalen Gesundheitsdatenschutzrechtssystems vorgesehen hatte.

Art. 9 DS-GVO enthält gemischte Öffnungsklauseln, die einerseits in bestimmte Sektoren (Sozialdatenschutz; Gesundheitsdatenschutz) ausstrahlen. Andererseits sind sie, angesichts der Breite und Relevanz besonderer Datenkategorien, jedoch letztlich von erheblicher und tendenziell horizontaler Bedeutung. Da die Norm keine Konkretisierung erfordert, sondern lediglich Abweichungsmöglichkeiten vorsieht, handelt es sich um fakultative Öffnungsklauseln.⁷⁷ Ein Handlungsbedürfnis auf nationaler Ebene ist daher nur indiziert, wenn der nationale Gesetzgeber die Anforderungen an die Verarbeitung besonderer Datenkategorien verschärfen, erleichtern oder modifizieren möchte. Dabei sind sowohl horizontale Regelungen für alle Kategorien besonderer Daten möglich (wie etwa mit Blick auf die Einwilligung), als auch Bestimmungen in einzelnen Sektoren wie dem Gesundheitsdatenschutz. Adressat der Regelung sind sowohl öffentliche als auch nicht-öffentliche Stellen in der überkommenen deutschen datenschutzrechtlichen Differenzierung, da besondere Datenkategorien durch sämtliche Verantwortliche verarbeitet werden.

c) Besonderheiten mit Blick auf die Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO

Art. 9 Abs. 2 lit. a DS-GVO verlangt für die Ausnahme bei sensiblen Daten eine „ausdrückliche“ Einwilligung. Art. 9 Abs. 2 lit. a DS-GVO formuliert jedoch eine Rückausnahme von der Möglichkeit, das Verarbeitungsverbot durch Einwilligung einzuschränken. Sie räumt den Mitgliedstaaten die Befugnis ein, die Verarbeitung trotz Vorliegens einer ausdrücklichen Einwilligung durch Gesetz zu untersagen.⁷⁸ Eine weitere Konditionierung der Voraussetzungen, um diese Rückausnahme zu aktivieren, nimmt die Verordnung nicht vor. Die Mitgliedstaaten sind daher grundsätzlich vollkommen frei, von dieser Regelungsoption Gebrauch zu machen. Beachten müssen sie jedoch grundrechtliche Grenzen – insbesondere mit Blick auf die informationelle Selbstbestimmung, die in einer Einwilligung Ausdruck findet. Bereichsspezifische Regelungen lassen sich damit im deutschen Recht ebenso aufrechterhalten wie allgemeine, horizontale Einschränkungen der Einwilligung.⁷⁹ Im Übrigen sind auch weitere Konkretisierungen

⁷⁷ Zu den Öffnungsklauseln des Art. 9 DS-GVO siehe auch *Kühnl/Rohrer/Schneider*, DuD 2018, 735.

⁷⁸ Vgl. dazu *Weichert*, in: Kühling/Buchner (Hrsg.), 2. Aufl. 2018, Art. 9 Rn. 48.

⁷⁹ Hierzu bereits *Kühling/Martini u.a.*, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, S. 55.

des Anforderungsprofils an Einwilligungen im nationalen Recht denkbar. Dies ist mit Blick auf zahlreiche bereichsspezifische Regelungen im Gesundheitsdatenschutzrecht relevant, wenn etwa in § 8 Abs. 1 GenDG nicht nur eine ausdrückliche, sondern auch eine „schriftliche“ Einwilligung vor Durchführung einer genetischen Untersuchung oder Analyse verlangt wird.

Insoweit spricht die den Mitgliedstaaten eingeräumte weitreichende und unkonditionierte Konkretisierungs- und Ausschlussbefugnis der Einwilligung in Bezug auf sensible Daten dafür, dass auch eine Verschärfung der Anforderungen an die Einwilligung in spezifischen Verwendungssituationen der Daten abgedeckt ist. Das ist zwar im Wortlaut der Öffnungsklausel nicht zwingend angelegt, ergibt sich aber als Minus angesichts der weitgehenden mitgliedstaatlichen Gestaltungsbefugnis. Zudem ermöglicht Art. 9 Abs. 4 DS-GVO zumindest für genetische, biometrische und Gesundheitsdaten ohnehin die Schaffung zusätzlicher Bedingungen, einschließlich Beschränkungen, was selbst bei einem engeren Verständnis des Art. 9 Abs. 2 lit. a DS-GVO Konkretisierungen bei der Einwilligung zulassen würde.

d) Öffnungsklausel für die Datenverarbeitung im Gesundheitswesen insbesondere in Art. 9 Abs. 2 lit. h DS-GVO

Vorliegend besonders relevant ist sodann jedoch die Öffnungsklausel des Art. 9 Abs. 2 lit. h DS-GVO einschließlich der korrespondierenden Erwägungsgründe 52 und 53 DS-GVO. Danach können Mitgliedstaaten die Verarbeitung zu Zwecken u. a. der medizinischen Diagnose oder zum Zwecke des Managements von Gesundheits- oder Sozialfürsorgesystemen im Gesetzeswege näher in ihrer Zulässigkeit ausgestalten. Art. 9 Abs. 3 DS-GVO lässt die Verarbeitung besonderer Daten insoweit allerdings zu Zwecken des Art. 9 Abs. 2 lit. h DS-GVO nur zu, sofern der Verarbeiter ein Berufsheimnisträger ist. Letzteres kann sich auch nach dem mitgliedstaatlichen Recht richten. Damit wird die Ausgestaltungsbefugnis *ratione personae* erheblich eingeschränkt und auf entsprechendes Fachpersonal beschränkt.⁸⁰

Ähnliches gilt für Art. 9 Abs. 2 lit. i mit Erwägungsgrund 54 DS-GVO, der eine strukturell vergleichbare Öffnungsklausel für die Verarbeitung im Bereich der öffentlichen Gesundheit insgesamt vorsieht, ohne allerdings eine derartige Einschränkung *ratione personae* vorzunehmen. Der Begriff der öffentlichen Gesundheit ist dabei weit zu verstehen, wie Erwägungsgrund 54 S. 3 DS-GVO deutlich macht:

⁸⁰ So bereits *Kühling/Martini u.a.*, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, S. 51.

„In diesem Zusammenhang sollte der Begriff ‚öffentliche Gesundheit‘ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen.“

Lediglich geringfügig einschränkend ergänzt Erwägungsgrund 54 S. 4 DS-GVO:

„Eine solche Verarbeitung personenbezogener Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber, Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.“⁸¹

Art. 9 Abs. 4 DS-GVO (ergänzt durch die letzten beiden Sätze des Erwägungsgrundes 54 der DS-GVO) eröffnet den Mitgliedstaaten schließlich die Möglichkeit, weitere Voraussetzungen einschließlich weiterer Beschränkungen – aber eben auch Zulässigkeitstatbeständen, Modifikationen etc. – für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten national zu regeln.

Damit erlangen die Mitgliedstaaten letztlich eine faktisch weitreichende Freiheit, die Datenverarbeitung im Bereich der Gesundheit und Sozialfürsorge eigenständig zu gestalten und die Vorgaben der DS-GVO insoweit zu konkretisieren, aber auch zu modifizieren im Sinne einer Verschärfung oder Erleichterung. Dabei sieht die DS-GVO auch – anders als noch der ursprünglich vorgesehene Art. 81 im Kommissionsentwurf, bestätigt im Parlamentsentwurf – keine Konditionierung dieser Gestaltungsbefugnis vor. Der Verweis auf die angemessenen Grundrechtsgarantien in Art. 9 Abs. 2 lit. i DS-GVO einschließlich der Wahrung des Berufsgeheimnisses und des Erforderlichkeitsgrundsatzes ist insoweit wenig limitierend. Denn diese

⁸¹ Angelehnt an Kühling/Martini u.a., Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, S. 51 f.

Gehalte sind ohnehin in Deutschland durch die verfassungsrechtlichen Vorgaben indiziert, die durch das Datenschutzgrundrecht der Grundrechtecharta in Art. 8 GRCh ergänzt werden.⁸²

e) **Zwischenfazit: nationaler Flickenteppich statt unionaler Vollharmonisierung**

Der ursprüngliche Harmonisierungsansatz der Europäischen Kommission ist damit für das Gesundheitswesen auf den Kopf gestellt: Das Konzept einer umfassenden Vollharmonisierung im Rahmen einer Verordnung mit zahlreichen normativen Konkretisierungsmöglichkeiten durch die Kommission im Wege delegierter Rechts- und Durchführungsrechtsakte ist mutiert zu einer weitreichenden Ausgestaltungsmöglichkeit bloß rudimentärer unionsrechtlicher Vorgaben durch den nationalen Gesetzgeber. In der Folge bleibt es bei einem nationalen Flickenteppich, der im deutschen Recht besonders bunt und eng gewebt ist (dazu bereits oben A. III. 2.). Die Hoffnungen von 2015 auf eine umfassende unionsweite Harmonisierung und in der Folge auch Vereinfachung und „Harmonisierung“ auf nationaler Ebene haben sich damit gerade im Gesundheitsdatenschutzrecht in besonderem Maße zerschlagen.⁸³ Vor dem Hintergrund dieses komplexen Zusammenspiels aus nationalem Recht und dem der DS-GVO einschließlich ihrer Öffnungsklauseln sind sodann die weiteren Reformvorschläge in Bezug auf das SGB V und SGB X zu entwickeln.

2. **Sachlicher Anwendungsbereich der Datenschutzordnung**

Das Datenschutzrecht schützt die Privatsphäre von natürlichen Personen. Es ist daher nur anwendbar, soweit es um Daten geht, die sich auf die betroffene Person beziehen (dazu a)), einschließlich pseudonymer, nicht aber anonymer Daten (zur Abgrenzung b)). Die Identifizierung der Handlungsmöglichkeiten im Rahmen der geltenden Datenschutzordnung erfordert zunächst eine Klärung des insoweit eröffneten sachlichen Anwendungsbereichs des Datenschutzrechts.⁸⁴ Dies ist auch vorliegend relevant, da diese Ansätze grundsätzlich für das Datenschutzrecht im SGB V und SGV X gelten.

⁸² Kühling/Martini u.a., Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016, S. 52.

⁸³ Siehe dazu auch Kühnl/Rohrer/Schneider, DuD 2018, 735, 740.

⁸⁴ Die folgenden Ausführungen sind stark orientiert an Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 248 ff.

a) Personenbezogene Daten

Zentrales Schutzobjekt der DS-GVO ist das personenbezogene Datum. Der Anwendungsbereich und die Schutzfunktion der DS-GVO sind nur dann eröffnet und einschlägig, wenn es sich bei den betreffenden Daten um personenbezogene Daten handelt. Hierunter sind nur solche Informationen, die sich auf eine natürliche Person beziehen, zu verstehen. Die DS-GVO nennt diese „betroffene Person“.

Art. 4 Nr. 1 DS-GVO umfasst ohne Einschränkung „alle Informationen“, die sich auf eine Person beziehen und ist daher grundsätzlich weit zu verstehen. Unter die Vorschrift fallen sowohl im Kontext verwendete persönliche Informationen wie Identifikationsmerkmale (z.B. Name, Anschrift und Geburtsdatum), äußere Merkmale (wie Geschlecht, Augenfarbe, Größe und Gewicht, Behinderungen) oder innere Zustände (vorliegend insbesondere der psychische Gesundheitszustand) als auch sachliche Informationen wie etwa Verwandtschaftsverhältnisse, Versicherungseigenschaft und Vertragsbeziehungen sowie alle sonstigen Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt.

Die Informationen müssen sich auf eine identifizierte oder identifizierbare Person beziehen. Ob die betreffende Person identifiziert oder lediglich identifizierbar ist, spielt in rechtlicher Hinsicht keine Rolle, da hieran jeweils keine unterschiedlichen gesetzlichen Voraussetzungen geknüpft werden. Bei einer Interessenabwägung (z.B. im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO) kann dieser Umstand gegebenenfalls aber von Bedeutung sein.

Wann eine Person i.S.d. Art. 4 Nr. 1 „identifiziert“ ist, wird in der DS-GVO nicht näher erläutert. Von einer identifizierten Person ist auszugehen, wenn die Identität der Person unmittelbar aus der Information selbst folgt.⁸⁵ Das ist beispielsweise der Fall, wenn die Information ein Identifikationsmerkmal (z.B. Name, Anschrift und Geburtsdatum) der Person beinhaltet oder wenn der Inhalt der Information oder der Kontext eine eindeutige Identifikation erlaubt, ohne dass auf weitere Informationen zurückgegriffen werden muss.

Dagegen ist eine Person identifizierbar, wenn die Information zwar für sich genommen nicht ausreicht, um sie einer Person zuzuordnen, dies aber gelingt, sobald die Information mit weiteren Informationen, die für den Verantwortlichen verfügbar sind, verknüpft wird.⁸⁶ So bestimmt Art. 4 Nr. 1 DS-GVO, dass eine Person dann identifizierbar ist, wenn sie direkt oder

⁸⁵ EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 38 – Breyer = ZD 2016, 24 m. Anm. Kühling/Klar.

⁸⁶ Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 Rn. 19.

indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Nach Erwägungsgrund 26 der DS-GVO sind bei der Frage, ob eine Person identifizierbar ist, alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Frage, welche Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, sind nach Erwägungsgrund 26 der DS-GVO alle über die betreffende Person bekannten oder ermittelbaren Informationen sowie alle objektiven Faktoren heranzuziehen, wie z.B. die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand. Inwieweit auch das Wissen und die Mittel Dritter zu berücksichtigen sind, die diese zur Identifizierung einer Person verwenden können, ist umstritten. Die Problematik betrifft die Frage, ob es bei der Herstellbarkeit des Personenbezugs auf den jeweils Verantwortlichen ankommt (relativer Personenbezug) oder ob es ausreicht, dass irgendein Dritter einen Personenbezug herstellen kann (absoluter Personenbezug). Zwischen beiden Extrempositionen findet sich eine Reihe von Mischformen.⁸⁷ Der EuGH hat im Zusammenhang mit dem Personenbezug von IP-Adressen erste richtungsweisende Ausführungen dazu gemacht, welche Anforderungen an die Berücksichtigung des Wissens und der Mittel Dritter zu stellen sind.⁸⁸ Danach ist ein Personenbezug zu bejahen, wenn der Verantwortliche über rechtliche Mittel verfügt, um sich die Daten des Dritten verfügbar zu machen.⁸⁹ Dabei soll unerheblich sein, ob dies über den Umweg staatlicher Behörden erfolgt. Nach Ansicht des EuGH sollen gesetzlich verbotene Möglichkeiten außer Betracht bleiben, da sie regelmäßig nicht „vernünftigerweise“ i.S.v. Erwägungsgrund 26 der DSRL – bzw. übertragen auf Erwägungsgrund 26 der DS-GVO nicht „nach allgemeinem Ermessen wahrscheinlich“ – zur Bestimmung der betreffenden Person eingesetzt werden.⁹⁰ Der BGH hat sich dieser Auffassung angeschlossen.⁹¹

⁸⁷ Dazu *Bergt*, ZD 2015, 365 ff.

⁸⁸ EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 31 ff. – Breyer = ZD 2016, 24 m. Anm. *Kühling/Klar*.

⁸⁹ Vgl. EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 47 ff. – Breyer = ZD 2016, 24 m. Anm. *Kühling/Klar*.

⁹⁰ EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – Breyer = ZD 2016, 24 m. Anm. *Kühling/Klar*.

⁹¹ BGH, Urt. v. 16.5.2017, VI ZR 135/13 = MMR 2017, 605, Rn. 26.

Juristische Personen sowie Personenmehrheiten und -gruppen sind aus dem Schutzbereich ausgenommen. Soweit Informationen über die Personengruppe aber auf ein identifiziertes oder identifizierbares Mitglied „durchschlagen“, handelt es sich bei der Information um ein personenbezogenes Datum.⁹² Dies kann etwa der Fall sein, wenn eine Angabe zur finanziellen Situation einer als Personen- oder Kapitalgesellschaft organisierten Arztpraxis oder einer sonstigen Gesundheitseinrichtung gemacht wird und der Namen einer Gesellschaft auf einen oder mehrere natürliche Personen hinweist („Stadt-Apotheke Ludwig und Helma Schmidt e.K.“ oder „Hausarztpraxis Dr. med. Heinz Huber“ oder „Privatklinik Prof. Dr. med. Simon Meier GmbH“).

Im Gesundheitswesen kann vor diesem Hintergrund insbesondere auch das Institutionskennzeichen (IK-Nummer) zur Abrechnung mit den gesetzlichen Krankenkassen im Regelfall als personenbezogenes Datum klassifiziert werden. Das „personale Substrat“ hinter dem Leistungserbringer, der in unterschiedlichen Rechtsformen organisiert sein kann, ist stets zumindest der konkret behandelnde Arzt. Der behandelnde Arzt ist anhand des Institutionskennzeichens auch ermittelbar, da der Zugriff auf die Unterlagen des Leistungserbringers für die Krankenkassen rechtlich möglich ist (etwa im Zuge von Einzelfallprüfungen) und die Identifizierbarkeit des behandelnden Arztes nicht de facto ausgeschlossen erscheint.⁹³ Man könnte insoweit bei Leistungserbringern, die als größere Einheit organisiert sind (etwa ein Krankenhaus oder eine sehr große Arztpraxis), für Dritte, die keine Kontrollbefugnisse und damit rechtlich keinen Zugriff auf die Behandlungsunterlagen erhalten können, annehmen, dass nach dem relativen Personenbezugsbegriff insoweit nicht-personenbezogene Daten vorliegen würden. Im Interesse eines effektiven Privatsphärenschutzes ist jedoch von einem weiten Personenbezugsbegriff auszugehen und auch die nur theoretische rechtliche Möglichkeit einer Zuordnung zu einer konkreten Person zu berücksichtigen. Im Zuge etwa eines Strafverfahrens und einem anschließenden Akteneinsichtsgesuch hat jedoch letztlich theoretisch jeder Dritte die nicht völlig fernliegende rechtliche Möglichkeit, einen personalen Bezug zu den hinter dem Leistungsträger stehenden Personen und den dort behandelnden Ärzten Zugriff zu erlangen. Im Ergebnis müssen Institutionskennzeichen und mit diesem verknüpfte Daten also als personenbeziehbare Daten behandelt werden.

⁹² So noch zur DSRL *Art.-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 20.6.2007, S. 27; im Rahmen des BDSG a.F. *Dammann*, in: Simitis (Hrsg.), Kommentar zum BDSG, 8. Aufl. 2014, § 3 Rn. 19.

⁹³ Vgl. dazu EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – Breyer.

b) Anonyme und pseudonyme Daten

aa) Anonyme Informationen

In engem Zusammenhang mit dem Begriff des personenbezogenen Datums steht der Begriff der anonymen Information. Nach Erwägungsgrund 26 der DS-GVO gelten die Grundsätze des Datenschutzrechts nicht für anonyme Informationen, d.h. für Informationen, die sich (von vornherein) nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die (nachträglich) in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.⁹⁴

Durch die Formulierung macht der Verordnungsgeber deutlich, dass das anonyme Datum die Kehrseite des personenbezogenen Datums darstellt und ein Datum entweder personenbezogen oder anonym ist.⁹⁵ Anonyme Daten weisen also keinen Personenbezug auf. Ob eine natürliche Person nicht (mehr) identifizierbar und das Datum damit anonym ist, ist nach Maßgabe des Erwägungsgrundes 26 der DS-GVO zu prüfen, d.h. es sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, wobei insbesondere die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand zu berücksichtigen sind. Das bedeutet, dass bei der Frage, ob ein Datum anonym ist oder nicht, eine Risikobewertung zu erfolgen hat, inwieweit es zu einer Identifizierung kommen kann.⁹⁶

Die Verordnung macht keine technischen Vorgaben dazu, welche Anforderungen an eine Anonymisierung zu stellen sind. Erwägungsgrund 26 der DS-GVO bestimmt jedoch, dass im Rahmen der Feststellung der Identifizierbarkeit einer Person die zum Zeitpunkt der Verarbeitung jeweils verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Daraus folgt, dass eingesetzte Anonymisierungsverfahren zumindest dem aktuellen Stand der Technik entsprechen müssen.

Als Verfahren der Anonymisierung kommen in der Praxis eine Löschung von identifizierenden Merkmalen (z.B. Name, Anschrift, Kontodaten), eine Aggregation von Daten, die Bildung von Gruppen bzw. die kontrollierte Einbringung von Zufallsfehlern in Betracht.⁹⁷

⁹⁴ Ausführlich *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 Rn. 31 ff.

⁹⁵ Ebenso *Karg*, DuD 2015, 520, 523.

⁹⁶ Vgl. *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, Art. 4 Nr. 1 Rn. 22; und bereits *Klar/Kühling*; NJW 2013, 3611, 3613.

⁹⁷ Ausführlich *Art.-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 10.4.2014; *Schefzig*, K&R 2014, 772, 776.

bb) Pseudonymisierung

Auch der Begriff der Pseudonymisierung nach Art. 4 Nr. 5 DS-GVO ist im Zusammenhang mit personenbezogenen Daten von Bedeutung. Eine Pseudonymisierung bietet sich in der Praxis immer dann an, wenn die jederzeitige Kenntnis der Identität einer Person verzichtbar ist, die Daten jedoch gleichzeitig unter bestimmten Bedingungen mit einer konkreten Person verknüpfbar bleiben sollen. Charakteristisch für pseudonyme Daten – im Unterschied zu anonymen Daten – ist das Bestehen einer Zuordnungsregel, die den unter einem Pseudonym erfassten Daten ein Identifikationsmerkmal einer Person zuweist. Eine Pseudonymisierung stellt daher keine Anonymisierung, sondern – wie Art. 32 Abs. 1 lit. a DS-GVO verdeutlicht – eine bloße Sicherungsmaßnahme dar.⁹⁸ Das Ziel der Pseudonymisierung besteht nach Erwägungsgrund 28 der DS-GVO darin, die Risiken für betroffene Personen zu senken und den Verantwortlichen und Auftragsverarbeiter bei der Einhaltung der Datenschutzpflichten zu unterstützen.

Die DS-GVO definiert in Art. 4 Nr. 5 DS-GVO das Pseudonymisieren als die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzufügung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. In Abgrenzung zur Anonymisierung sind die zusätzlichen Informationen aber nicht zu löschen, sondern zu ersetzen und gesondert aufzubewahren. Die personenbezogenen Daten sind zudem besonderen technischen und organisatorischen Maßnahmen zu unterwerfen, die gewährleisten, dass die Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. In Betracht kommen insoweit die Maßnahmen nach Art. 32 DS-GVO. Diese müssen sicherstellen, dass der Nutzer der pseudonymisierten Daten keinen Zugang zur Zuordnungsregel hat. Ausweislich des Erwägungsgrundes 29 der DS-GVO sollte der Verantwortliche die insoweit zur Nutzung befugten Personen angeben.

Eine Pseudonymisierung personenbezogener Daten kann auf verschiedene Arten vorgenommen werden. So kann die Zuweisung des Pseudonyms durch die betroffene Person selbst erfolgen, etwa indem sie unter einer frei gewählten Nutzer-ID auftritt. Denkbar ist es auch, dass ein Dritter, z.B. eine Zertifizierungsstelle oder ein Datentreuhänder, das Pseudonym zuweist. Schließlich kann die Zuweisung des Pseudonyms durch den Verantwortlichen erfolgen (beispielsweise durch Zuweisung einer Kennziffer), dem die Identität der betroffenen Person bekannt ist.

⁹⁸ Ebenso bereits *Art.-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 10.4.2014, S. 3 und 12.

Für den Vorgang der Pseudonymisierung kommen verschiedene Möglichkeiten in Betracht, etwa die logische Trennung der Information, die Implementierung eines Rechte- und Rollenkonzepts oder die Erzeugung von Zufallswerten und die Zuordnung zur betroffenen Person mittels Referenzliste. Auch die Verschlüsselung von Daten kann eine Pseudonymisierung darstellen, obgleich Art. 6 Abs. 4 lit. e und Art. 32 Abs. 1 lit. a DS-GVO „Verschlüsselung“ und „Pseudonymisierung“ als zwei unterschiedliche im Abwägungsprozess zu berücksichtigende Maßnahmen beschreiben. Denn die Daten können erst nach Hinzuziehung zusätzlicher Informationen (des Schlüssels) wieder lesbar gemacht werden. Erwägungsgrund 83 der DS-GVO sieht insoweit vor, dass Verschlüsselungsmaßnahmen unter Berücksichtigung des Stands der Technik erfolgen sollen.

Erwägungsgrund 26 der DS-GVO bestimmt, dass pseudonymisierte Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können, als Informationen über eine identifizierbare natürliche Person zu betrachten sind. Pseudonymisierte Daten weisen folglich einen Personenbezug auf. In dogmatischer Hinsicht handelt es sich bei pseudonymisierten Daten daher um einen Unterfall von personenbezogenen Daten.⁹⁹ Dies hat zur Folge, dass die Regelungen der DS-GVO für die Verarbeitung pseudonymisierter Daten im vollen Umfang zu beachten sind. Problematisch sind Fälle, in denen ein Verantwortlicher pseudonymisierte Daten selbst nicht durch das Heranziehen zusätzlicher Informationen einer natürlichen Person zuordnen kann, aber ein Dritter im Besitz einer Zuordnungsregel ist. Virulent wird dies im Gesundheitswesen etwa dann, wenn ein Arzt pseudonymisierte Blutproben in ein Labor einschickt. Der Arzt kennt regelmäßig die Zuordnungsregel, wohingegen sie dem Labor unbekannt ist. Eine ähnliche Problematik besteht, wenn ein Treuhänder oder die betroffene Person selbst das Pseudonym verwaltet. Ob in diesen Fällen auch für die Stelle, die nicht über die Zuordnungsregel verfügt, ein Personenbezug vorliegt, ist vor dem Hintergrund der Grundsätze des EuGH zu beantworten, die dieser zur Frage der Berücksichtigung des Zusatzwissens Dritter entwickelt hat.¹⁰⁰ Ist das Zusatzwissen nicht zu berücksichtigen, so ist von anonymen Daten auszugehen.

⁹⁹ Ebenso *Karg*, DuD 2015, 520, 524.

¹⁰⁰ EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 31 ff. – Breyer = ZD 2016, 24 m. Anm. *Kühling/Klar*.

Eine ausdrückliche Privilegierung der Verarbeitung pseudonymisierter Daten enthält die DSGVO nicht.¹⁰¹ Der praktische Anreiz, personenbezogene Daten zu pseudonymisieren, liegt aber darin, dass eine Interessenabwägung eher zugunsten des Verantwortlichen ausfallen wird, der eine Pseudonymisierung vornimmt als wenn es zu keiner Pseudonymisierung kommt.¹⁰² Auch ist der technisch-organisatorische Schutzbedarf bei pseudonymen Daten geringer. Zudem besteht im Falle von Datenschutzverstößen nach Art. 34 Abs. 3 lit. a DS-GVO keine Benachrichtigungspflicht gegenüber der betroffenen Person, wenn Verschlüsselungsverfahren angewandt wurden. Kommt es zu einer Zweckänderung bei der Datenverarbeitung, fließt die Tatsache, dass die Daten pseudonymisiert verarbeitet werden, nach Art. 6 Abs. 4 lit. e DS-GVO in den Abwägungsprozess ein. Überdies kann die privilegierte Verarbeitung von personenbezogenen Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken nach Art. 89 DS-GVO eine Pseudonymisierung erfordern. Erwägungsgrund 29 der DS-GVO enthält zudem eine Privilegierung für die Verarbeitung im Rahmen allgemeiner Analysen. Danach sollen solche Pseudonymisierungsmaßnahmen, die eine „allgemeine Analyse“ zulassen, bei dem selben Verantwortlichen „möglich“ sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um für die jeweilige Verarbeitung die Umsetzung der DSGVO zu gewährleisten.

3. Zentrale Steuerungskonzepte

Die vorliegend relevanten zentralen Datenschutzgrundsätze der Datensparsamkeit bzw. Datenminimierung (dazu a)), der Zweckbestimmung bzw. -begrenzung (dazu b)), das Erforderlichkeitsprinzip (dazu c)) sowie die Voraussetzungen für eine wirksame Einwilligung (dazu d)) sollen im Folgenden untersucht werden. Die beiden erst genannten Prinzipien sind hier schon deshalb von besonderem Interesse, da sie vom Deutschen Ethikrat in seiner Stellungnahme problematisiert worden sind.

¹⁰¹ Piltz, K&R 2016, 557, 562; kritisch hierzu Härtling, ITRB 2016, 36, 38.

¹⁰² Härtling, NJW 2013, 2067; Karg, DuD 2015, 520, 524.

a) **Datensparsamkeit bzw. Datenminimierung**

Der Grundsatz der Datenminimierung und seine nähere Ausgestaltung insbesondere in Art. 25 DS-GVO konkretisieren den aus dem Verhältnismäßigkeitsprinzip folgenden Erforderlichkeitsgrundsatz (dazu c)) mit der Zielvorgabe, die Verarbeitung personenbezogener Daten und die Gestaltung und Auswahl von Datenverarbeitungssystemen am Grundsatz der Datenminimierung auszurichten.¹⁰³ Der Umgang mit personenbezogenen Daten und Systemstrukturen soll so konzipiert werden, dass personenbezogene Daten nur im unbedingt erforderlichen Umfang verarbeitet werden.

Mit immer weiteren Möglichkeiten, Datenbestände zu vernetzen, wuchs auch die Einsicht, dass die bloße Verrechtlichung des Datenschutzes keine Gewähr für seine Einhaltung bietet.¹⁰⁴ Moderner und effektiver Datenschutz muss die technischen Möglichkeiten und Gegebenheiten berücksichtigen und in ein Konzept des Systemdatenschutzes einbinden.¹⁰⁵ Schon auf technischer Ebene soll ausgeschlossen werden, was nicht erlaubt ist, und unterstützt werden, was gefordert wird.

Technischer Datenschutz und eine datenschutzfreundliche Systemstruktur von Datenverarbeitungssystemen sollen so von vornherein zu einem hohen Datenschutzniveau beitragen. Entsprechend ist die Vorgabe der Datensparsamkeit ergänzend auch in Art. 25 DS-GVO als technische Datenschutzvorgabe normiert.¹⁰⁶

b) **Zweckbestimmung bzw. -begrenzung**

Ein weiteres zentrales und seit jeher im deutschen Datenschutzrecht verankertes Regelungselement ist der Zweckbindungsgrundsatz.¹⁰⁷ Er entspringt dem datenschutzrechtlichen Konzept

¹⁰³ Die Ausführungen in diesem Abschnitt sind stark orientiert an *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 345 ff.

¹⁰⁴ Zur Historie *Dix*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 3.5 Rn. 19 ff.; *Scholz*, in: Simitis (Hrsg.), Kommentar zum BDSG, 8. Aufl. 2014, § 3a Rn. 3 f.

¹⁰⁵ Vgl. bereits *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministerium des Innern, 4.1.2010, abrufbar unter https://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile&v=3, abgerufen am 24.6.2019; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253, 255.

¹⁰⁶ *Buchner*, DuD 2016, 155, 156.

¹⁰⁷ Die Ausführungen in diesem Abschnitt sind stark orientiert an *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 338 ff.

der normativen Zweckbegrenzung.¹⁰⁸ Gemäß Art. 5 Abs. 1 lit. b DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Sie dürfen also nicht ohne Zweckbestimmung gleichsam auf Vorrat erhoben und gespeichert werden. Aus dem Wortlaut der Norm und des Erwägungsgrundes 39 der DS-GVO geht klar hervor, dass die Zwecke der Erhebung und beabsichtigten Verarbeitung bereits zum Zeitpunkt der Datenerhebung festgelegt sein müssen.¹⁰⁹ Der Zweckbindungsgrundsatz dient der Überschaubarkeit und Kontrolle der Datenverarbeitung. Die betroffene Person soll nicht den Überblick verlieren, sondern in der Lage sein, Umgangsphasen nachzuvollziehen und gegebenenfalls einschreiten zu können.

Die Verarbeitungszwecke müssen „eindeutig“ i.S.v. explizit bzw. konkret¹¹⁰ festgelegt sein. Voraussetzung für die Funktionserfüllung des Zweckbindungsgrundsatzes ist also nach wie vor die hinreichende Bestimmtheit der Zweckfestlegung. Das Maß des durch das Zweckbindungsgebot gewährten Schutzes des Rechts auf informationelle Selbstbestimmung ist abhängig vom Bestimmtheitsgrad der Zweckfestlegung. Es ist zu fordern, dass der Zweck so eindeutig, bestimmt und klar wie möglich festgelegt wird. Zwar können personenbezogene Daten auch für mehrere Zwecke erhoben werden, sie müssen dann aber ebenfalls genau und transparent festgelegt werden. Der Bestimmtheitsgrad der Zweckfestlegung spielt auch für den dem Verhältnismäßigkeitsprinzip entspringenden Erforderlichkeitsgrundsatz eine entscheidende Rolle. Der Verhältnismäßigkeitsgrundsatz dominiert das gesamte staatliche Handeln und ist auch im Datenschutzrecht ein zentrales Regelungsinstrument, das den Zweckbindungsgrundsatz flankiert. Er besagt als Erforderlichkeitsgrundsatz, dass in den Persönlichkeitsbereich der betroffenen Person grundsätzlich nur insoweit eingegriffen werden darf, als es für die (rechtmäßige) Zweckerreichung *unerlässlich* ist. Im öffentlichen Bereich ist es die staatliche Aufgabenzuweisung, die das Handeln von grundrechtsgebundenen Institutionen begrenzt und für die Zweckfestlegung und den Grad der Erforderlichkeit eine Richtschnur bildet. Im privaten Bereich schlägt sich das Erforderlichkeitsprinzip in zumeist offenen Abwägungsklauseln nieder (etwa Art. 6

¹⁰⁸ Ausführlich zum Konzept der normativen Zweckbegrenzung v. *Zezschwitz*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 3.1 Rn. 1 ff.

¹⁰⁹ *Herbst*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 31.

¹¹⁰ *Pötters*, in: Gola (Hrsg.), DS-GVO, 2017, Art. 5 Rn. 14 mit dem Hinweis auf die englische („explicit“) und französische („explicites“) Sprachfassung der Verordnung.

Abs. 1 UAbs. 1 lit. c DS-GVO). Insbesondere in diesem Bereich kann das Erforderlichkeitsprinzip nur dann fruchtbar eingesetzt werden, wenn die Zweckbestimmung hinreichend eindeutig und transparent formuliert wird. Eine nur vage Festlegung des verfolgten Zwecks lässt sowohl die Zweckbindung als auch den Erforderlichkeitsgrundsatz ins Leere laufen. Die Verarbeitungszwecke müssen darüber hinaus auch „legitim“¹¹¹ sein, also allgemeinen Rechtsprinzipien und sonstigem einschlägigen Recht außerhalb des Datenschutzes entsprechen.¹¹²

Art. 5 Abs. 1 lit. b DS-GVO bestimmt weiter, dass personenbezogene Daten nur in einer mit den ursprünglich festgelegten Zwecken zu vereinbarenden Weise weiterverarbeitet werden dürfen. Eine Zweckänderung, also die (Weiter-)Verarbeitung von personenbezogenen Daten zu anderen Zwecken als jenen, die bei der ursprünglichen Erhebung festgelegt wurden, ist damit grundsätzlich nicht zulässig. Etwas anderes gilt nur, wenn die Weiterverarbeitung zu „neuen“ Zwecken gemäß Art. 6 Abs. 4 DS-GVO auf einer Einwilligung der betroffenen Person oder einer qualifizierten Rechtsvorschrift der Union oder der Mitgliedstaaten¹¹³ beruht oder aber mit den ursprünglichen Zwecken „vereinbar“ ist. Um festzustellen, ob eine solche „Vereinbarkeit“ gegeben ist, hat der Verantwortliche eine wertende Beurteilung der fraglichen Verarbeitung vorzunehmen, die die ursprüngliche Zweckfestlegung und die Funktion des Zweckbindungsgrundsatzes berücksichtigt.¹¹⁴ Die DS-GVO liefert dabei einen nicht abschließenden Beispielskatalog mit Prüfkriterien in Art. 6 Abs. 4 DS-GVO (z.B. jede Verbindung zwischen ursprünglichen und „neuen“ Zwecken, Erhebungskontext, Art der personenbezogenen Daten oder mögliche Folgen der Weiterverarbeitung für die betroffene Person). Ist die Weiterverarbeitung zu geänderten Zwecken in diesem Sinne mit den ursprünglichen Zwecken vereinbar, muss sie nicht kumulativ durch eine eigenständige Rechtsgrundlage legitimiert werden, wie sich insbesondere aus dem eindeutigen Wortlaut des Erwägungsgrundes 50 S. 2 der DS-GVO ergibt.¹¹⁵ Das gilt nach zutreffendem Verständnis der Norm auch für Gesundheitsdaten und

¹¹¹ Die englische Fassung verwendet hier den Begriff „legitimate“, genau wie in der Parallelvorschrift des Art. 6 Abs. 1 UAbs. 1 lit. b DSRL, die in der deutschen Fassung von „rechtmäßige(n)“ Zwecken sprach.

¹¹² Heberlein, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 15, der als Beispiele das Diskriminierungsverbot und einschlägige Anforderungen des Arbeitsrechts, Vertragsrechts und Verbraucherschutzrechts nennt.

¹¹³ Gemäß Art. 6 Abs. 4 DS-GVO muss es sich um eine Rechtsvorschrift der Union oder der Mitgliedstaaten handeln, „die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt“.

¹¹⁴ Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 43.

¹¹⁵ So auch Frenzel, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 5 Rn. 31; Härting, DS-GVO, 2016, Rn. 514 f.; Kühling/Martini, EuZW 2016, 448, 451; Piltz, K&R 2016, 557, 566; Richter, DuD 2016, 581, 584; a.A. Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 48 f.; Schantz,

andere besondere Datenkategorien in Art. 9 DS-GVO, wie im Wortlaut des Art. 6 Abs. 4 lit. c DS-GVO vorausgesetzt wird.¹¹⁶ In der Konsequenz muss allerdings bei der Gesamtabwägung der Zweckvereinbarkeit die besondere Schutzwürdigkeit von Gesundheitsdaten berücksichtigt werden, um ein den Maßstäben des Art. 9 DS-GVO vergleichbares Schutzniveau zu erreichen. Dies führt gerade im vorliegenden Kontext des Umgangs mit Gesundheitsdaten zu der Frage, in welchem Verhältnis Art. 6 und Art. 9 DS-GVO zueinanderstehen. Teilweise wird in der Literatur angenommen, dass Art. 9 DS-GVO als einzige Rechtsgrundlage für die Datenverarbeitung besonderer Kategorien von Daten ausreicht.¹¹⁷ Es wird aber auch eine kumulative Lesart vertreten, derzufolge Art. 9 DS-GVO eine zusätzliche Schranke für diese Datenkategorien darstellt, so dass neben den Anforderungen des Art. 9 DS-GVO stets auch diejenigen des Art. 6 DS-GVO erfüllt sein müssen.¹¹⁸ Zudem gibt es vermittelnde Ansätze, denen zufolge Art. 9 DS-GVO Art. 6 DS-GVO nur teilweise verdrängen würde.¹¹⁹ Entscheidungspraxis ist zu dieser Frage nicht ersichtlich. Da die Anforderungen des Art. 9 DS-GVO strenger sind als diejenigen des Art. 6 DS-GVO bleibt der Streit in den meisten Fällen ein dogmatischer: Jedenfalls müssen die strengeren Anforderungen eingehalten werden und diese ergeben sich aus Art. 9 DS-GVO. Im Ergebnis kommt es daher im Regelfall nicht darauf an, ob man subsidiär auch noch die (niedrigeren) Anforderungen des Art. 6 DS-GVO prüft.

Dass beide Normen allerdings nicht beziehungslos nebeneinander stehen, zeigt schon die Anwendbarkeit des Art. 6 Abs. 4 DS-GVO auch auf besondere Datenkategorien nach Art. 9 DS-

NJW 2016, 1841, 1844; *Schulz*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 11; im Ergebnis ebenso, aber für eine einschränkende Auslegung des Erwägungsgrundes 50 S. 2 der DS-GVO *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 19 f.; *Monreal*, ZD 2016, 507, 510.

¹¹⁶ So auch *Schulz*, in: Gola (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 9 Rn. 7, allerdings mit dem wenig überzeugenden Hinweis auf Erwägungsgrund 51 der DS-GVO; a.A. *Schiff*, in: Ehmann/Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 9 Rn. 10.

¹¹⁷ In diese Richtung etwa *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 18, wonach ein „Rückgriff auf Art. 6 Abs. 1 ausgeschlossen“ sei; ähnlich auch *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 705; siehe auch *Albrecht/Jotzo*, Das neue Datenschutzrecht in der EU, 2017, Teil 3 Rn. 58, wonach Art. 9 DS-GVO „die allgemeinen Erlaubnisgründe aus Art. 6 Abs. 1 DS-GVO verdrängen“ würde.

¹¹⁸ Dafür etwa *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, 28. Edition, Art. 9 Rn. 24; siehe auch *Kühnl/Rohrer/Schneider*, DuD 2018, 735, 737 f.; so auch Kommissions-Expertengruppe zur Verordnung (EU) 2016/679 und Richtlinie (EU) 2016/680, Protokoll zur Sitzung vom 20. Februar 2018, S. 2, abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=12943>, abgerufen am 28.8.2019.

¹¹⁹ Siehe etwa *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 4; ähnlich *Schulz*, in: Gola (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 9 Rn. 5, der eine „teilweise Sperrwirkung“ des Art. 9 DS-GVO annimmt.

GVO.¹²⁰ Art. 9 DS-GVO verdrängt Art. 6 DS-GVO jedenfalls nicht vollständig.¹²¹ Allerdings überzeugt es auch nicht vollends, beide Vorschriften im Sinne einer zweistufigen Prüfung grundsätzlich als parallel anwendbar zu betrachten, wenn ohnehin die Vorgaben des Art. 9 DS-GVO den strengeren Maßstab bilden. Vor diesem Hintergrund sprechen wohl die besseren Argumente dafür, Art. 9 DS-GVO grundsätzlich als eigenständige Rechtmäßigkeitsvoraussetzung für die Verarbeitung besonderer Kategorien von Daten anzusehen und die Wertungen des Art. 6 DS-GVO nur insoweit heranzuziehen, als Art. 9 DS-GVO keine abschließende Bestimmung trifft. Es ist jedoch nicht auszuschließen, dass sich der EuGH im Falle einer Befassung mit dieser Frage auch der gegenteiligen Einschätzung, wie sie im Dokument der Kommission¹²² zum Ausdruck gekommen ist, anschließen könnte.

Derzeit sind keine Fälle ersichtlich, in denen eine Datenverarbeitung nach Art. 9 DS-GVO zulässig wäre, nicht jedoch nach Art. 6 DS-GVO. Insoweit wäre eine zweistufige Prüfung, selbst wenn man diese für dogmatisch überzeugend hielte, ohne Relevanz im Ergebnis. Jedenfalls steht Art. 9 DS-GVO – unabhängig von der Interpretation des Verhältnisses zu Art. 6 Abs. 1 DS-GVO – einer Anwendung des Art. 6 Abs. 4 DS-GVO auf Gesundheitsdaten und andere besondere Kategorien personenbezogener Daten nicht im Wege.

Grundsätzlich können sodann nach einer umfassenden Abwägung gemäß den Maßstäben des Art. 6 Abs. 4 DS-GVO (und im Falle von Gesundheitsdaten) unter Berücksichtigung der Wertungen des Art. 9 DS-GVO auch ohne andere Rechtsgrundlage oder Einwilligung bei hinreichender Vereinbarkeit der Zwecke und insbesondere zu Forschungszwecken auch personenbezogene Daten rechtmäßig verarbeitet werden. In der praktischen Bedeutung kommt Art. 6 Abs. 4 DS-GVO daher eine ähnliche Funktion wie einem gesetzlichen Zulässigkeitstatbestand zu, wie auch die systematische Stellung in Art. 6 DS-GVO nahelegt. Der Wortlaut lässt dabei offen, ob dies nur für denselben Verantwortlichen gilt oder Art. 6 Abs. 4 DS-GVO auch eine Übermittlung an Dritte und die weitere Verarbeitung durch diese legitimieren kann. Hierfür spricht zunächst, dass in Art. 4 Nr. 2 DS-GVO die Offenlegung durch Übermittlung als eine Variante der Verarbeitung personenbezogener Daten genannt ist. Dagegen spricht hingegen, dass nach Art. 6 Abs. 4 lit. b DS-GVO das Verhältnis zwischen der betroffenen Person und

¹²⁰ So im Ergebnis wohl auch *Schiff*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 9 Rn. 10 f.

¹²¹ *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 4.

¹²² Kommissions-Expertengruppe zur Verordnung (EU) 2016/679 und Richtlinie (EU) 2016/680, Protokoll zur Sitzung vom 20. Februar 2018, S. 2, abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=12943>, abgerufen am 28.8.2019.

dem Verantwortlichen für die Frage der Zweckvereinbarkeit zu berücksichtigen ist.¹²³ Die besseren Argumente sprechen daher dafür, die Übermittlung an Dritte als nur im Einzelfall von der Zweckänderung umfasst anzusehen.¹²⁴ So kann etwa innerhalb eines Konzerns die Übermittlung an andere Verantwortliche zu kompatiblen Zwecken legitimiert werden.

Gemäß Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO sind Weiterverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke dergestalt privilegiert, dass sie nicht als unvereinbar mit den ursprünglichen Zwecken gelten (Fiktion der Vereinbarkeit), die Vereinbarkeitsprüfung entfällt also insoweit.¹²⁵ Voraussetzung ist indessen, dass die entsprechende Weiterverarbeitung „gemäß Artikel 89 Absatz 1“ erfolgt. Es ist also durch technische und organisatorische Maßnahmen sicherzustellen, dass sie geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person unterliegt.¹²⁶ Nicht zuletzt vor dem Hintergrund der Erwägungsgründe 156 ff. der DS-GVO ist diese Privilegierung überdies stets eng auszulegen und es sind hohe Anforderungen an solche Zwecksetzungen zu stellen, so dass etwa Big-Data-Analysen nicht per se als „Statistik“ privilegiert und vom Zweckbindungsgrundsatz ausgenommen sein können.¹²⁷

c) Die Erforderlichkeit der Datenverarbeitung

Das Erforderlichkeitsprinzip¹²⁸ tritt neben das Verbot mit Zulässigkeitsvorbehalt, wie insbesondere an den Zulässigkeitstatbeständen des Art. 6 Abs. 1 UAbs. 1 lit. b bis f DS-GVO deutlich wird: Die Verarbeitung personenbezogener Daten ist demnach nur dann zulässig, wenn dies im Rahmen des jeweiligen Zulässigkeitsstatbestands erforderlich ist, wenn es also zur beabsichtigten Art und Weise der Datenverarbeitung keine sinnvolle oder zumutbare Alternative gibt, um die verfolgte Zielsetzung zu erreichen.¹²⁹

¹²³ Zu dieser Frage ausführlich auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 6 Rn. 44 ff.

¹²⁴ So im Ergebnis auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 6 Rn. 44 ff.

¹²⁵ *Herbst*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 50.

¹²⁶ *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 17; *Herbst*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 51.

¹²⁷ *Buchner*, DuD 2016, 155, 157; *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 17.

¹²⁸ *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 9; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 323 ff.

¹²⁹ *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 15.

d) Reichweite und Grenzen der Einwilligung

Im Folgenden sollen die allgemeinen und bereichsspezifischen Vorgaben für eine wirksame Einwilligung dargestellt werden, um ihre Eignung als Handlungsoption unter dem gegenwärtigen Rechtsregime bewerten zu können.

aa) Allgemeine Voraussetzungen der Einwilligung

Neben der Möglichkeit, die Datenverarbeitung auf gesetzliche Zulässigkeitstatbestände zu stützen, sieht die DS-GVO in Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO die Möglichkeit vor, die Verarbeitung über eine Einwilligung der betroffenen Person zu legitimieren.¹³⁰ In der Praxis ist es für private Verantwortliche in der Regel vorzugswürdig, Datenverarbeitungen über eine Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO rechtfertigen zu können. Allerdings lässt sich oft nicht mit abschließender Sicherheit bestimmen, ob die Interessenabwägung zugunsten oder zulasten des Verantwortlichen ausfallen wird. Dann kann es aus Gründen der Rechtssicherheit geboten sein, eine Einwilligung der betroffenen Person einzuholen und die Rechtmäßigkeit der Datenverarbeitung auf diese Einwilligung zu stützen. Eine Einwilligung kommt erst recht in Betracht, wenn keine Zweifel bestehen, dass die schutzwürdigen Interessen der betroffenen Person überwiegen.

Die Einwilligung wird in Art. 4 Nr. 11 DS-GVO definiert. Danach ist hierunter jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung zu verstehen, mit der die betroffene Person signalisiert, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Die Bedingungen für die Einwilligung werden sodann in Art. 7 DS-GVO festgelegt. Danach muss der Verantwortliche die Einholung einer Einwilligung nachweisen können (Art. 7 Abs. 1 DS-GVO). Aus der Formulierung folgt, dass die Beweislast für den Nachweis dem Verantwortlichen obliegt. Die Einwilligung unterliegt keinem Formerfordernis. Wie aus Erwägungsgrund 32 der DS-GVO folgt, kann die Einwilligung schriftlich, elektronisch oder mündlich abgegeben werden. Die Abgabe einer wirksamen Einwilligung erfordert ein sog. Opt-In, verlangt also ein aktives Tun der betroffenen Person. Bereits vorangekreuzte Kästchen reichen für eine wirksame Einwilligung nicht aus (vgl. Erwägungsgrund 32 der DS-GVO). Aus

¹³⁰ Die Ausführungen zur Einwilligung sind stark orientiert an *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 362 ff. sowie 439 ff.

Art. 7 Abs. 2 DS-GVO folgt weiter, dass sofern die schriftliche Einwilligung mit anderen Sachverhalten verbunden werden soll, eine Pflicht zur besonderen Hervorhebung und Gestaltung der Einwilligungserklärung besteht. Des Weiteren muss die Einwilligung jederzeit widerrufbar sein (Art. 7 Abs. 3 DS-GVO).

Die Freiwilligkeit der Einwilligung ist nicht gegeben, wenn die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig gemacht wird, die für die Erfüllung des Vertrags nicht erforderlich ist (Art. 7 Abs. 4 DS-GVO). Insoweit gilt ein umfassendes Koppelungsverbot, das nicht unerhebliche Auswirkungen für die Praxis hat.¹³¹

Insbesondere das Geschäftsmodell „Bezahlung mit Daten“ gerät regelmäßig in ein Spannungsfeld mit dem Koppelungsverbot.¹³² Denn nach Art. 7 Abs. 4 DS-GVO muss bei der Beurteilung der Freiwilligkeit „im größtmöglichen Umfang“ auch geklärt werden, ob der Vertragspartner die Erfüllung des Vertrags von einer Einwilligung zur Verarbeitung personenbezogener Daten abhängig gemacht hat, die für die Vertragserfüllung nicht erforderlich ist.

Handelt es sich bei der betroffenen Person, deren Einwilligung eingeholt werden soll, um ein Kind, d.h. um eine Person, die jünger als 16 Jahre alt ist, gelten nach Art. 8 DS-GVO besondere Anforderungen. Eine solche Einwilligung muss durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt werden. Vom Verantwortlichen verlangt der Verordnungsgeber insoweit, angemessene Anstrengungen zu unternehmen, um sicherzustellen, dass die Einwilligung auf die vorgesehene Weise eingeholt wird.

bb) Besondere Voraussetzungen der Einwilligung bei der Verarbeitung von Gesundheitsdaten

Der Verordnungsgeber normiert in Art. 9 DS-GVO strenge Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten. Hierunter fallen auch Gesundheitsdaten sowie genetische Daten.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zunächst zulässig, wenn eine Einwilligung der betroffenen Person vorliegt (Art. 9 Abs. 2 lit. a DS-GVO). Damit die Einwilligung wirksam und die Datenverarbeitung folglich gerechtfertigt ist, muss die betroffene Person vor Erteilung der Einwilligung ausreichend darüber informiert worden sein,

¹³¹ Hierzu *Weidert/Klar*, BB 2017, 1858, 1860.

¹³² So *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 21; *Schantz*, NJW 2016, 1841, 1845; zweifelnd dagegen *Stemmer*, in: BeckOK Datenschutzrecht, 27. Ed. 2018, Art. 7 DS-GVO Rn. 46.1.

welche Daten zu welchen Zwecken verarbeitet werden. Die betroffene Person muss ihre Einwilligung sodann ausdrücklich erklären. Schlüssiges Handeln ist dabei nicht ausreichend.¹³³ Inhaltlich muss sich die Einwilligung explizit auf die Verarbeitung besonderer Kategorien personenbezogener Daten beziehen. Insoweit gilt ein erhöhtes Maß an Bestimmtheit und Präzision.¹³⁴ Im Übrigen gelten die allgemeinen Anforderungen an wirksame Einwilligungserklärungen. Zu beachten ist, dass die Einholung einer Einwilligung durch staatliche Stellen grundsätzlich problematisch ist, da eine wirksame Einwilligung eine gewisse Gleichordnung der Beteiligten voraussetzt.¹³⁵

Ausweislich der Regelung können das Unionsrecht oder das Recht der Mitgliedstaaten das Verbot nach Art. 9 Abs. 1 DS-GVO „einwilligungsfest“ machen, d.h. Konstellationen vorsehen, in denen eine Einwilligung ausscheidet.

II. Regelungssystematik der §§ 303a ff. SGB V als Schwerpunkt der Betrachtung

Einer gesonderten Betrachtung bedürfen die Regeln zur Datentransparenz in den §§ 303a ff. SGB V, wobei im Folgenden die aktuelle Rechtslage im Zusammenspiel von DS-GVO, SGB X und SGB V, der DaTraV und der Nutzungsordnung Versorgungsdaten dargestellt wird. Ausgangspunkt ist dabei der Normzweck des Regelungsabschnitts im SGB V, nämlich die Datentransparenz und der Datenschutz (dazu 1.). Wichtig ist es auch, die Herkunft und die Art der Daten (dazu 2.), die dabei relevanten Akteure (dazu 3.) und die dabei erfolgende Bereitstellung der Daten (einschließlich der Zweckbindung; dazu 4.) zu klären. Schließlich ist vor dem Hintergrund der bisherigen Ausführungen zur Steuerungswirkung der DS-GVO (dazu I.) das Regelungsverhältnis der beiden Normebenen zueinander zu erläutern (dazu 4.).

1. Normzweck: Datentransparenz und Datenschutz

Die §§ 303a bis 303e SGB V enthalten Regelungen zur sog. Datentransparenz innerhalb der gesetzlichen Krankenkassen. Zweck der Vorschriften zur Datentransparenz ist es, Rahmenbedingungen zu schaffen, um einen umfangreichen Datensatz für Analysen zur Verbesserung der Versorgung bereitzustellen. Dieser soll hierzu bestimmten Einrichtungen zu Verfügung gestellt

¹³³ Vgl. *Schiff*, in: Ehmman/Selmayr (Hrsg.), DS-GVO, 2017, Art. 9 Rn. 28; *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 47.

¹³⁴ *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 47.

¹³⁵ *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 24.

werden, um das Gesundheitswesen weiterzuentwickeln und zu optimieren.¹³⁶ Zweck der Datenverarbeitung ist also die zielgerichtete Forschung zur Verbesserung der Versorgung. Die auf Grundlage der §§ 303a ff. SGB V geschaffene Datenbasis soll z.B. durch Kosten- und Nutzenanalysen Ausgangspunkt gesundheitspolitischer Entscheidungen sein.¹³⁷ Zeitgleich soll ein hohes Datenschutzniveau gewährleistet werden.¹³⁸ Die gesetzliche Regelung sucht demnach einen Kompromiss zwischen dem Interesse des Schutzes des Rechts auf informationelle Selbstbestimmung der Versicherten auf der einen und dem Allgemeininteresse an der Fortentwicklung, Verbesserung und Kosteneffizienz des Gesundheitssystems auf der anderen Seite. Zusätzlich stellt die Forschungsfreiheit ein Abwägungskriterium dar.

2. Herkunft und Art der Daten im Dateisystem

Wie aus § 303b Abs. 1 S. 1 SGB V und § 268 Abs. 3 S. 14 i.V.m. S. 1 Nrn. 1 bis 7 SGB V hervorgeht, stammen die gesammelten Daten ursprünglich von den gesetzlichen Krankenkassen. Die nach den §§ 294 bis 303 SGB V erhobenen Daten werden im Zuge des morbiditätsorientierten Risikostrukturausgleichs nach § 268 Abs. 3 S. 14 i.V.m. S. 1 Nrn. 1 bis 7 SGB V an das Bundesversicherungsamt (BVA) übermittelt.¹³⁹ Es handelt sich demnach bisher ausschließlich um Daten, die ohnehin von den Krankenkassen erhoben und an das BVA übermittelt werden. Für den Datengrundsatz der Datentransparenz nach den §§ 303a ff. SGB V werden also bislang keine eigenen Daten generiert, sondern nur bereits im System vorhandene verwendet.

Konkret handelt es sich bei den aus dem Risikostrukturausgleich stammenden Daten vor allem um die Stammdaten und Informationen über ambulante und stationäre Behandlungen eines Versicherten, sowie um Angaben zu den verschriebenen Arzneimitteln. Dies geht aus der Auflistung in § 268 Abs. 3 S. 1 Nrn. 1 bis 7 SGB V hervor, sowie aus dem die Art der Daten weiter konkretisierenden § 30 Abs. 1 der Risikostruktur-Ausgleichsverordnung (RSAV). Zu den Stammdaten zählen vor allem das Geburtsjahr und Geschlecht, vgl. § 30 Abs. 1 Nr. 1 RSAV.

¹³⁶ Vgl. *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018, § 303a Rn. 1.

¹³⁷ Vgl. *Scholz*, in: BeckOK Sozialrecht, Rolfs/Giesen/Kreikebohm/Udsching (Hrsg.), 52. Edition, Stand: 1.13.2019, § 303a SGB V Rn. 1.

¹³⁸ Vgl. *Spindler*, MedR 2016, 691, 698; *Hess*, in: Kassler Kommentar Sozialversicherungsrecht, 103. EL März 2019, SGB V § 303d, Rn. 3.

¹³⁹ Vgl. *Torbohm*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 363 f., dort insbesondere Fn. 1342.

Bei ambulanten Behandlungen werden nach § 268 Abs. 3 S. 1 Nr. 5 SGB V bzw. nach § 30 Abs. 1 Nr. 6 RSAV jeweils mit Verweis auf § 295 Abs. 1 S. 1 Nr. 2 SGB V vor allem die Behandlungszeit (Quartal der Behandlung) und die ICD-Codes, die Rückschlüsse auf die gestellten Diagnosen zulassen, erfasst. Neben den Diagnosen sind bei stationären Aufenthalten in einem Krankenhaus nach § 268 Abs. 3 S. 1 Nr. 1 SGB V und § 30 Abs. 1 Nr. 5 RSAV vor allem das Entlassungsdatum relevant. Bei Arzneimitteln werden gemäß § 268 Abs. 3 S. 1 Nr. 3 SGB V i.V.m. § 30 Abs. 1 Nr. 4 RSAV die Pharmazentralnummer und das Verordnungsdatum sowie die Anzahl der Verordnungen erfasst. Diese Daten sind allesamt pseudonymisiert, wie bereits aus § 268 Abs. 3 S. 3 SGB V, aber auch aus § 303b Abs. 1 S. 1 SGB V hervorgeht. Nicht umfasst sind unstrukturierte Daten wie z.B. Arztbriefe. Zu beachten ist weiterhin, dass die Daten erst mit einem Zeitverzug von mehreren Jahren zur Verfügung stehen.

Außerdem sind die Datensätze nach § 303b Abs. 2 SGB V mit Regionalkennzeichen zu versehen, die Rückschlüsse auf den Wohnort des Versicherten zulassen.¹⁴⁰ Diese regionale Zuordnung ist einerseits für eine sinnvolle Versorgungsforschung notwendig.¹⁴¹ Andererseits steigt dadurch das Risiko einer Reidentifizierung eines Versicherten, zumal viele der Datensätze einzigartig sind (dazu B. III. 1.).

3. Akteure und Verfahren der Datenübermittlung

Unter Datenübermittlung i.S.v. § 303b SGB V wird hier ein erster Schritt hin zur Schaffung von Datentransparenz verstanden, bei dem die Datensätze zunächst „intern“ übermittelt und gespeichert werden, um sie dann später dritten Institutionen „extern“ zur Verfügung stellen zu können. Bei der Übermittlung und der Speicherung der Daten spielen verschiedene Institutionen eine Rolle. Dies hat einerseits damit zu tun, dass die Verlässlichkeit und Richtigkeit der Daten sichergestellt werden muss. Andererseits dient dies auch dem Datenschutz. Die Datenübermittlung ist demnach ein erster, die spätere Bereitstellung an nutzungsberechtigte Stellen vorbereitender Schritt. Das Verfahren hierfür richtet sich nach den §§ 303b bis 303d SGB V. Relevante Akteure sind dabei das Bundesversicherungsamt (BVA; dazu a)), das Bundesministerium für Gesundheit (BMG; dazu b)) sowie die Vertrauensstelle (dazu c)) und die Datenaufbereitungsstelle (dazu d)) beim Deutschen Institut für Medizinische Dokumentation und Information (DIMDI).

¹⁴⁰ Vgl. hierzu *Fischinger/Monsch*, in: Spickhoff (Hrsg.), *Medizinrecht*, 3. Aufl. 2018, SGB V § 303b Rn. 3.

¹⁴¹ Vgl. *Beschlussempfehlung und Bericht des Ausschusses für Gesundheit*, BT-Drs 18/1657 S. 68, wo von einer Verbesserung der „Datenlage für die Versorgungsforschung“ die Rede ist.

a) Bundesversicherungsamt (BVA)

Das BVA ist gemäß § 303b Abs. 1 S. 1 SGB V Ausgangspunkt der Datensammlung, zumal es nach § 268 Abs. 3 S. 14 i.V.m. S. 1 Nrn. 1 bis 7 SGB V die „Risikostrukturausgleichsdaten“¹⁴² von den Krankenkassen erhält. Gemäß § 303b Abs. 1 S. 2 SGB V prüft das BVA die zu übermittelnden Daten auf Vollständigkeit und Plausibilität. Anschließend gibt das BVA gemäß § 303b Abs. 1 S. 1 SGB V den Datensatz pseudonymisiert an die Datenaufbereitungsstelle i.S.v. § 303d SGB V weiter. Die dazugehörigen Pseudonyme und die Krankenversicherungsnummer übermittelt das BVA der Vertrauensstellen nach § 303c SGB V.

b) Bundesministerium für Gesundheit (BMG)

Eine wichtige Rolle spielt auch das Bundesministerium für Gesundheit (BMG). Zunächst kann es gemäß § 303a Abs. 1 S. 2 SGB V durch Verordnung bestimmen, welche öffentliche Stelle Datenaufbereitungs- bzw. Vertrauensstelle ist. Nach § 303a Abs. 2 SGB V hat das BMG zudem eine Verordnungsermächtigung in Bezug auf den Datenumfang, das Verfahren der Datenübermittlung nach den §§ 303a bis 303e SGB V, das Pseudonymisierungsverfahren und die Kriterien der Bereitstellung von nicht anonymisierten Daten. Von dieser Verordnungsermächtigung wurde mit der Datentransparenzverordnung (DaTraV) Gebrauch gemacht. Zudem ist das BMG Rechtsaufsichtsbehörde der Datenaufbereitungsstelle nach § 303c Abs. 4 S. 2 SGB V und der Vertrauensstelle gemäß § 303d Abs. 2 S. 2 SGB V.

c) Vertrauensstelle nach § 303c SGB V, Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)

Nach § 2 Abs. 1 DaTraV ist die Aufgabe der Vertrauensstelle i.S.v. § 303c SGB V dem Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) zugewiesen. Das DIMDI ist eine dem BMG nachgeordnete nichtrechtsfähige Bundesanstalt mit verschiedenen gesetzlichen Aufgaben im medizinischen Bereich.¹⁴³ Unter anderem zählt es zu den Aufgaben des DIMDI, medizinische Datenbanken anzulegen und zu unterhalten und daraus Informatio-

¹⁴² Vgl. *Torbohm*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 363 f.

¹⁴³ Vgl. § 1 des Erlasses über die Errichtung des Deutschen Instituts für Medizinische Dokumentation und Information vom 1. September 1969, abrufbar unter <https://www.dimdi.de/dynamic/de/das-dimdi/aufgaben/rechtliche-grundlagen/>, abgerufen am 24.6.2019.

nen für die durch Gesetz und Verordnungen bestimmten Zwecke zugänglich zu machen. Gemäß § 303c Abs. 4 S. 2 SGB V unterliegt die Vertrauensstelle dem Sozialgeheimnis. Zuständige Rechtsaufsichtsbehörde ist das BMG.

Als Vertrauensstelle i.S.v. § 303c SGB V ist es nach den Absätzen 1 und 2 Aufgabe des DIMDI, die vom BVA übermittelte Liste temporärer Pseudonyme in permanente Pseudonyme zu überführen.¹⁴⁴ Die temporären Pseudonyme werden mit regelmäßig wechselnden Schlüsseln erzeugt, so dass hier zunächst keine langfristige Zuordnung von Leistungsdaten zu einem bestimmten Versicherten möglich wäre.¹⁴⁵ Diese langfristige Zuordenbarkeit ist notwendig, damit beispielsweise in der epidemiologischen Forschung Längsschnittanalysen durchgeführt werden können.¹⁴⁶ Mit einem von der Vertrauensstelle zu generierenden permanenten oder auch periodenübergreifenden Pseudonym ist der einem konkreten Versicherten zugewiesener Datensatz auch über längere Zeiträume oder auch über den Wechsel der Krankenkasse hinweg nachverfolgbar.¹⁴⁷ Näheres zu diesem Verschlüsselungsverfahren regelt neben § 303c Abs. 2 SGB V auch § 4 Abs. 1 DaTraV. Zudem ist nach § 303c Abs. 1 SGB V das Bundesamt für Sicherheit in der Informationstechnik (BSI) in das anzuwendende Verfahren einzubinden.

Relevant ist darüber hinaus § 303c Abs. 2 S. 2 SGB V, der klarstellt, dass eine Reidentifikation des Versicherten über das permanente Pseudonym durch die Vertrauensstelle, die Datenaufbereitungsstelle oder eine nutzungsberechtigte Stelle nicht möglich sein darf. Das Verfahren der Ableitung des permanenten Pseudonyms ist so auszugestalten, dass eine Ableitung der Krankenversicherungsnummer nicht möglich ist.

Schließlich übermittelt die Vertrauensstelle nach § 303c Abs. 3 S. 1 SGB V die permanenten Pseudonyme an die Datenaufbereitungsstelle. Danach ist in § 303c Abs. 3 S. 2 SGB V die Löschung sowohl der permanenten als auch der temporären Pseudonyme bei der Vertrauensstelle vorgesehen.

¹⁴⁴ Vgl. *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018, § 303c Rn. 3.

¹⁴⁵ Vgl. *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018, § 303c Rn. 1.

¹⁴⁶ Vgl. *Hess*, in: Kassler Kommentar Sozialversicherungsrecht, 103. EL März 2019, SGB V § 303d Rn. 3.

¹⁴⁷ Vgl. *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018, § 303c Rn. 5.

d) Datenaufbereitungsstelle nach § 303d SGB V, Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)

Zuständig für die Aufgabe der Datenaufbereitungsstelle i.S.v. § 303d SGB V ist gemäß § 2 Abs. 2 DaTraV ebenfalls das DIMDI. Dies scheint zunächst widersprüchlich, denn § 303c Abs. 4 S. 1 SGB V schreibt vor, dass die Vertrauensstelle räumlich, personell und organisatorisch eigenständig zu führen ist. Dass nun das DIMDI sowohl Vertrauens- als auch Datenaufbereitungsstelle sein kann, wird durch eine vollständige organisatorische Trennung innerhalb des DIMDI realisiert. Vollständig getrennt sind hierbei nicht nur Datenaufbereitungs- und Vertrauensstelle voneinander, sondern auch die beiden Stellen jeweils von den restlichen organisatorischen Einheiten des DIMDI und vom BMG. Dies ist in § 3 Abs. 3 DaTraV festgeschrieben und wird dadurch abgesichert, dass die verschiedenen Aufgaben von unterschiedlichen Organisationseinheiten wahrgenommen werden müssen, die räumlich, personell und organisatorisch getrennt voneinander arbeiten.

Das DIMDI erhält als Datenaufbereitungsstelle – wie bereits erläutert (s.o. B. II. 3. a)) – den Datensatz vom BVA im Zuge des Übermittlungsvorgangs nach § 303b Abs. 1 S. 1 SGB V. Von der Vertrauensstelle erhält die Datenaufbereitungsstelle die permanenten Pseudonyme. Gemäß § 303d SGB V ist es nun die Aufgabe dieser öffentlichen Stelle, den Datensatz mit dem entsprechenden permanenten Pseudonym zu verknüpfen und so aufzubereiten, dass er durch eine der in § 303e Abs. 1 SGB V genannten Stellen und insbesondere zu einem der in § 303e Abs. 2 genannten Zwecke genutzt werden kann.

4. Bereitstellung der Daten und Zweckbindung

Im nächsten Schritt werden die Versorgungsdaten von der Datenaufbereitungsstelle auf Antrag den in § 303e Abs. 1 SGB V abschließend aufgezählten Stellen bereitgestellt. Diese können die Daten dann im Rahmen der Zweckbindung nutzen. Gemäß § 303e Abs. 3 S. 2 SGB V die Bereitstellung an die nutzungsberechtigten Stellen grundsätzlich in anonymisierter und nur ausnahmsweise nach § 303e Abs. 3 S. 3 SGB V in pseudonymisierter Form statt. Vor diesem Hintergrund sind im Folgenden die nutzungsberechtigten Stellen (dazu a)), der Zweckbindungsgrundsatz (dazu b)) und die Art der Datenbereitstellung zu skizzieren (dazu c)).

a) Nutzungsberechtigte Stellen

Die verschiedenen nutzungsberechtigten Stellen sind in § 303e Abs. 1 Nrn. 1 bis 18 SGB V abschließend aufgezählt. Hierzu zählen die Krankenkassen, verschiedene Institute, Behörden

und nach § 303e Abs. 1 Nr. 8 Alt. 1 SGB V auch Universitäten. Die abschließende Liste enthält mit Formulierungen wie „sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung“ in § 303e Abs. 1 Nr. 8 Alt. 2 SGB V oder „den Institutionen der Gesundheitsversorgungsforschung“ in § 303e Abs. 1 Nr. 7 SGB V unbestimmte Rechtsbegriffe, die einer Auslegung bedürfen.¹⁴⁸

Mit den Universitäten können hier beispielsweise auch Institutionen, die grundsätzlich nicht verantwortliche Stellen nach § 35 Abs. 1 SGB I i.V.m. § 67 Abs. 2 SGB X sind, in eingeschränktem Maße Zugang zu Sozialdaten erlangen.¹⁴⁹

b) Zweckbindungsgrundsatz des § 303e Abs. 2 SGB V

Gemäß § 303e Abs. 2 SGB V unterliegt die Datenbereitstellung an die nutzungsberechtigten Stellen der Zweckbindung. Hierzu gibt § 303e Abs. 2 SGB V eine Liste von Zwecken vor. Manche der Zwecke sind auf bestimmte nutzungsberechtigte Stellen zugeschnitten, wie beispielsweise § 303e Abs. 2 S. 1 Nr. 1 SGB V, der von der „Wahrnehmung von Steuerungsaufgaben durch die Kollektivvertragspartner“ spricht. Andere Zwecke wie Nr. 2 („Verbesserung der Qualität der Versorgung“) oder Nr. 4 („Längsschnittanalysen“) sind offener gestaltet.

Aufgrund der widersprüchlichen Regelung ist unklar,¹⁵⁰ ob dieser Liste abschließender Charakter zukommt. Der Wortlaut des § 303e Abs. 2 S. 1 SGB V („insbesondere“) scheint eindeutig auf den nicht abschließenden Charakter der Norm hinzuweisen.¹⁵¹

Dem widerspricht jedoch möglicherweise die systematische Auslegung in Zusammenhang mit § 303e Abs. 3 S. 1 SGB V, wonach von der Datenaufbereitungsstelle zu prüfen ist, „ob der Zweck der Verarbeitung und Nutzung der Daten dem Katalog nach Absatz 2 entspricht“.¹⁵² Deshalb wird zum Teil der Schluss gezogen, der Katalog der Zwecke sei trotz des Wortlauts

¹⁴⁸ Vgl. hierzu *Schneider*, in: Krauskopf (Hrsg.), Soziale Krankenversicherung, Pflegeversicherung, 102. EL Februar 2019, SGB V, § 303e Rn. 7.

¹⁴⁹ Vgl. *Torbohm*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 363 f.

¹⁵⁰ Vgl. *Hornung*, in: Hänlein/Schuler (Hrsg.), Sozialgesetzbuch, 5. Aufl. 2016, SGB V, § 303e Rn. 2.

¹⁵¹ Zu diesem Schluss kommen im Ergebnis *Fischinger/Monsch*, in: Spickhoff (Hrsg.), Medizinrecht, 3. Aufl. 2018, SGB V § 303e Rn. 2; *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018, § 303e Rn. 3; *Schäfer*, in: Berchtold/Huster/Rehborn (Hrsg.), Gesundheitsrecht, 2. Aufl. 2018, SGB V § 303e Rn. 5; *Scholz*, in: BeckOK Sozialrecht, Rofls/Giesen/Kreikebohm/Udsching (Hrsg.), 52. Edition, Stand: 1.3.2019, SGB V § 303e Rn. 2.

¹⁵² Vgl. *Hornung*, in: Hänlein/Schuler (Hrsg.), Sozialgesetzbuch, 5. Aufl. 2016, SGB V § 303e Rn. 2.

abschließend.¹⁵³ Die Rede ist sogar von einem Redaktionsversehen des Gesetzgebers bei der offenen Fassung des Katalogs, was aber kein Problem darstelle, da der Katalog teilweise ohnehin offen formuliert sei und so genügend Spielraum ließe.¹⁵⁴

Von Vertretern der gegenläufigen Auffassung wird § 303e Abs. 3 S. 1 SGB V hingegen so interpretiert, dass der Zweck der Verarbeitung zwar nicht vom Katalog des Abs. 2 umfasst sei, den dort aufgelisteten Zwecken jedoch „entsprechen“ muss.¹⁵⁵

Insoweit besteht die Möglichkeit einer Klarstellung durch den Gesetzgeber. Dies ist angesichts der bestehenden Unklarheiten zweckmäßig.

c) Art der Bereitstellung

Gemäß § 303e Abs. 3 S. 1 SGB V prüft das DIMDI als Datenaufbereitungsstelle auf einen Antrag hin, ob die Voraussetzungen zur Bereitstellung der Daten vorliegen und entscheidet durch Verwaltungsakt. Hierbei kann das DIMDI der nutzungsberechtigten Stelle nach § 5 Abs. 7 S. 2 DaTraV Auflagen machen, die dem Schutz der Daten der Versicherten dienen. Auf einer dritten Ebene nach den §§ 303a ff. SGB V und der DaTraV hat das DIMDI in einer Nutzungsordnung¹⁵⁶ genauere Regeln zum Ablauf der Bereitstellung der Daten formuliert. Den nutzungsberechtigten Stellen werden dabei im Regelfall gemäß § 303e Abs. 3 S. 2 SGB V lediglich anonymisierte Daten zur Verfügung gestellt. Nur ausnahmsweise können nach § 303e Abs. 3 S. 3 SGB V i.V.m. § 5 Abs. 5 DaTraV pseudonymisierte Daten bereitgestellt werden, wenn dies zur Zweckerreichung erforderlich ist. Nach § 5 Abs. 5 S. 3 DaTraV darf dies jedoch nur in den Räumen des DIMDI erfolgen. Zu einer Übermittlung der Einzeldaten kommt es demnach nicht. Wie auch im ersten Fall werden letztlich lediglich die soweit wie möglich anonymisierten Ergebnismengen freigegeben.

¹⁵³ Vgl. *Hornung*, in: Hänlein/Schuler (Hrsg.), Sozialgesetzbuch, 5. Aufl. 2016, SGB V §303e Rn. 2; im Ergebnis auch *Torbohm*, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 364.

¹⁵⁴ Vgl. *Hornung*, in: Hänlein/Schuler (Hrsg.), Sozialgesetzbuch, 5. Aufl. 2016, SGB V §303e Rn. 2.

¹⁵⁵ Vgl. *Scholz*, in: BeckOK Sozialrecht, Rolfs/Giesen/Kreikebohm/Udsching (Hrsg.), 52. Edition, Stand: 1.3.2019, SGB V § 303e Rn. 2; *Schäfer*, in: Berchtold/Huster/Rehborn (Hrsg.), Gesundheitsrecht, 2. Aufl. 2018, SGB V § 303e Rn. 5.

¹⁵⁶ Informationssystem Versorgungsdaten (Datentransparenz): Nutzungsordnung, Version 01-05-000, abrufbar unter <https://www.dimdi.de/static/.downloads/deutsch/versorgungsdaten-nutzungsordnung.pdf>, abgerufen am 24.6.2019.

5. Verhältnis zur DS-GVO

Die Normen der §§ 303a bis 303e SGB V stammen aus dem Jahr 2004¹⁵⁷ und wurden zuletzt 2012¹⁵⁸ substanziell geändert. Zu klären ist vor diesem Hintergrund, wie die Regelungen zur Datentransparenz in den gesetzlichen Krankenkassen im Verhältnis zu der seit dem 25. Mai 2018 geltenden DS-GVO stehen. Eine Anpassung der datenschutzrechtlich relevanten bereichsspezifischen Normen des SGB V ist bislang nicht erfolgt. Das zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU, das im bisherigen Gesetzesentwurf¹⁵⁹ auch im SGB V verschiedene Änderungen vorsieht, befindet sich derzeit im Gesetzgebungsprozess.

a) Grundsätzliche Anwendbarkeit

Die aus dem Risikostrukturausgleich stammenden Datensätze weisen zunächst jeweils einen Bezug zu einem Versicherten und damit einen Personenbezug i.S.v. Art. 4 Nr. 1 DS-GVO auf. Soweit die Daten nicht im technischen Sinne anonym sind (vgl. hierzu bereits B. I. 2. a) und b)), ist der Anwendungsbereich der DS-GVO nach Art. 2 Abs. 1 DS-GVO daher grundsätzlich eröffnet, was auch Erwägungsgrund 26 der DS-GVO klarstellt.¹⁶⁰

Dies gilt demnach insbesondere für die Datenübertragung i.S.v. § 303b SGB V, bei der pseudonymisierte Daten vom BVA an das DIMDI übermittelt werden. Bei der späteren Bereitstellung der Daten durch das DIMDI an die Stellen i.S.v. § 303e SGB V ist zu differenzieren. Im Normalfall einer Bereitstellung des Datensatzes in anonymisierter Form nach § 303e Abs. 3 S. 2 SGB V liegen schon keine personenbezogenen Daten mehr vor, sodass die DS-GVO keine Anwendung findet (hierzu im Detail unten B. III. 1. b) aa)). Jedoch ist nach § 303e Abs. 3 S. 3 SGB V i.V.m. § 5 Abs. 5 DaTraV ausnahmsweise auch eine Bereitstellung lediglich pseudonymisierter Daten durch das DIMDI möglich, wenn der Nutzungszweck i.S.v. § 303e Abs. 2 SGB V anders nicht erreicht werden kann. Für diesen Fall trifft § 5 Abs. 5 DaTraV Sonderregelungen. So darf der pseudonymisierte Datensatz ausschließlich in den Räumen des DIMDI eingesehen werden. Hier ist der Anwendungsbereich der DS-GVO dann wieder eröffnet (hierzu im Detail unten B. III. 1. b) bb)).

¹⁵⁷ Eingeführt in das SGB V durch das Gesetz zur Modernisierung der GKV v. 14.11.2003, BGBl. I 2190.

¹⁵⁸ Durch das GKV-Versorgungsstrukturgesetz v. 22.12.2011, BGBl. I S. 2983, 3012 ff.

¹⁵⁹ Siehe BT-Drucks. 19/4674.

¹⁶⁰ Siehe hierzu *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 262 ff.

b) Umfassende Öffnungsklauseln im Gesundheitswesen

Ob es – gerade in Bezug auf die Zulässigkeitstatbestände der Datenverarbeitung – auf die Regelungen der DS-GVO ankommt oder aber mitgliedstaatliches Recht weitestgehend maßgebend ist, hängt im Wesentlichen davon ab, ob man sich im Bereich einer Öffnungsklausel der DS-GVO befindet und wie weit diese reicht. Im gesamten Gesundheitssektor und gerade im Gesundheitswesen findet man vor allem in Art. 9 DS-GVO sehr weit reichende Öffnungsklauseln (s.o. B. I. 1.).¹⁶¹ Vorliegend ist vor allem Art. 9 Abs. 2 lit. h DS-GVO heranzuziehen, der für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich und für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich dem nationalen Recht den Vorrang gewährt.

Hiervon umfasst ist auch die Datenanalyse zur Fortentwicklung des Gesundheitswesens, so dass sich die §§ 303a ff. SGB V innerhalb des Rahmens der Öffnungsklausel bewegen.¹⁶² Daneben kann auch Art. 9 Abs. 2 lit. j i.V.m. Art. 89 DS-GVO einschlägig sein, soweit die wissenschaftliche Forschung betroffen ist.¹⁶³

Geht es etwa um die Datenverarbeitung durch Wissenschaftler einer Universität, die zum Zwecke der Versorgungsforschung tätig werden, dann ist Art. 9 Abs. 2 lit. j i.V.m. Art. 89 DS-GVO vorrangig einschlägig. Sofern dagegen etwa die Krankenkassen zur Analyse und Entwicklung von sektorenübergreifenden Versorgungsformen sowie von Einzelverträgen der Krankenkassen auf die Daten zugreifen, § 303e Abs. 1 Nr. 3 i.V.m. Abs. 2 S. 1 Nr. 6 SGB V, ist Art. 9 Abs. 2 lit. h DS-GVO passgenauer als Art. 9 Abs. 2 lit. j i.V.m. Art. 89 DS-GVO als einschlägige Öffnungsklausel. Demnach können sich die §§ 303a ff. SGB V auf beide Öffnungsklauseln stützen, je nach Verarbeitungskontext.

Sollte es sich bei den Daten, die im Zuge der Datentransparenz verarbeitet werden, ausnahmsweise nicht um Gesundheitsdaten oder andere besondere Kategorien personenbezogener Daten handeln, so ist hier die Öffnungsklausel des Art. 6 Abs. 2 i.V.m. Abs. 1 S. 1 lit. e DS-GVO passender.

¹⁶¹ Vgl. Kühling/Martini, Die Datenschutzgrundverordnung und das nationale Recht, 2016, S. 48 f.

¹⁶² So im Ergebnis auch Spindler, MedR 2016, 691, 699; vgl. auch Buchner/Schwichtenberger, GuP 2016, 218, 223, die zwar nicht konkret Bezug auf die §§ 303a ff. SGB V nehmen, doch mit der Aussage das Sozialdatenschutzrecht würde „auch künftig als [...] ein eigenständiger Regelungsbereich erhalten bleiben“, dieselbe Richtung einschlagen.

¹⁶³ Siehe hierzu Kingreen/Kühling, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, 43, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019.

Damit kommt es im Ergebnis nicht auf die Zulässigkeitstatbestände der DS-GVO an, sondern ausschließlich auf die §§ 303a ff. SGB V, da diese den nach Unionsrecht vorgesehenen Voraussetzungen gerecht werden. Bezüglich anderer sich aus der DS-GVO ergebender Regelungen, z.B. zur Eröffnung des Anwendungsbereichs des Datenschutzrechts auf personenbezogene Daten (einschließlich pseudonymer Daten und in Abgrenzung zu anonymen Daten), zu den Betroffenenrechten oder institutionellen Vorgaben, kann jedoch auch in diesem Bereich das allgemeine europäische Datenschutzrecht greifen.

III. Problematische Einzelfragen

Im Folgenden soll eine Reihe problematischer Einzelfragen detailliert analysiert werden, die im Rahmen eines möglichen Gesetzgebungsvorhabens besondere Relevanz haben.

1. Anonymität und Reidentifikation

Im Rahmen von Big-Data-Analysen stellt sich die Frage, wann bzw. ob von anonymen Daten auszugehen ist und in der Folge die Datenverarbeitung nicht in den Anwendungsbereich des Datenschutzrechts fällt (s.o. B. I. 2. a)). Die Löschung des Personenbezugs aus einem Datensatz kann eine Anonymisierung darstellen (s.o. B. I. 2. b) aa)). Getrennt davon zu betrachten ist eine bloße Pseudonymisierung der Datensätze (s.o. B. I. 2. b) bb)). Entscheidendes Kriterium für die Frage, ob Daten anonym sind, ist nach Art. 4 Nr. 1 DS-GVO, ob die (ursprünglich) betroffenen Personen nicht mehr identifizierbar sind. Nach Erwägungsgrund 26 der DS-GVO sind bei der Frage der Identifizierbarkeit alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Auch künftig technisch mögliche Identifizierungsmethoden können hiernach also bereits Auswirkungen auf den aktuellen Anwendungsbereich des Datenschutzrechts haben, soweit sie absehbar sind.¹⁶⁴ Grenze des Datenschutzrechts unter der DS-GVO ist keineswegs die absolute (unumkehrliche) Anonymität, sondern die Anonymisierung ist lediglich „faktisch“ erforderlich.¹⁶⁵ Vor diesem Hintergrund hat in Bezug auf jedes

¹⁶⁴ Schantz, NJW 2016, 1841, 1843.

¹⁶⁵ Schneider, Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen, 2015, S. 17.

Datum eine Risikobewertung zu erfolgen, inwieweit es zu einer Identifizierung kommen kann.¹⁶⁶

Besonders relevant ist vorliegend die Frage, ab wann Daten als formal anonym anzusehen sind, zumal ein Spezifikum von Big-Data-Analysen die Möglichkeit der Reidentifikation von Daten ist, deren Identifikatoren (z.B. Name oder Adresse) bereits gelöscht wurden.¹⁶⁷ Dieses Phänomen taucht dort auf, wo Analyseprogramme durch Musterbildung bzw. durch die Herstellung von Korrelationen Rückschlüsse auf die Identität einer vermeintlich nicht mehr identifizierbaren Person ziehen können.¹⁶⁸

Bei dem System der Datentransparenz gemäß den §§ 303a ff. SGB V stellt sich dieses Problem im Besonderen. Ein ausgeprägtes Reidentifikationsrisiko ergibt sich hier allein schon aus der Einzigartigkeit mancher versichertenbezogener Einzeldatensätze. Einige in einem solchen Einzeldatensatz gespeicherte Krankheits- und Behandlungsverläufe besitzen Ausprägungen, die so nicht noch einmal existieren. Dies gilt insbesondere in Kombination mit Regionalkennzeichen, die Rückschlüsse auf den Wohnort des Versicherten zulassen. Der bloßen Einzigartigkeit der Information ist dabei noch keine grundsätzliche Bedeutung für die Frage der Identifizierbarkeit beizumessen. Das Risiko einer Reidentifikation ist jedoch deutlich höher.¹⁶⁹ Der Rückschluss auf die Identität eines Versicherten ist demnach die über allem schwebende Gefahr bei der Verarbeitung der Versorgungsdaten. Zunächst bedarf es hierbei einer näheren Betrachtung, welche statistischen Besonderheiten zu einer Reidentifikation führen können (a.), um sodann die Frage zu beantworten, ob eine Reidentifikation bei den verschiedenen Arten der Datenbereitstellung der Datenaufbereitungsstelle möglich bzw. wahrscheinlich ist, um letztlich über die Frage der Anonymität entscheiden zu können (b.).

a) Fallgruppen der Reidentifikation

In Datensätzen allgemein und damit auch innerhalb der Versorgungsdaten im Speziellen sind bestimmte Fallgruppen von Reidentifikationsmöglichkeiten denkbar. Naheliegend sind die beiden im Folgenden dargestellten Gruppen.

¹⁶⁶ Vgl. Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 4 Nr. 1 Rn. 22; und bereits Klar/Kühling, NJW 2013, 3611, 3613.

¹⁶⁷ Vgl. zu den datenschutzrechtlichen Problemstellungen Sarunski, DuD 2016, 424; Boehme-Neßler, DuD 2016, 419.

¹⁶⁸ Siehe Spindler, ZD 2017, 303, 306; Ladeur, DuD 2016, 360, 363.

¹⁶⁹ Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 319.

aa) Fallzahlproblem

Zunächst stellt sich das Fallzahlproblem, auch bekannt unter dem Begriff des Problems kleiner Ergebnismengen. Dieses tritt auf, wenn Ausprägungen in den Daten nur auf ein oder zwei Merkmalsträger zurückgehen bzw. eine Kombination von Merkmalen nur ein- oder zweimal im Datensatz auftaucht.¹⁷⁰ Insbesondere wenn es sich um nur einen Fall handelt, ist dies problematisch. Beispiel hierfür kann eine seltene Krankheit sein, die in einem bestimmten Bereich nur einmal vorkommt. Verfügt jemand über Zusatzwissen oder ist dieses Wissen allgemein zugänglich, so kann man so teilweise einzelne Versicherte identifizieren. Damit sind aber auch alle weiteren Informationen zugänglich, die die Versorgungsdaten über diese Person enthalten. Als Lösung wird gemeinhin die Festlegung einer Mindestfallzahl verstanden. Dies kann jedoch zugleich den Informationsgehalt der Daten mindern.¹⁷¹

bb) Randsummenproblem

Zudem stellt sich das sog. Randsummen- oder Randwertproblem. Von einem solchen ist die Rede, wenn bei der Auswertung eines Datensatzes „innerhalb einer Tabellenzeile oder -spalte alle Merkmalsträger in dieselbe Kategorie fallen“.¹⁷² Hier können auch wesentlich mehr Versicherte als nur ein bis zwei betroffen sein und doch lässt sich eine Aussage bezüglich aller Merkmalsträger treffen. Als Beispiel kann die Aussage dienen „alle im Jahr 2014 im Krankenhaus XYZ behandelten Patienten im Alter von 99 litten an Demenz“. Kennt man einen 99-jährigen, der 2014 im Krankenhaus XYZ behandelt wurde, so weiß man um dessen Demenz, auch wenn einem diese Information zunächst nicht bekannt war. Dies gilt unabhängig von der Zahl der behandelten Patienten mit den obigen Merkmalen.

b) Arten von nutzbaren Daten im Versorgungssystem

Die Datenaufbereitungsstelle verfügt über den Datensatz der Versorgungsdaten in nicht unmittelbar identifizierter Form. Sobald die Vertrauensstelle die Liste der Pseudonyme löscht (s.o.

¹⁷⁰ Vgl. bzgl. der amtlichen Statistik *Rothe*, Bayern in *Zahlen 2015*, 294, 299; abrufbar unter https://www.forschungsdatenzentrum.de/sites/default/files/fdz_aufsatz_1_gh.pdf, abgerufen am 24.6.2019; *Höhne*, Berliner Statistik 2003, 96, 97; abrufbar unter https://www.statistik-berlin-brandenburg.de/publikationen/aufsätze/2003/MS-BE_200303-01.pdf, abgerufen am 24.6.2019.

¹⁷¹ Vgl. *Rothe*, Bayern in *Zahlen 2015*, 294, 299; abrufbar unter https://www.forschungsdatenzentrum.de/sites/default/files/fdz_aufsatz_1_gh.pdf, abgerufen am 24.6.2019.

¹⁷² Vgl. *Rothe*, Bayern in *Zahlen 2015*, 294, 301; abrufbar unter https://www.forschungsdatenzentrum.de/sites/default/files/fdz_aufsatz_1_gh.pdf, abgerufen am 24.6.2019.

B. II. 3. c)), ist weder der Vertrauens-, noch der Datenaufbereitungsstelle eine Identifizierung der Versicherten durch eine Zuordnung von Pseudonymen möglich. Um Versicherte zu reidentifizieren, müsste insbesondere die Datenaufbereitungsstelle über Zusatzwissen verfügen, zu dem sie in der Regel keinen Zugang hat. Es sind auch keine rechtlichen Möglichkeiten¹⁷³ (s.o. B. I. 2.) ersichtlich, wie die Datenaufbereitungsstelle an das Zusatzwissen zur Reidentifizierung gelangen soll. Soweit nicht im Einzelfall öffentlich zugängliche Informationen zur Reidentifikation genügen, sind weite Teile der Daten aus Sicht der Datenaufbereitungsstelle also bereits nicht mehr identifizierbar im Sinne der Logik der DS-GVO.

Diese Daten gibt die Datenaufbereitungsstelle nach der aktuellen Fassung von § 303e Abs. 3 SGB V i.V.m. § 5 DaTraV auf zwei verschiedene Arten an nutzungsberechtigte Stellen heraus.

aa) Aggregierte Daten

Dem Grunde nach werden Daten nur „anonymisiert“ i.S.v. § 303e Abs. 3 S. 2 SGB V bzw. „anonymisiert und zusammengefasst“ nach § 5 Abs. 4 DaTraV weitergegeben.¹⁷⁴ Die nutzungsberechtigte Stelle erhält nur die Ergebnismengen, ohne dabei Zugriff auf einen versichertenbezogenen Datensatz zu erlangen. Es erfolgt im Regelfall also eine Zusammenfassung bzw. Aggregation der Daten durch die Datenaufbereitungsstelle nach den von der nutzungsberechtigten Stelle angeforderten Parametern, so dass diese nur die Ergebnismengen erhält. Der Begriff der aggregierten Daten kommt zwar nicht im Wortlaut der §§ 303a ff. SGB V oder der DaTraV vor. Auch handelt es sich nicht um einen in der DS-GVO definierten Begriff, so dass der Aggregation per se keine datenschutzrechtliche Rechtsfolge zukommt.¹⁷⁵ Jedoch wirkt sie sich faktisch auf die Frage aus, welche Daten noch identifizierbar sind. Es gilt der Grundsatz, je stärker zusammengefasst und je größer die Ergebnismengen bzw. die Mindestfallzahlen sind, desto unwahrscheinlicher ist eine Identifizierung. Ab welchem Aggregierungsgrad tatsächlich von einem Entfallen der Identifizierbarkeit auszugehen ist, hängt dabei im Wesentlichen davon ab, inwieweit Rückschlüsse auf einzelne Personen möglich sind.¹⁷⁶ Eine Reidentifikation ist demnach per se nicht ausgeschlossen, denn Randsummen- oder Fallzahlprobleme können auch

¹⁷³ Kriterium des EuGH, vgl. EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 f. – Breyer = ZD 2016, 24 m. Anm. Kühling/Klar.

¹⁷⁴ Vgl. hierzu Michels, in: Becker/Kingreen (Hrsg.), SGB V, 6. Aufl. 2018, § 303e Rn. 5.

¹⁷⁵ Siehe Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 4 Nr. 1 Rn. 15 f.; Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 314.

¹⁷⁶ Siehe Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 4 Nr. 1 Rn. 15.

in Ergebnismengen auftauchen. Jedoch prüft hier die Datenaufbereitungsstelle für jeden Einzelfall nach, ob solche Fälle gegeben sind, so dass im Zweifel nie personenbezogene Daten herausgegeben werden. Die Bezeichnung der Daten als anonymisiert in § 303e Abs. 3 S. 2 SGB V und § 5 Abs. 4 DaTraV entspricht also aufgrund der Nachprüfung im Einzelfall durch die Datenaufbereitungsstelle den Anforderungen des Art. 4 Nr. 1 DS-GVO und ist daher mit der DS-GVO konsistent. Ein verbleibendes Restrisiko der Reidentifizierung nach erfolgter Aggregation und Prüfung auf Vorliegen von Randsummen- und Fallzahlproblemen ist insofern unbedenklich. Allerdings bedeutet die Vorgehensweise, um dieses Ergebnis zu gewährleisten, für die Datenaufbereitungsstelle einen hohen Arbeitsaufwand. Der Vorgang der Bereitstellung der aggregierten Daten wirft mithin – soweit er korrekt umgesetzt wird – keine weiteren datenschutzrechtlichen Fragen auf. Die Daten sind anonym und fallen nicht (mehr) in den Anwendungsbereich der DS-GVO.

bb) Einzeldatensätze

Ausnahmsweise können Daten auch lediglich „pseudonymisiert“ i.S.v. § 303e Abs. 3 S. 3 SGB V bzw. „als Einzeldatensätze pseudonymisiert“ nach § 5 Abs. 5 DaTraV von nutzungsberechtigten Stellen verarbeitet werden, soweit dies erforderlich ist. Dies ist dann jedoch nur in den Räumen der Datenaufbereitungsstelle möglich.¹⁷⁷ Auch der von der DaTraV verwendete Begriff der Einzeldatensätze hat zunächst keine datenschutzrechtliche Bedeutung. Zumindest bedeutet er nicht zwingend, dass von einer Identifizierbarkeit für die nutzungsberechtigte Stelle auszugehen ist. Beispielsweise ist ein Einzeldatensatz, der lediglich die Information enthält „Patient X wurde im Jahr 2014 wegen eines grippalen Infekts behandelt“ oder noch deutlicher „Patient Y war im Jahr 2014 gesetzlich versichert und erhielt keine Behandlung“ kaum als personenbezogenes Datum aus Sicht einer nutzungsberechtigten Stelle zu verstehen. Die Identität der Patienten X und Y aus den obigen Beispielen dürfte unter der Fülle der gleich lautenden Einzeldatensätze für eine zugangsberechtigte Stelle nicht aufzudecken sein. Andererseits ist durch die hohe Anzahl an gespeicherten Merkmalen, die vielen möglichen Merkmalsausprägungen und die individuellen Behandlungsverläufe ein großer Teil der versichertenbezogenen Datensätze einzigartig. Mit Vorwissen zu einigen Merkmalen eines Versicherten besteht damit ein Reidentifikationspotenzial. Wenn man beispielsweise über eine bestimmte Person weiß, wie alt sie ist, wann sie in etwa zuletzt einen Arzt oder ein Krankenhaus besucht hat und

¹⁷⁷ Vgl. hierzu *Michels*, in: Becker/Kingreen (Hrsg.), SGB V, 6. Aufl. 2018, § 303e Rn. 5.

dass sie an zwei bestimmten (nicht zwingend seltenen) Krankheiten leidet, so ist mit relativ hoher Wahrscheinlichkeit der Einzeldatensatz dieser Person aufzufinden und ihr zuzuordnen. Ebenfalls denkbar ist ein Szenario, in dem einige (Gesundheits-)Daten einer prominenten Person über die Medien an die Öffentlichkeit gelangen, so dass mit Hilfe dieses Wissens eine Identifikation des versichertenbezogenen Einzeldatensatzes der prominenten Person möglich ist.

Betrachtet man jeden versichertenbezogenen Einzeldatensatz individuell, so ist gerade aus Sicht einer nutzungsberechtigten Stelle teilweise, aber nicht immer von personenbezogenen Daten auszugehen, wie die obigen Beispiele verdeutlichen. Auch ist in den Fällen, in denen theoretisch eine Reidentifikation im Zuge eines Randsummen- oder Fallzahlproblems, also aufgrund der Einzigartigkeit oder Besonderheit des Einzeldatensatzes, denkbar ist, stets Zusatz- oder Vorwissen von Nöten. Soweit es nicht um allgemein zugängliche Informationen geht, stellt sich also die Frage, inwieweit Mittel zur Verfügung stehen, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden (Erwägungsgrund 26 DS-GVO). Es ist also zu prüfen, ob ein realistisches Risiko besteht, dass die nutzungsberechtigte Stelle auf das Zusatzwissen zugreifen kann. Es sind Fälle denkbar, in denen die nutzungsberechtigte Stelle über eigene Daten verfügt, die sie zumindest theoretisch mit den Versorgungsdaten abgleichen könnte. Das wäre etwa gegeben, wenn Krankenkassen selbst Untersuchungen durchführen oder bei einem Mitglied einer Universität, das gleichzeitig Zugriff auf Behandlungsdaten aus dem zugehörigen Universitätsklinikum hat. In solchen Fällen wird zumindest teilweise vom Vorliegen von personenbezogenen Daten aus Sicht dieser Stellen auszugehen sein. In die Wahrscheinlichkeitsprüfung der Identifikation mit einzubeziehen ist auch die Frage, welches Interesse überhaupt an einer Reidentifikation besteht. Dabei hat ein erheblicher Teil der nutzungsberechtigten Stellen meist keinen Nutzen von einer Identifikation einzelner Versicherter. So ist es für einen Wissenschaftler nicht bedeutsam, wessen Datensatz gerade untersucht wird, lediglich die Krankheits- und Behandlungsverläufe sind von Interesse. Jedoch sind generell durchaus kommerzielle und andere Interessen an der Zuordnung der Daten zu ihrem Ursprung denkbar. Insbesondere bei der Vergabe von Krediten oder beim Abschluss von Versicherungen können Informationen über den Gesundheitszustand eines möglichen Vertragspartners sehr wertvoll sein. Ebenfalls denkbar sind Hackerangriffe, entweder mit dem Ziel der pauschalen Veröffentlichung aller Daten oder der Veräußerung dieser. Nicht zuletzt könnten in einem solchen Szenario insbesondere in der Öffentlichkeit stehende Personen erpresst oder diskreditiert werden.

Ist das Identifikationsrisiko eines Einzeldatensatzes jedoch im vernachlässigbaren Bereich, so handelt es sich für die nutzungsberechtigten Stellen teilweise auch um anonyme Daten. Denn rechtliche Mittel¹⁷⁸ (s.o. B. I. 2.), um mögliches Zusatzwissen über Versicherte zu erlangen, das über die eigenen Informationen hinausgeht, sind nicht ersichtlich. Legt man also den verschärften relativen Personenbezugsbegriff¹⁷⁹ des EuGH als Maßstab zugrunde, so ist im Einzelfall zu differenzieren und nicht alle Einzeldatensätze können als personenbezogen angesehen werden.

Über die Anonymität bzw. Personenbeziehbarkeit der Einzeldatensätze lässt sich mithin keine pauschale Aussage treffen. Ein beachtlicher Teil der Einzeldatensätze wird als anonym zu betrachten sein. Für diese wäre kein datenschutzrechtlicher Zulässigkeitstatbestand zur Verarbeitung notwendig. Wegen des Restrisikos ist es gleichwohl erforderlich, dass § 303e Abs. 3 S. 2 SGB V i.V.m. § 5 Abs. 5 DaTraV für alle verbleibenden identifizierbaren Daten einen Zulässigkeitstatbestand innerhalb des Spielraums der Öffnungsklauseln der DS-GVO (s.o. B. II. 5. b)) generiert.

c) Verbot der Reidentifikation

Ein ausdrückliches Verbot der Reidentifikation durch nutzungsberechtigte Stellen findet sich bislang nur in der Nutzungsordnung der Datenaufbereitungsstelle.¹⁸⁰ Das Verbot der Reidentifikation aus § 303c Abs. 2 S. 2 SGB V richtet sich nach Wortlaut und Systematik der Norm an die Datenaufbereitungsstelle. Dieser Regelung liegt das Verständnis zugrunde, dass die Datenaufbereitungsstelle die Reidentifikation durch nutzungsberechtigte Stellen unmöglich machen soll. Es ist daher zweckmäßig, das Reidentifikationsverbot in die §§ 303a ff. SGB V aufzunehmen.

2. Forschungsprivileg und Erforderlichkeit

Bei Forschungsanträgen an die Datenaufbereitungsstelle nimmt diese nach § 303e Abs. 3 S. 1 SGB V i.V.m. § 5 Abs. 3 Nr. 4 DaTraV eine Erforderlichkeitsprüfung bezüglich des Datenumfangs vor. Die Erforderlichkeitsprüfung aus § 303e Abs. 3 S. 1 SGB V i.V.m. § 5 Abs. 3

¹⁷⁸ Kriterium des EuGH, vgl. EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 f. – Breyer = ZD 2016, 24 m. Anm. Kühling/Klar.

¹⁷⁹ Siehe zum Begriff Kühling/Klar, ZD 2016, 27.

¹⁸⁰ Informationssystem Versorgungsdaten (Datentransparenz): Nutzungsordnung, Version 01-05-000, S. 3, abrufbar unter <https://www.dimdi.de/static/.downloads/deutsch/versorgungsdaten-nutzungsordnung.pdf>, abgerufen am 24.6.2019.

Nr. 4 DaTraV ist nicht zu verwechseln mit der Frage, ob die Datenverarbeitung *zur Erfüllung der Aufgabe der Nutzungsberechtigten Stelle* erforderlich ist, § 303e Abs. 1 SGB V. Ebenfalls eine andere Frage wird in § 303e Abs. 3 S. 3 SGB V geregelt, nämlich ob ausnahmsweise der *Zugriff auf Einzeldatensätze* erforderlich ist. Bei § 303e Abs. 3 S. 1 SGB V i.V.m. § 5 Abs. 3 Nr. 4 DaTraV geht es hingegen darum, ob *Umfang und Struktur der Daten* im beantragten Maße erforderlich sind. In praktischer Hinsicht bedeutet dies, dass geprüft wird, ob die gewählte Auswertungsmethodik nur auf die Daten zugreift, die für die Beantwortung der Forschungsfragen benötigt werden.

Diese Erforderlichkeitsprüfung birgt ein gewisses Kollisionspotenzial mit der Forschungsfreiheit aus Art. 5 Abs. 3 S. 1 GG. Soweit sich eine Nutzungsberechtigte Stelle auf die Forschungs- bzw. Wissenschaftsfreiheit berufen kann, also insbesondere bei Anträgen von Universitäten¹⁸¹, sind der Erforderlichkeitsprüfung durch eine verfassungskonforme Auslegung des SGB V und der DaTraV Grenzen zu setzen. So darf es nicht zu einer Forschungszensur durch die Datenaufbereitungsstelle als grundrechtsverpflichtete öffentliche Stelle kommen. Dies wäre der Fall, wenn man den Forschenden diktieren würde, welche Daten sie für ihre Forschung „zu brauchen haben“, um die selbst gewählten Forschungsziele zu erreichen. Denn eine staatliche Beeinflussung von der Definition wissenschaftlicher Fragestellung über die Wahl der Methodik bis hin zur Bewertung der Forschungsergebnisse verstieße gegen die Forschungsfreiheit aus Art. 5 Abs. 3 S. 1 GG.¹⁸²

Geboten ist eine Erforderlichkeitsprüfung, wenn auch in eingeschränktem Umfang, mit Blick auf das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dennoch (zum Recht auf informationelle Selbstbestimmung siehe C. I. 2.). Denn es besteht die Gefahr, dass es bei missbräuchlicher Nutzung der Versorgungsdaten über die Grenzen der Erforderlichkeit hinaus zu Persönlichkeitsrechtsverletzungen kommt. Insofern bietet sich eine auf eine „Plausibilitätsprüfung“ beschränkte Erforderlichkeitsprüfung als einschränkende verfassungskonforme Auslegung des § 303e Abs. 3 S. 1 SGB und des § 5 Abs. 3 Nr. 4 DaTraV an. Die Datenaufbereitungsstelle gleicht hiernach also nur ab, ob es plausibel erscheint, welche Daten mit Blick auf die Forschungsfrage abgerufen werden sollen.

Soweit ersichtlich, ist dies ohnehin schon gängige Praxis bei der Datenaufbereitungsstelle. So nimmt die Datenaufbereitungsstelle eine zweistufige Prüfung vor, wobei sie zunächst bewertet,

¹⁸¹ Siehe *Kempfen*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 40. Edition, Stand: 15.2.2019, Art. 5 Rn. 185.

¹⁸² Siehe *Starck/Paulus*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 5 Rn. 488; *Kempfen*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 40. Edition, Stand: 15.2.2019, Art. 5 Rn. 191.

ob die gewählte Methodik generell geeignet scheint, das Forschungsziel zu erreichen. Insoweit geht es nur darum, dass die gewählte Art der Datenanalyse nicht völlig widersprüchlich zum gesetzten Ziel ist. In einem zweiten Schritt werden dann die bei der Analyse erzielten Ergebnismengen betrachtet, wobei auch hier eine grobe Einschätzung erfolgt, ob diese nicht wesentlich zu weit gefasst sind und ob ein Reidentifikationsrisiko besteht. Ein derartiges Vorgehen kann künftig zweckmäßigerweise auch in den §§ 303a ff. SGB V oder zumindest in der DaTraV verankert werden (siehe hierzu C. III. 1. e)).

3. Reichweite der Zweckbindung im Bereich der Wissenschaft

Unklar ist derzeit, inwieweit Universitäten und dort tätige Forscher nach aktueller Gesetzeslage tatsächlich zur Forschung mit den Versorgungsdaten des DIMDI berechtigt sind. Das DIMDI als Datenaufbereitungsstelle zieht die Grenze der Zweckbindung relativ eng. So dürften Universitätsmitarbeiter zwar einen Datenzugang beantragen, aber keinesfalls für private Zwecke weiterverwenden, wozu auch Forschungsvorhaben wie Promotionen oder Habilitationen gerechnet werden.¹⁸³ Dabei stützt sich das DIMDI auf die Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).¹⁸⁴ Man könnte jedoch mit Blick auf den Gesetzeswortlaut durchaus zu einem weiteren Verständnis gelangen und eine umfassende Nutzung im universitären Umfeld als von § 303e SGB V umfasst ansehen.

Diese Frage schließt sich an die Frage an, ob der Katalog des § 303e Abs. 2 SGB V abschließend ist (s.o. B. II. 4. b)). Die beiden Fragen sind jedoch nicht deckungsgleich. Insbesondere sofern man dem Wortlaut des § 303e Abs. 2 S. 1 SGB V folgt und den Katalog als nicht abschließend versteht, lassen sich durchaus Anknüpfungspunkte für ein weites Verständnis zugunsten der Wissenschaft finden. Denn Hochschulen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung sind nach § 303e Abs. 1 Nr. 8 SGB V nutzungsberechtigte Stellen. Zwar ist in der Zweckbestimmung des § 303e Abs. 2 SGB V kein Punkt eingefügt, der ausdrücklich die „freie wissenschaftliche Forschung“ oder dergleichen mit einschließt. Doch betrachtet man den systematischen Zusammenhang zwischen dem wohl nicht abschließenden Katalog des Abs. 2 und Abs. 1 Nr. 8 des § 303e SGB V, so ist festzustel-

¹⁸³ So zumindest das *DIMDI* unter der Kategorie „FAQ Versorgungsdaten“ auf https://www.dimdi.de/dynamic/de/faq/#faq_1c499114_1, abgerufen am 24.6.2019.

¹⁸⁴ So das *DIMDI* unter der Kategorie „FAQ Versorgungsdaten“ auf https://www.dimdi.de/dynamic/de/faq/#faq_1c499114_1, abgerufen am 24.6.2019; zur Stellung der oder des BfDI siehe *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 693 f.

len, dass die „unabhängige wissenschaftliche Forschung“ auch Empfänger der Versorgungsdaten sein soll. Außerdem können Zwecke wie die „Verbesserung der Qualität der Versorgung“ oder „Längsschnittanalysen [...] zum Erkennen von Fehlentwicklungen und von Ansatzpunkten für Reformen“ durchaus durch eine auf Publikationen basierende freie wissenschaftliche Forschung erreicht werden. Auch die Wissenschaftsfreiheit aus Art. 5 Abs. 3 S. 1 GG als „objektive, das Verhältnis von Wissenschaft, Forschung und Lehre zum Staat regelnde Grundsatznorm“¹⁸⁵ spricht als Wertungsgesichtspunkt eher für ein weites Verständnis.¹⁸⁶ Schließlich stellt sich auch die Frage, wie die Trennung zwischen „öffentlicher“ und „privater“ Versorgungsforschung praktisch vollzogen werden soll. Denn die Interpretation, dass Forschungsvorhaben wie eine Promotion oder Habilitation einen vorwiegend privaten Zweck verfolgen, verkennt die Realität des Forschungsbetriebs. Nach dieser Logik wäre es auch nicht zulässig, dass ein Forscher einer Universität die Ergebnisse einer Studie auf Basis der Versorgungsdaten in einer Fachzeitschrift veröffentlicht, soweit dies auf eigene Rechnung geschieht. Vielmehr ist in diesem Kontext von einer Untrennbarkeit von Forschungsvorhaben und Veröffentlichung auszugehen. Denn es wird stets zumindest auch ein privater Zweck mit der Forschung verfolgt. Hierbei kann es keinen Unterschied machen, in welcher Form die Publikation einer Studie erfolgt. Auch Promotionen und Habilitationen leisten einen Beitrag zum wissenschaftlichen Prozess und sollten damit nicht vom Zugang zu den Versorgungsdaten ausgeschlossen werden. Nutzungsberechtigte Stelle ist dabei freilich nur die Hochschule, doch in welcher Form deren Mitglieder die Erkenntnisse publizieren, ist kaum ein tauglicher Anknüpfungspunkt für die Entscheidung über den Datenzugang.

Insgesamt lässt sich also schon nach derzeitiger Rechtslage sehr gut vertreten, dass jegliche wissenschaftliche Forschung im universitären Kontext, also auch beispielsweise im Rahmen einer Promotion oder Habilitation im Bereich der Versorgungsforschung, zum Datenzugang gemäß § 303e SGB V berechtigt ist.

Doch auch für die vom DIMDI und vom BfDI vertretene engere Auslegung finden sich gute Gründe. Diese Auffassung interpretiert den Telos der Norm enger und begrenzt den Zugang zu

¹⁸⁵ BVerfGE 35, 79, 114; 111, 333, 353; 130, 263, 299.

¹⁸⁶ Vgl. zum Einfluss der Forschungsfreiheit auf § 303e SGB V – allerdings dort in Bezug auf die Frage, ob ein Anspruch auf Bereitstellung des Volldatensatzes besteht – *Kingreen/Kühling*, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 42 f., abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019.

den Versorgungsdaten auf die öffentliche Versorgungsforschung. Zweck der §§ 303a ff. SGB V ist hiernach ausschließlich die Verbesserung der Versorgung durch öffentliche Stellen. Diese Interpretation lässt sich dabei durchaus auf die Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG stützen, wonach hier der Gesetzesvorbehalt besonders streng zu handhaben ist.¹⁸⁷ Konkret bedeutet dies, dass die Ermächtigungsgrundlagen zur Verarbeitung personenbezogener Daten stets besonders klar und bestimmt formuliert sein müssen, um das Recht auf informationelle Selbstbestimmung der Betroffenen zu wahren.¹⁸⁸ Vor diesem Hintergrund ist es durchaus verständlich, dass das DIMDI nicht in weiterem Maße Daten bereitstellt, als dies vom Gesetzeswortlaut des § 303e Abs. 2 SGB V ausdrücklich angeordnet wird. Aufgrund der jedenfalls verbleibenden Zweifel ist eine gesetzgeberische Klarstellung zweckmäßig (dazu C. III. 1. d)).

4. Prozedurale Ausdifferenzierung des Antragsverfahrens und Möglichkeit zur Risikoabwägung

Das Antragsverfahren sieht de lege lata die folgenden Prüfungspunkte für die Datenaufbereitungsstelle bei Bearbeitung eines Antrags auf Bereitstellung von Daten vor.

Zunächst wird die Nutzungsberechtigung der beantragenden Stelle nach § 303e Abs. 1 SGB V und § 5 Abs. 3 Nr. 1 DaTraV geprüft. Die Erforderlichkeit zur Aufgabenerfüllung der Stelle ist zwar Rechtmäßigkeitsvoraussetzung, wird aber von der Datenaufbereitungsstelle nicht geprüft, soweit man dem Wortlaut des § 303e Abs. 3 S. 1 SGB V folgt.

Sodann ist nach § 303e Abs. 2 und 3 S. 1 SGB V und § 5 Abs. 3 Nr. 1 DaTraV zu prüfen, ob der Zweck der Verarbeitung so gesetzlich vorgesehen ist.

Als nächster Schritt wird gemäß § 303e Abs. 3 S. 1 SGB V und § 5 Abs. 3 Nr. 4 DaTraV die Erforderlichkeit bezüglich Umfang und Struktur der Daten geprüft, wobei die Erforderlichkeitsprüfung teilweise auf eine Plausibilitätsprüfung zu beschränken ist (s.o. B. III. 2.).

¹⁸⁷ Vgl. hierzu umfassend *Kingreen/Kühling*, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 12 f., abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019.

¹⁸⁸ Vgl. *Kingreen/Kühling*, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 12, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019; kritisch dazu allerdings *Kingreen/Kühling*, JZ 2015, 213.

Zuletzt wird über die Art der Bereitstellung der Daten nach § 303e Abs. 3 S. 2 und 3 SGB V und § 5 Abs. 4 und 5 DaTraV entschieden, wobei nur Zugang zu Einzeldatensätzen gewährt wird, soweit dies erforderlich ist (s.o. B. II. 4. c)). Im Regelfall werden nur anonymisierte Ergebnismengen bereitgestellt.

Dabei ist gemäß § 303c Abs. 2 S. 2 SGB V i.V.m. § 5 Abs. 3 Nr. 5 DaTraV von Seiten der Datenaufbereitungsstelle sicherzustellen, dass es nicht zu einer Reidentifikation der Versicherten kommt. Eine weitergehende Ausdifferenzierung der Zugriffsberechtigungen (z.B. eine Differenzierung nach Vertrauenswürdigkeit und Sicherheitsstandards der jeweiligen nutzungsberechtigten Stelle, siehe hierzu unten C. III. 1. f)) ist gegenwärtig nicht im SGB V und in der DaTraV angelegt. Auch die Nutzungsordnung Datentransparenz nimmt keine weitere Differenzierung vor. Anknüpfungspunkt für eine Risikoabwägung kann nach geltendem Recht also vor allem § 303c Abs. 2 S. 2 SGB V sein, wonach eine Reidentifikation stets zu verhindern ist.

5. Auskunftsansprüche von Versicherten

Geht man davon aus, dass es sich bei einem Datensatz um personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO handelt, so hat die betroffene Person grundsätzlich ein Auskunftsrecht aus Art. 15 DS-DVO. Dies gilt, wie bereits festgestellt (s.o. B. I. 2.), nur für pseudonymisierte und nicht für anonymisierte Daten. Die meist mit anonymen Daten arbeitenden nutzungsberechtigten Stellen i.S.v. § 303e Abs. 1 SGB V sind demnach in der Regel keinen solchen Ansprüchen ausgesetzt. Anders stellt sich dies für die Datenaufbereitungsstelle dar, die über die pseudonymisierten Datensätze verfügt, bei denen teilweise eine Identifizierung möglich ist. Problematisch ist hierbei, dass die Datenaufbereitungsstelle, soweit sie sich gesetzeskonform i.S.v. § 303c Abs. 2 S. 2 SGB V verhält, keine versichertenbezogenen Auskünfte geben kann. Denn ihr selbst ist eine Zuordnung der Datensätze zu einzelnen Versicherten nicht möglich. Der Auskunftsanspruch kann daher nicht erfüllt werden, ohne zusätzliche Daten zu erheben. Art. 11 Abs. 2 DS-GVO stellt insoweit klar, dass hierzu auch keine Verpflichtung des Verantwortlichen besteht, sondern die betroffene Person gegebenenfalls ergänzende Informationen bereitstellen muss. In der Praxis wird sich die Datenaufbereitungsstelle daher nicht mit erfolgversprechenden Auskunftsansprüchen konfrontiert sehen.

6. Regelungsebene datenschutzrechtlicher Zulässigkeitstatbestände

Im Bereich der Datentransparenz gemäß den §§ 303a ff. SGB V stellt sich die Frage, inwieweit es zulässig ist, Regelungen auf der Ebene des SGB V offen zu lassen und erst auf der Verordnungsebene zu regeln. Der Parlamentsvorbehalt, der insbesondere im Datenschutzrecht eine besondere Prägung erfahren hat, könnte entgegenstehen.¹⁸⁹ Auch das Bestimmtheitsgebot aus Art. 80 Abs. 1 S. 2 GG muss gewahrt werden. Bei der Datentransparenz stellt sich dieses Problem insbesondere bei der Konkretisierung des Datenumfangs.

a) Parlamentsvorbehalt und Bestimmtheitsgebot

Grundsätzlich besagt der vom Bundesverfassungsgericht entwickelte Parlamentsvorbehalt, dass alle „wesentlichen“ Entscheidungen vom Gesetzgeber selbst zu treffen sind.¹⁹⁰ Dies leitet das Bundesverfassungsgericht aus dem Vorbehalt des Gesetzes und damit letztlich aus dem Rechtsstaatsprinzip, aber auch aus dem Demokratieprinzip, jeweils verankert in Art. 20 GG, ab.¹⁹¹ Wie weitreichend der Parlamentsvorbehalt zu verstehen ist, also letztlich die Frage, was „wesentlich“ ist, hängt von der jeweiligen Regelungsmaterie und insbesondere deren Grundrechtssensibilität ab.¹⁹² Für das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gilt dies in besonderer Weise. Eingriffe bedürfen hier grundsätzlich einer formell-gesetzlichen Grundlage, bloße Verwaltungsvorschriften genügen nicht.¹⁹³ Jedoch sollte dies nicht missverstanden werden. Der Gesetzgeber muss nicht für jede Art von Eingriff eine spezialgesetzliche Ermächtigung schaffen, soweit beispielsweise auch Generalklauseln genügen.¹⁹⁴ Was jedoch aus dem Parlamentsvorbehalt hervorgeht, ist eine Verpflichtung des Gesetzgebers zur Schaffung einer hohen Normklarheit bei gleichzeitiger Realisierung ausreichender Normbestimmtheit.¹⁹⁵

¹⁸⁹ Vgl. Kingreen/Kühling, JZ 2015, 213, 215 ff.

¹⁹⁰ BVerfGE 49, 89, 126 = NJW 1979, 359; BVerfGE 61, 260, 275; BVerfGE 80, 124, 132 = NJW 1989, 2877; BVerfGE 83, 130, 142, 151 f. = NJW 1991, 1471; BVerfGE 101, 1, 34 = NJW 1999, 3253; siehe auch Huster/Rux, in: Epping/Hillengruber (Hrsg.), BeckOK GG, 40. Edition, Stand: 15.2.2019, Art. 20 Rn. 106.

¹⁹¹ BVerfGE 104, 151 (208) = NJW 2002, 1559; BVerfGE 121, 135 = NJW 2008, 2018.

¹⁹² BVerfGE 98, 218, 251 = NJW 1998, 2515; BVerfGE 139, 69 = NVwZ 2014, 1219; Kalscheuer/Jacobsen, DÖV 2018, 523, 525.

¹⁹³ Kingreen/Kühling, JZ 2015, 213, 215.

¹⁹⁴ Kingreen/Kühling, JZ 2015, 213, 215, 218.

¹⁹⁵ Kingreen/Kühling, JZ 2015, 213, 215.

In Art. 80 Abs. 1 S. 2 GG findet sich zudem ein Bestimmtheitsgebot speziell hinsichtlich der Möglichkeit zur Verordnungsermächtigung. Zweck hiervon ist es, zu verhindern, dass der Gesetzgeber sich selbst entmachtet und Blankoermächtigungen erteilt.¹⁹⁶ Es muss demnach eine gewisse Vorstrukturierung der Verordnung durch den Gesetzgeber stattfinden.

Ein unionsrechtlicher Parlamentsvorbehalt spielt dagegen im Gesundheitsdatenschutzrecht bislang keine Rolle.¹⁹⁷

b) Bedeutung für die Regelungen der Datentransparenz

Konkret stellt sich die Frage bei § 303b Abs. 1 i.V.m. § 303a Abs. 2 Nr. 1 SGB V, woraus sich ergibt, in welchem Umfang Daten zum Zwecke der Datentransparenz erhoben werden. Hierbei wird in § 303b Abs. 1 SGB V auf den Datenumfang des Risikostrukturausgleichs aus § 268 Abs. 3 S. 14 i.V.m. S. 1 Nrn. 1 bis 7 SGB V verwiesen. § 303a Abs. 2 Nr. 1 SGB V ermächtigt das BMG, den Datenumfang in der DaTraV genauer zu definieren. Dort wird in § 3 Abs. 1 DaTraV aber lediglich ebenfalls auf § 268 Abs. 3 S. 14 i.V.m. S. 1 Nrn. 1 bis 7 SGB V verwiesen. Der Katalog des § 268 Abs. 3 S. 1 Nrn. 1 bis 7 SGB V gibt den groben Rahmen vor, welche Daten für den Risikostrukturausgleich erhoben werden. Gemäß § 268 Abs. 3 S. 14 SGB V wird dies noch weiter in der Risikostruktur-Ausgleichsverordnung (RSAV) konkretisiert.

Ein Gesetz im formellen Sinne als mögliche Eingriffsgrundlage liegt hier mit den obigen Normen des SGB V zumindest vor. Auch gibt § 268 Abs. 3 SGB V eine hinreichende Vorstrukturierung in Bezug darauf vor, welche Daten dann laut Verordnung konkret erhoben werden. Die bloße Tatsache, dass diese letzte Konkretisierungsstufe auf der Ebene einer Verordnung vollzogen wird, ist damit im Hinblick auf Art. 80 Abs. 1 S. 2 GG nicht bedenklich. Einzig die Normklarheit leidet unter der schwer nachzuvollziehenden Verweisungstechnik zwischen SGB V, DaTraV und RSAV. Immerhin findet hier in den §§ 303a ff. SGB V eine „Doppelverweisung“ statt, sowohl direkt auf § 268 SGB V als auch auf die DaTraV, die wiederum auf § 268 SGB V verweist. Nimmt man noch die RSAV hinzu, entsteht ein komplexes Bild, das gewisse Restzweifel daran entstehen lässt, ob das Gebot der Normklarheit gewahrt ist. Insoweit ist eine Vereinfachung der Verweisungen zu erwägen (dazu C. III. 1. b)).

¹⁹⁶ Voßkuhle/Wischmeyer, JuS 2015, 311, 313.

¹⁹⁷ Siehe hierzu Kingreen/Kühling, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 456 f.

7. Weitere Problemstellungen aus SGB V und X

a) § 76 SGB X

Neben den Datenschutzvorgaben sind für Gesundheitsdaten insbesondere die aus dem Berufs- bzw. Strafrecht abgeleiteten Berufsgeheimnisschutzvorschriften von großer Bedeutung. Diese sind zusätzlich zu den datenschutzrechtlichen Anforderungen zu prüfen („Zwei-Schranken-Prinzip“).¹⁹⁸ Ein Bruch des Geheimnisses, das das Vertrauensverhältnis zwischen Ärzten und Patienten schützt, wird in § 203 Abs. 1 Nr. 1 StGB mit Strafe bedroht. Neben den Berufsträgern, an die sich die Geheimhaltungspflichten originär richten, sind auch viele weitere Personen und Akteure in den Pflichtenkreis einbezogen. Dies gilt etwa für die berufsmäßig tätigen Gehilfen oder die bei Berufsträgern zur Vorbereitung auf den Beruf tätigen Personen sowie sonstige an der Berufsausübung mitwirkende Personen. Im Gesundheitswesen müssen derart von § 203 StGB geschützte Daten an Sozialversicherungsträger übermittelt werden, um insbesondere eine ordnungsgemäße Abrechnung zu ermöglichen. Diese Daten unterliegen dann dem Sozialgeheimnis nach Art. 35 SGB I. Werden derartige Daten, die ursprünglich von einem Berufsgeheimnis geschützt waren und nun dem Sozialgeheimnis unterliegen, an außenstehende Dritte übermittelt, so müssen – über die allgemeinen sozialdatenschutzrechtlichen Vorgaben hinaus – ergänzend die zusätzlichen Voraussetzungen des § 76 Abs. 1 SGB X erfüllt sein. Eine Übermittlung ist demnach nur zulässig, wenn auch ein Berufsträger die Daten übermitteln dürfte. Damit wird der Berufsgeheimnisschutz in gewisser Weise verlängert auf die Sozialträger. Das System gewährleistet die Vertraulichkeit besonders schützenswerter Sozialdaten und schützt damit auch das Vertrauensverhältnis zwischen Arzt und Patient, soweit aus zwingenden Gründen Daten aus diesem Vertrauensverhältnis an Sozialträger übermittelt wurden. Ausnahmen sind daher nur unter engen Voraussetzungen vorgesehen. Die Zulässigkeit von Ausnahmen aus diesem Schutzsystem ist daher neben dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) auch am Maßstab des Art. 12 Abs. 1 GG zu messen.

Es wäre zu erwägen, eine Übermittlung zu Forschungszwecken auch dann zuzulassen, wenn der Berufsträger selbst sie nicht zu diesem Zweck hätte übermitteln dürfen. Es ist jedoch grundsätzlich nicht einsichtig, dass Daten, die von einem Arzt an einen Sozialgeheimnisträger übermittelt wurden und die der Arzt selbst nicht zu Forschungszwecken übermitteln hätte dürfen,

¹⁹⁸ Weichert, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 Rn. 146.

nun vom Sozialgeheimnisträger an einen Dritten übermittelt werden sollen. Eine Globalausnahme für jegliche Forschungszwecke ist daher nicht zweckmäßig, da der Schutz des auch grundrechtlich (Art. 12 Abs. 1 GG) verbürgten Berufsgeheimnisses nicht dadurch unterlaufen werden darf, dass die Daten einen Umweg über einen Sozialgeheimnisträger nehmen. Zu Forschungszwecken können auch besonders schützenswerte Sozialdaten jedoch dann übermittelt werden, wenn sie im datenschutzrechtlichen Sinne anonym sind und zudem im Sinne des Berufsgeheimnisschutzes keine Zuordnung zu einer konkreten Person zulassen und damit kein Geheimnis darstellen, das die geschützte Arzt-Patienten-Beziehung betreffen könnte. Ferner kann das Interesse der Forschung, das sich in Art. 5 Abs. 3 S. 1 GG ebenfalls grundrechtlich verorten lässt, im Einzelfall das Interesse am besonderen Schutz der Vertraulichkeit einer Arzt-Patienten-Beziehung überwiegen. Dies kommt aber nur dann in Betracht, wenn ein erheblicher Mehrwert für die Forschung besteht und keine ernsthaften Gefahren für den Vertraulichkeitsschutz zu befürchten sind, also insbesondere die Identifizierung eines Patienten aufgrund der Art der Daten sehr unwahrscheinlich ist. Insoweit stellt sich jedoch das Problem, dass derzeit in § 76 Abs. 2 SGB X keine Ausnahme für die Forschung vorgesehen ist, so dass einer derartigen Datenübermittlung § 76 Abs. 1 SGB X derzeit im Regelfall entgegensteht (weiterführend dazu C. III. 2. a)).

b) § 78 SGB X i.V.m. § 305 Abs. 1 SGB V

Das Zusammenspiel des § 78 SGB X mit § 305 Abs. 1 SGB V erfordert eine vertiefte Betrachtung. § 78 Abs. 1 SGB X regelt eine Art verlängerten Sozialdatenschutz, indem es Empfängern von Daten, die dem Sozialdatenschutz unterliegen und die auch selbst nicht Sozialgeheimnisträger gemäß § 35 SGB I sind, auferlegt, diese Daten nur zu dem Zweck zu verarbeiten, zu dem sie übermittelt worden sind. Dadurch wird der Schutz der Sozialdaten auch gewährleistet, wenn im Einzelfall an einen außerhalb der Sozialgeheimnisträger stehenden Dritten Daten übermittelt werden müssen. Diese grundsätzlich sinnvolle Systematik ist dem Wortlaut nach auch anzuwenden, soweit die Übermittlung an den Dritten auf expliziten Wunsch des Versicherten erfolgt, denn ein Ausnahmetatbestand findet sich insoweit nicht. Der Telos der Norm muss jedoch zu einem anderen Ergebnis führen, denn der Versicherte könnte die Daten auch mit Hilfe des in § 305 Abs. 1 SGB V spezialgesetzlich und in Art. 15 Abs. 1 und 3 DS-GVO allgemein normierten Auskunftsanspruch an sich übermitteln lassen. Art. 15 Abs. 3 DS-GVO sieht auch explizit ein Recht auf eine Datenkopie vor. Die hierdurch erlangten Daten könnte

der Versicherer sodann an einen beliebigen Dritten übermitteln, der dann nicht den Restriktionen des § 78 SGB X unterliegen würde. Im Ergebnis kann es jedoch keinen Unterschied machen, ob der Versicherte einen umständlicheren Weg wählt oder aber auf seine Veranlassung Daten an den Dritten von dem auskunftspflichtigen Sozialgeheimnisträger übermittelt werden. Dogmatisch lässt sich das Ergebnis über eine teleologische Reduktion des § 78 SGB X unter Heranziehung des Rechtsgedankens aus § 305 Abs. 1 SGB V bzw. Art. 15 Abs. 3 DS-GVO erreichen. Unter der Voraussetzung, dass der Versicherte Anspruch auf den Erhalt einer Datenkopie hat und anstelle der Übermittlung an sich die Übermittlung an einen Dritten erbittet und der Sozialgeheimnisträger dieser Bitte Folge leistet, finden die Einschränkungen des § 78 SGB X keine Anwendung.

Es empfiehlt sich insoweit eine gesetzgeberische Klarstellung durch Aufnahme einer entsprechenden Ausnahme in § 78 SGB X (dazu C. III. 2. b)).

IV. Konsequenzen für die Reformvorschläge des Deutschen Ethikrates

Im Lichte der hier entwickelten Ergebnisse können die Konsequenzen für die Reformvorschläge des Deutschen Ethikrates aufgezeigt werden. Die Möglichkeiten und Grenzen der Anwendung der Grundprinzipien der Datensparsamkeit und Datenminimierung einerseits sowie der Zweckbindung andererseits wurden bereits dargelegt (s.o. I. 3. a) und b)), daher sollen im Folgenden noch ergänzend die Schlussfolgerungen für die Möglichkeiten einer zweckungebundenen Datenspende (dazu 1.) und das Konzept der Datensouveränität (dazu 2.) gezogen werden.

1. Die Möglichkeit einer zweckungebundenen Datenspende de lege lata

Die Möglichkeit, eigene Daten freiwillig für die Forschung zur Verfügung zu stellen, ist gerade im Gesundheitskontext von großer Bedeutung. Soweit Gesundheitsdaten durch die betroffene Person bewusst einem unbestimmten Personenkreis zugänglich gemacht wurden,¹⁹⁹ also veröffentlicht wurden, bedarf es keines besonderen Zulässigkeitstatbestandes und auch keiner Einwilligung, wie sich aus Art. 9 Abs. 2 lit. e DS-GVO ergibt. Daran dürfte der Betroffene aber regelmäßig angesichts der Sensibilität der Gesundheitsdaten kein Interesse haben. Für eine Datenspende zur medizinischen Forschung müssen die Daten jedoch nicht zwingend allgemein veröffentlicht werden, da auch der Zugriff eines bestimmten Personenkreises, namentlich von

¹⁹⁹ Weichert, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 78.

Forschern, grundsätzlich genügt. Die Zugänglichmachung an einen bestimmten Personenkreis kann durch die betroffene Person auch unter dem geltenden Recht legitimiert werden. Typisches Instrument dafür ist die Einwilligung der betroffenen Person. Die Einwilligung ist auch für die Verarbeitung besonderer Kategorien eine hinreichende Rechtsgrundlage, wenn sie die Voraussetzungen des Art. 9 Abs. 2 lit. a DS-GVO erfüllt. Problematisch ist insoweit aus datenschutzrechtlicher Sicht, dass häufig noch nicht genau absehbar ist, für welche konkreten Forschungsvorhaben die jeweiligen personenbezogenen Daten benötigt werden.

a) Allgemeine Anforderungen an eine Einwilligung im Forschungskontext

Die DS-GVO privilegiert im Gegensatz zur früheren Rechtslage²⁰⁰ die wissenschaftliche Forschung, indem sie eine Zweckänderung in gewissen Grenzen zulässt (Art. 6 Abs. 4 DS-GVO). Der strenge Zweckbindungsgrundsatz gilt insoweit also nur eingeschränkt. Ergänzend kann unter bestimmten Voraussetzungen eine Einwilligung in die Datenverarbeitung zu Forschungszwecken auch noch nicht absolut präzise absehbare Zwecke beinhalten und damit weiter gefasst sein („broad consent“)²⁰¹. Eine Einwilligung kann nach dem Erwägungsgrund 33 der DS-GVO für ganze Forschungsbereiche erteilt werden, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die DS-GVO, die grundsätzlich eine forschungsfreundliche Tendenz aufweist,²⁰² ermöglicht also bereits eine Datenspende in Form einer breit gefassten Einwilligung. Problematisch bleibt jedoch die trennscharfe Abgrenzung, wie weit die Zwecke der Datenverarbeitung gefasst werden können und die sich daraus ergebende Rechtsunsicherheit.

b) Rechtsunsicherheit als Hemmnis für eine effektive Forschung

Aufgrund der hohen Sanktionsdrohungen der DS-GVO ist insbesondere bei so sensiblen Daten wie Gesundheitsdaten der Verantwortliche möglicherweise eher geneigt, eine Datenverarbeitung im Zweifel besser zu unterlassen.²⁰³ Gerade für die medizinische Forschung ist diese Tatsache ein großes Hemmnis, denn die Reichweite einer Einwilligung und die Zulässigkeit einer

²⁰⁰ Vgl. zu den Änderungen durch die DS-GVO sehr instruktiv auch *Rammos*, Die Datenschutzrechtliche Zulässigkeit von Broad Consent für Forschungszwecke nach der DS-GVO, abrufbar unter: https://dsri.de/downloads/ha2017/2017_09_08_ppt_Rammos.pdf, abgerufen am 24.6.2019.

²⁰¹ Vgl. dazu Erwägungsgrund 33 der DS-GVO.

²⁰² *Bieresborn*, NZS 2017, 926, 931.

²⁰³ Dazu schon *Kühling/Sackmann*, DuD 2019, 347.

etwaigen Zweckänderung ist stets eine Frage des Einzelfalles. Jedenfalls in der gegenwärtigen Migrationsphase mit noch sehr geringer Rechtsprechungsdichte stehen die Verantwortlichen vor besonderen Herausforderungen.

2. Konzept der Datensouveränität

Bei aller Nebulösität des Konzepts der Datensouveränität, dürften die erkennbaren Kernforderungen, die sich um dieses Konzept ranken, im Bereich des SGB V und SGB X von geringerer Bedeutung sein als in anderen Sektoren der Gesundheitswirtschaft. Denn bei den Sozialgesetzbüchern geht es um eine hoheitlich überformte Materie, die in dem vom Ethikrat vorgelegten Konzept der Datensouveränität der strenger regulierten öffentlichen Sphäre und nicht der weniger regulierten marktlichen Sphäre zuzuordnen ist. Vor diesem Hintergrund ist auch das Instrument der Einwilligung im Sozialdatenschutzrecht bislang wenig wirkmächtig. Die Einwilligung wäre wohl das zentrale Vehikel, um Ansätzen einer Datensouveränität auf Basis des gegenwärtigen Rechtsrahmens stärker zum Durchbruch zu verhelfen. Es ist allerdings hervorzuheben, dass dabei die Unterschiede zu einer stärkeren Akzentuierung des eine Datenverarbeitung legitimierenden Verständnisses des Rechts auf informationelle Selbstbestimmung, die nach den verfassungsrechtlichen Grundsätzen möglich ist (dazu sogleich C. I. 2.), nur schwer auszumachen sind.

C. Mögliche Reformen de lege ferenda

Aufbauend auf den vorstehenden Ausführungen können nun der normative Änderungsbedarf identifiziert und konkrete Gesetzgebungsvorschläge entwickelt werden. Ein bereits vorliegender Referentenentwurf zur Reform des SGB V (im Folgenden SGV V-E) soll in diese Überlegungen miteinbezogen werden. Dazu sind zunächst die grundrechtlichen Steuerungsvorgaben zu klären (dazu I), die den Rahmen jeglicher Reformvorschläge bilden. Dasselbe gilt für die DS-GVO (dazu II.), die angesichts der vorliegend eingenommen mittelfristigen Reformperspektive nicht selbst Gegenstand von Reformüberlegungen sein kann, sondern vielmehr jeglichen Reformüberlegungen auf nationaler Ebene Grenzen setzt. Diese Rahmenbedingungen berücksichtigend, können sodann konkrete Reformvorschläge für das SGB V und SGB X erwo-gen und entwickelt werden (dazu III.). Die abgesehen von der Idee einer Datenspende eher auf einer abstrakteren Ebene angesiedelten Vorschläge des Deutschen Ethikrates sollen sodann in einem weiteren, abschließenden Schritt geprüft werden (dazu IV.).

I. Grundrechtliche Steuerungsvorgaben

Um den Handlungsspielraum des nationalen Gesetzgebers aufzuzeigen, ist zunächst eine Analyse der grundrechtlichen Rahmenbedingungen auf der Unionsebene (dazu 1.) und auf nationaler Ebene (dazu 2.) erforderlich.

1. Vorgaben aus dem Datenschutzgrundrecht des Art. 8 GrCh (und Art 7 GrCh)

Die Unionsrechte binden die Mitgliedstaaten „bei der Durchführung von Unionsrecht“, Art. 51 Abs. 1 S. 1 GrCh. Der EuGH legt den Begriff weit aus, so dass es ausreicht, wenn auch Unionsrecht berührt ist.²⁰⁴ Angesichts der prägenden DS-GVO als Sekundärrechtsakt und dem fast immer betroffenen freien Datenverkehr im Binnenmarkt gibt es im Datenschutzrecht kaum mehr denkbare Fälle, bei denen Unionsgrundrechte keine Anwendung finden. Dies ist – trotz Öffnungsklauseln – auch vorliegend der Fall.

Art. 7 GrCh normiert das Recht auf Achtung des Privatlebens und der Kommunikation und entspricht in Formulierung und Gewährleistungsgehalt weitgehend Art. 8 EMRK. Der Europäische Konvent, der den Text der Charta formuliert hat, stellt fest, dass die Rechte nach Art. 7 GrCh den Rechten entsprechen, die durch Art. 8 EMRK garantiert werden. Sie haben

²⁰⁴ EuGH, Urt. v. 26.2.2013, C-617/10, ECLI:EU:C:2013:105 – Åkerberg Fransson.

daher gemäß Art. 52 Abs. 3 GrCh grundsätzlich die gleiche Bedeutung und Tragweite wie die Konventionsrechte. Lediglich der Begriff der Korrespondenz wurde durch den Begriff der Kommunikation ersetzt, ohne dass sich hieraus materielle Unterschiede ergäben.²⁰⁵ Auch der EuGH hat die Entsprechung des Art. 7 GrCh mit Art. 8 EMRK sowohl in der Gewährleistungs- als auch in der Rechtfertigungsdimension festgestellt.²⁰⁶ Zentrale ebenfalls in Art. 8 GrCh zu berücksichtigende Einschränkungsgründe sind in Art. 52 Abs. 1 GrCh enthalten. Die Bestimmung formuliert darüber hinaus die wesentlichen Schranken der Einschränkungsmöglichkeiten, nämlich

- die Notwendigkeit einer gesetzlichen Ermächtigungsgrundlage für einen Eingriff in das betreffende Grundrecht,
- die Verfolgung eines legitimen Ziels und
- den Verhältnismäßigkeitsgrundsatz.²⁰⁷

Art. 8 GrCh normiert explizit ein Datenschutzgrundrecht. Die Bestimmung ist damit grundsätzlich *lex specialis* gegenüber Art. 7 GrCh.²⁰⁸ Zunächst stellte der EuGH in diesem Zusammenhang lediglich fest, dass Art. 8 Abs. 1 GrCh in engem, konkretisierendem Verhältnis zu Art. 7 GrCh stehe,²⁰⁹ ohne damit jedoch insoweit eine grundlegende und dogmatisch überzeugende Abgrenzung vorzunehmen. Zuletzt wurde indes deutlich, dass das Gericht beide Grundrechte nebeneinander anwendet und weitgehend parallel begreift.²¹⁰

Der sachliche Schutzbereich umfasst in Anlehnung an das sekundärrechtliche Datenschutzrecht personenbezogene Daten, also alle Informationen über eine bestimmte oder bestimmbare

²⁰⁵ Erläuterungen des Präsidiums des Europäischen Konvents, ABl. EU 2004, C 310, 430; *Jarass*, EU-Grundrechte, 2005, § 12 Rn. 2 f.; *Bernsdorff*, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 7 Rn. 24; *Grabenwarter/Pabel*, EMRK, 6. Aufl. 2016, § 22 Rn. 10; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, GrCh Art. 7 GrCh Rn. 10.

²⁰⁶ EuGH, Urt. v. 9.11.2010, C-92/09 u. C-93/09, ECLI:EU:C:2010:662 – Schecke und Eifert, Rn. 52, 59, 72 u. 87.

²⁰⁷ *Jarass*, Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 8 Rn. 11 ff.

²⁰⁸ *Jarass*, Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 8 Rn. 4; *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 8 GrCh Rn. 1 f.; *Wolff*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar EUV, GRC, AEUV, Bd. 1, 2017, Art. 8 GrCh Rn. 3.

²⁰⁹ EuGH, Urt. v. 9.11.2010, C-92/09 u. C-93/09, ECLI:EU:C:2010:662, Rn. 47 – Schecke und Eifert.

²¹⁰ EUGH, Urt. v. 8.4.2014, C-293/12 und C-594/12, ECLI:EU:C:2014:238 – Digital Rights Ireland und Seitlinger u.a.; vgl. zuletzt auch Gutachten 1/15 v. 26.7.2017, ECLI:EU:C:2017:592, Rn. 133 – PNR-Abkommen mit Kanada.

Person.²¹¹ In den persönlichen Schutzbereich fallen natürliche und juristische Personen, sofern das Grundrecht wesensmäßig auf diese anwendbar ist.²¹² Diese Auffassung wird vom EuGH geteilt. Allerdings erachtet er juristische Personen beispielsweise bereits dann als grundrechtsberechtigt im Hinblick auf Art. 8 Abs. 1 GrCh, soweit der zu veröffentlichende Name der juristischen Person eine oder mehrere natürliche Personen bestimmt.²¹³

Einen Eingriff²¹⁴ in Art. 8 GrCh stellt die Verarbeitung personenbezogener Daten dar, so wie sie i.S.d. ergangenen Sekundärrechts und des SGB V und X zu verstehen ist. Verarbeitung ist somit der Oberbegriff für alle Datenverarbeitungsschritte, von der Erhebung über die Weitergabe bis hin zur Löschung der personenbezogenen Daten.²¹⁵

Ein Eingriff bedarf der Rechtfertigung. Unionsgrundrechte werden dabei nicht schrankenlos gewährleistet. Insbesondere ist auch hier wiederum Art. 52 GrCh zu beachten. Art. 8 Abs. 2 S. 1 GrCh enthält eine Qualifikation der Einschränkungsgünde.²¹⁶ So dürfen Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“. Damit werden neben dem in Art. 52 Abs. 1 S. 1 GrCh enthaltenen Erfordernis einer gesetzlichen Grundlage weitere, in der datenschutzrechtlichen Grundrechtsdogmatik und in der Datenschutzgesetzgebung entwickelte Vorgaben primärrechtlich verankert: nämlich zum einen der Zweck-

²¹¹ Kingreen, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, GrCh Art. 8 GrCh Rn. 9. Im Übrigen ist eine im Ergebnis unschädliche, in grundrechtsdogmatischer Hinsicht jedoch noch divergierende Schutzgehaltserfassung des EuGH und des EuG festzustellen, vgl. EuG, T-194/04, ECLI:EU:T:2007:334 – Bavarian Lager, Rn. 111 ff. und Urt. v. 29.6.2010, C-28/08 P, ECLI:EU:C:2010:378, – Kommission/Bavarian Lager, Rn. 59 f.; Wolff, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar EUV, GRC, AEUV, Bd. 1, 2017, Art. 8 GrCh Rn. 12.

²¹² Diff. Bernsdorff, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 8 Rn. 18; s.a. Goldhammer/Sieber, JuS 2018, 22.

²¹³ EuGH, Urt. v. 9.11.2010 C-92/09 u. C-93/09, ECLI:EU:C:2010:662 – Schecke und Eifert, Rn. 53; kritisch dazu Kingreen, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, GrCh Art. 8 GrCh Rn. 11.

²¹⁴ Die korrekte Terminologie der Grundrechtsprüfung auf Unionsebene ist eigentlich „Anwendungsbereich – Einschränkungen – Rechtfertigung“. Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im Folgenden auch bei den Unionsgrundrechten die ebenfalls gebräuchliche deutsche Terminologie verwendet.

²¹⁵ Vgl. auch Bernsdorff, in: Meyer (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 8 Rn. 16; Jarass, Kommentar zur Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 8 Rn. 8; Kingreen, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, GrCh Art. 8 GrCh Rn. 12.

²¹⁶ Vgl. auch Schorkopf, in: Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Aufl. 2015, § 16 III 3 Rn. 47.

bindungsgrundsatz und zum anderen der „Zulässigkeits-Dreiklang“ aus Einwilligung, gesetzlicher Spezial- und Allgemeinregelung. Eine Einwilligung kann dabei einen Grundrechtseingriff allerdings nur legitimieren, wenn sie hinreichend informiert und freiwillig erfolgt. Sodann sind nach der Rechtsprechung des EuGH bei Wahrung eines hohen Datenschutzstandards die Ausnahmen und Einschränkungen von Art. 8 Abs. 1 GrCh auf das „absolut Notwendige“ zu beschränken.²¹⁷ Dies schlägt auch auf die Abwägung durch, in dessen Rahmen der EuGH dem Datenschutz eine hohe Bedeutung beimisst.

Darüber hinaus normiert Art. 8 Abs. 2 S. 2 GrCh mit einem Auskunfts- und Berichtigungsanspruch prozedurale, Art. 8 Abs. 3 GrCh mit der Verpflichtung auf eine Überwachung der Einhaltung der Schutzgehalte durch eine unabhängige Instanz institutionelle Datenschutzrechtsaspekte. Hier schließt sich der Kreis zu den Vorgaben des Bundesverfassungsgerichts im Volkszählungsurteil, die dementsprechend aufgefächert wurden. Weder Art. 8 Abs. 2 GrCh noch Art. 8 Abs. 2 EMRK führen im Übrigen zu einer Ausdehnung der Schranken.²¹⁸

2. Vorgaben aus dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG

Die DS-GVO belässt den nationalen Gesetzgeber insbesondere durch die – gerade im Gesundheitswesen besonders relevanten – Öffnungsklauseln umfangreiche Spielräume, die unter anderem durch die bereichsspezifischen Regelungen in den SGB V und X ausgefüllt werden. Da der nationale Gesetzgeber bei der Ausgestaltung der Spielräume einerseits – wie bei jedem nationalen Gesetz – die nationale Verfassung zu beachten hat und andererseits in Durchführung von Unionsrecht handelt, gelten insoweit die Grundrechte des Grundgesetzes und europäische Grundrechte parallel.²¹⁹ Auch die Ausführung der datenschutzrechtlichen Normen erfolgt im Wesentlichen durch nationale Behörden, die insoweit ebenfalls einer parallelen Grundrechtsbindung unterliegen. Sollte es zu Interferenzen zwischen den Schutzbereichen der korrespondierenden Normen kommen, insbesondere in multipolaren Grundrechtssituationen, so bleibt es

²¹⁷ Zuletzt EuGH, Gutachten 1/15 v. 26.7.2017, ECLI:EU:C:2017:592 – PNR-Abkommen mit Kanada, Rn. 140; ferner Urt. v. 16.12.2008, C-73/07, ECLI:EU:C:2008:727, Rn. 56 ff. – Satakunnan Markkinapörssi und Satamedia und Urt. v. 9.11.2010, C-92/09 u. C-93/09, ECLI:EU:C:2010:662 – Schecke und Eifert, Rn. 77.

²¹⁸ Jarass, EU-Grundrechte, 2005, § 13 Rn. 11.

²¹⁹ EuGH, Urt. v. 26.2.2013, C-617/10, ECLI:EU:C:2013:105 – Åkerberg Fransson; Urt. v. 6.3.2014, C-206/13, ECLI:EU:C:2014:126 – Siragusa; vgl. außerdem allgemein zur Frage der parallelen Anwendbarkeit von Grundgesetz und Grundrechtecharta Ludwigs/Sikora, JuS 2017, 385, 390 f.

beim Anwendungsvorrang des Unionsrechts, so dass insoweit letztlich die Maßstäbe der Unionsgrundrechte ausschlaggebend sind.²²⁰ Von Bedeutung bleiben wird die nationale Grundrechtsdogmatik aber allemal, zumal ein Großteil der verfassungsgerichtlichen Rechtsprechung im Datenschutzrecht zu Normen im bipolaren Bürger-Staat-Verhältnis ergangen ist und in Bereichen, in denen erhebliche mitgliedstaatliche Ausgestaltungsspielräume verbleiben, was gerade für den vorliegenden Bereich des Sozialdatenschutzes besonders relevant ist.

Das Bundesverfassungsgericht hat 1983 in seinem wegweisenden Volkszählungsurteil, in dem das Gericht die Verfassungsmäßigkeit des damaligen Volkszählungsgesetzes zu beurteilen hatte, aus dem Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) das Recht auf informationelle Selbstbestimmung abgeleitet.²²¹ Darunter ist die Befugnis des Einzelnen zu verstehen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.²²² Aufgrund der Beeinflussung des Allgemeinen Persönlichkeitsrechts durch Art. 1 Abs. 1 GG besteht auch für das Recht auf informationelle Selbstbestimmung ein entsprechender Menschenwürdebezug. Der Schutzbereich erstreckt sich auf jede Form der Erhebung personenbezogener Informationen.²²³ Gerade vor dem Hintergrund der modernen Datenverarbeitungsmöglichkeiten setzt das Recht auf informationelle Selbstbestimmung den Schutz des Einzelnen gegen eine unbegrenzte Verarbeitung seiner persönlichen Daten voraus. Die im Bereich der modernen Datenverarbeitung häufig fehlende Transparenz und die Nichterkennbarkeit der vielfältigen Datenverarbeitungsvorgänge kann sich auf das Kommunikationsverhalten der Nutzer negativ auswirken. Daher hat der Schutzbereich des Rechts auf informationelle Selbstbestimmung auch das Ziel, Einschüchterungseffekte zu verhindern, die dann entstehen können, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß.²²⁴ Die Vermeidung abschreckender Effekte durch fremdes Geheimwissen stellt eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlich-demokratischen Gemeinwesens

²²⁰ Vgl. auch Kühling/Sackmann, JURA 2018, 364; Ludwigs/Sikora, JuS 2017, 385 (391); zu Besonderheiten der sog. Identitäts- und Ultra-Vires-Kontrolle vgl. BVerfG, Urt. v. 30.6.2009, 2 BvE 2/08 u.a. = BVerfGE 123, 267 – *Lissabon*.

²²¹ Skeptisch gegenüber der Verselbstständigung als eigenes Grundrecht *Simitis*, NJW 1984, 398, 399.

²²² BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1 (43) – Volkszählung.

²²³ BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1 (43) – Volkszählung; Urt. v. 17.7.1984, 2 BvE 11/8367 = BVerfGE 67, 100, 143.

²²⁴ BVerfG, Urt. v. 2.3.2006, 2 BvR 2099/04 = BVerfGE 115, 166, 184.

dar.²²⁵ Dabei fasst das Bundesverfassungsgericht den Schutzbereich des Rechts auf informationelle Selbstbestimmung weit, wenn es feststellt, dass es vor dem Hintergrund der Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologie unter den Bedingungen der automatischen Datenverarbeitung kein an sich „belangloses“ Datum mehr geben kann.²²⁶ Jegliches personenbezogenes Datum fällt demnach in den Schutzbereich des Rechts auf informationelle Selbstbestimmung.

Das Bundesverfassungsgericht stellte später ferner fest, dass der grundrechtliche Schutz von Verhaltensfreiheit und Privatheit durch das Recht auf informationelle Selbstbestimmung schon auf der Stufe der Persönlichkeitsgefährdung beginnt.²²⁷ Diese Gefährdungslage könne bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen.²²⁸ Damit besteht eine Vorfeldwirkung des Rechts auf informationelle Selbstbestimmung gegebenenfalls sogar bevor es zu einer Datenverarbeitung kommt, jedenfalls aber bevor die Datenverarbeitung schädliche Auswirkungen auf den Betroffenen hat.

Wichtig ist es gleichwohl zu betonen, dass es um eine Selbstbestimmung geht, die sich auch darin äußern kann, Daten in großem Umfang – etwa in Form einer Datenspende – preiszugeben. Insofern ist die verfassungsrechtliche Konzeption begrifflich nicht paternalistisch angelegt. Sofern etwa eine Einwilligung – auch im Rahmen einer Datenspende – auf Basis von Transparenz und Freiwilligkeit erfolgt, kann sie daher problemlos Datenverarbeitungsprozesse legitimieren und sie ist gerade Ausdruck des Konzepts der informationellen Selbstbestimmung. Das so entwickelte Grundrecht enthält demnach zunächst eine materiell-rechtliche Dimension. Dazu gehört auch eine strenge Zweckbindung, die einen Gesetzeswortlaut verlangt, der die Zweckfestlegung im Gesetz selbst klar werden lässt,²²⁹ insbesondere sofern es um die Datenverarbeitung durch öffentliche Entitäten geht.²³⁰ Eine Datensammlung auf Vorrat ohne zuvor festgelegten Zweck ist mithin verboten.²³¹ Allein ein strenges Zweckbestimmungsgebot und

²²⁵ Vgl. BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1, 43 – Volkszählung.

²²⁶ BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1, 43 = NJW 1984, 419 (423) – Volkszählung.

²²⁷ BVerfG, Beschl. v. 13.6.2007, 1 BvR 1550/03 u.a. = BVerfGE 118, 168 = DStRE 2007, 1196, 1200.

²²⁸ BVerfG, Beschl. v. 13.6.2007, 1 BvR 1550/03 u.a. = BVerfGE 118, 168 = DStRE 2007, 1196, 1200 f.

²²⁹ BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1 (46) – Volkszählung; siehe auch Urt. v. 27.6.1991, 2 BvR 1493/89 = BVerfGE 84, 239, 280; Beschl. v. 7.3.1995, 1 BvR 1564/93 = BVerfGE 92, 191, 197.

²³⁰ Zur Bedeutung der Unterscheidung zwischen einer Datenverarbeitung durch private und öffentliche Stellen vgl. auch *Kingreen/Kühling*, JZ 2015, 213.

²³¹ BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1 = NJW 1984, 419, 422 – Volkszählung.

ein anspruchsvoller Gesetzesvorbehalt reichen indes nicht aus, um die realen Gefährdungen hinreichend einzudämmen. Daher tritt ergänzend eine Grundrechtssicherung durch Verfahren und Organisation hinzu, die sich insbesondere in Form von Informationspflichten und institutionellen Einrichtungen wie der eines Datenschutzbeauftragten entfaltet. Die Konkretisierung jener begleitenden Organisationsaufgaben ist sodann Aufgabe des Gesetzgebers.

Zugleich hat das Bundesverfassungsgericht betont, dass ein derartiges Verfügungsrecht nicht schrankenlos gewährleistet sein kann. Trotz des Menschenwürdebezuges erlaubt die Gemeinwohlebindung des Rechts auf informationelle Selbstbestimmung eine Öffnung gegenüber Beschränkungen, die durch überwiegende Allgemeininteressen gerechtfertigt sind. Diese bedürfen aber einer gesetzlichen Grundlage, die insbesondere dem Grundsatz der Verhältnismäßigkeit und dem Gebot der Normenklarheit entsprechen muss.²³²

II. Die DS-GVO als Reformobjekt und Rahmen nationaler Reformen

Die gegenwärtigen Debatten um die DS-GVO zeigen zwar einerseits, dass sicherlich gute Gründe für Reformen bestehen. So wäre etwa zu erwägen, die Öffnungsklauseln zurück zu fahren. Allerdings zeigt die Genesis, dass die DS-GVO als mühsamer Kompromiss im Trilog von Kommission, Parlament und Rat ausverhandelt wurde und nun – nicht zuletzt aufgrund der Öffnungsklauseln – eine große Herausforderung darin besteht, in den Mitgliedstaaten einen DS-GVO-konformen Rechtszustand im Zusammenspiel mit den bestehenden und modifizierten sektorspezifischen und allgemeinen datenschutzrechtlichen Vorgaben herzustellen. Auch der schleppende Reformprozess hinsichtlich der ePrivacy-VO, der schon längst hätte abgeschlossen sein sollen, offenbart die Mühen einer Kompromissfindung in datenschutzrechtlichen Fragen. Vor diesem Hintergrund ist es mittelfristig wenig wahrscheinlich, dass eine Reformdebatte auf unionaler Ebene tatsächlich zu Reformen führen wird. So wurde die Überarbeitung der Vorgängerregelung in Form der RL 95/46/EG Anfang 2012 mit dem Entwurf der Kommission gestartet und konnte erst mehr als vier Jahre später im Mai 2016 abgeschlossen werden. Die Vorgängerregelung hat damit mehr als zwei Dekaden gegolten. Vor diesem Hintergrund ist der Abschluss einer substantiellen Reform der DS-GVO mittelfristig und jedenfalls in der nächsten Dekade sehr unwahrscheinlich. Angesichts der eher kurz- und mittelfristigen

²³² BVerfG, Urt. v. 15.12.1983, 1 BvR 209/83 u.a. = BVerfGE 65, 1, 43 f. – Volkszählung; Beschl. v. 4.4.2006, 1 BvR 518/02 = BVerfGE 115, 320 = MMR 2006, 531, 532.

Perspektive des vorliegenden Gutachtens wird die DS-GVO daher primär als Rahmen nationaler Reformoptionen und nicht als Reformobjekt betrachtet.

III. Reformen im SGB V und SGB X

Die nachfolgenden Vorschläge analysieren und entwickeln den bisherigen Überlegungen folgend eine Reihe von Anpassungen in SGB V und SGB X. Im Vordergrund stehen dabei die relevanten Kernvorgaben in den §§ 303a ff. SGB V (dazu 1.). Ergänzend wird in Bezug auf das SGB X ein punktueller Anpassungsbedarf in § 76 Abs. 2 und § 78 identifiziert (dazu 2.). Die soeben skizzierten grundrechtlichen Steuerungsvorgaben und die Regelungen der DS-GVO geben hierzu den Rahmen vor. Gerade die DS-GVO belässt jedoch auch einen nicht unerheblichen Spielraum. Davon bleibt die Tatsache unberührt, dass es sinnvoll wäre, den gesamten normativen Rahmen des Gesundheitsdatenschutzrechts einer komplexitätsreduzierenden Reform zu unterziehen.²³³

1. Datentransparenz gemäß den §§ 303a ff. SGB V

Im Lichte der obigen Ausführungen zur aktuellen Rechtslage (s.o. B. II. und III. 1. bis 6.) sind mit Blick auf die folgenden Reformüberlegungen bereits vorliegende Referentenentwürfe und ein Kabinettsentwurf mit einzubeziehen, deren Inhalt daher zunächst knapp zu skizzieren ist (dazu a)). Kern der folgenden Überlegungen soll sein, die Nutzbarkeit der Versorgungsdaten für die Wissenschaft und aus Allgemeinwohlinteressen heraus zur Verbesserung der Versorgung zu erhöhen und zugleich den hohen Standard des Persönlichkeitsrechtsschutzes zu wahren. Im Einzelnen betrifft dies nach einer Klärungen der Regelungsebene des Datenschutzes (dazu b)) die Möglichkeiten der Integration von Institutskennzeichen vor dem Hintergrund des Betriebs- und Geschäftsgeheimnisses (dazu c)), Fragen der Zweckbindung und Öffnung für die Forschung (dazu d)), den Umfang und die Ausrichtung der Erforderlichkeitsprüfung (dazu e)), die vor dem Hintergrund der Risikoabwägung mögliche prozedurale Ausdifferenzierung (dazu f)), die Verwendung und gegebenenfalls legislative Konkretisierung der Begriffe „anonymisiert“ und „pseudonymisiert“ (dazu g)), der Verbot der Reidentifikation und die Sanktionierung

²³³ Zum Reformbedarf bereits *Kingreen/Kühling*, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 2 ff., abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019; *Kingreen/Kühling*, in: *Kingreen/Kühling* (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 460 ff.; *Kingreen/Kühling*, JZ 2015, 213.

von Sanktionen dagegen (dazu h)) sowie schließlich die Verknüpfung mit weiteren Sozialdaten und Behandlungsdaten (dazu i)).

a) Referenten- und Kabinettsentwurf

aa) Referentenentwurf

Zu den §§ 303a ff. SGB V und zur DaTraV liegen jeweils Referentenentwürfe mit teils nicht unerheblichen Änderungsvorschlägen vor²³⁴, deren Neuerungen sich im Vergleich zum aktuellen Recht wie folgt zusammenfassen lassen:

Die erste und rechtstatsächlich relevante Änderung betrifft die Herkunft und den Umfang der Daten. Diese sollen nach § 303b Abs. 1 SGB V-E künftig nicht mehr vom Bundesversicherungsamt stammen, sondern beim Spitzenverband Bund der Krankenkassen als Datensammelstelle gesammelt werden. Jedoch sollen übergangsweise weiter die Methoden der Datensammlung verwendet werden, bis die Datensammelstelle ihre Arbeit vollständig aufgenommen hat (vgl. „Haushaltsausgaben“). Die Sammlung der Daten zum Zweck der Erhaltung des Informationssystems der Versorgungsdaten wird damit wohl aufwändiger. Dabei ist in § 303b Abs. 1 SGB V-E explizit vorgesehen, welche Daten erhoben werden (Alter, Geschlecht, Wohnort, Versicherungsverhältnis, Kosten- und Leistungsdaten nach §§ 294 bis 302 SGB V, usw.). Eine Konkretisierung dieser ohnehin recht ausführlichen Angaben über den Datenumfang soll nach § 303a Abs. 3 Nr. 1 SGB V-E und § 303b Abs. 1 S. 2 SGB V-E weiterhin auf der Verordnungsebene stattfinden. In § 3 Abs. 1 DaTraV-E wird sodann auf § 267 SGB V verwiesen. Dies würde inhaltlich eine Erweiterung der Angaben darstellen, insbesondere zumal bislang einige Informationen nur unvollständig vorhanden sind. Zu beachten ist insbesondere, dass gemäß § 303b Abs. 1 S. 1 SGB V-E auch „Angaben zu den abrechnenden Leistungserbringern“ gespeichert werden sollen. Damit sollen also auch Institutionskennzeichen mit einbezogen werden, die nach § 303b Abs. 2 S. 3 SGB V-E zu pseudonymisieren sind.

Die Verordnungsermächtigung in § 303a Abs. 3 SGB V-E für die DaTraV wurde auch im Übrigen leicht abgewandelt und um einige Aspekte erweitert (z.B. um die „Aufbereitung und Bereitstellung der Daten durch das Forschungszentrum“). Gleich bleiben soll jedoch, dass das DIMDI weiterhin zwei Funktionen ausführt, wobei die Datenaufbereitungsstelle nun in Forschungsdatenzentrum umbenannt werden soll.

²³⁴ §§ des Referentenentwurfs zu den §§ 303a ff. SGB V werden gekennzeichnet mit SGB V-E, solche des Referentenentwurfs zur DaTraV mit DaTraV-E.

Von der derzeitigen Regelung abweichend soll in § 303d Abs. 2 S. 1 SGB V-E eine 30-Jahres-Frist zur Löschung aller versichertenbezogener Einzelangaben eingeführt werden. Aktuell gilt gemäß § 303d Abs. 1 S. 2 SGB V eine Löschpflicht, sobald die Einzeldaten nicht mehr erforderlich sind.

Neu in § 303d Abs. 3 SGB V-E ist eine Konkretisierung der Aufgaben des Forschungsdatenzentrums. Derzeit heißt es in § 303d Abs. 1 S. 1 SGB V nur, die Datenaufbereitungsstelle habe die Daten aufzubereiten und zur Verfügung zu stellen. Eine weitere Spezifikation erfolgt erst auf der Ebene der DaTraV. Insbesondere führt § 303d Abs. 3 SGB V-E nun an, dass es zu den Aufgaben des Forschungsdatenzentrums gehört „das spezifische Reidentifikationsrisiko zu bewerten und unter größtmöglicher Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen zu reduzieren“, aber auch „die wissenschaftliche Erschließung der Daten zu fördern“.

Die nutzungsberechtigten Stellen bleiben unverändert. Hinzu kommen nun ausdrücklich in § 303e Abs. 1 Nr. 8 SGB V-E „außeruniversitäre Forschungseinrichtungen“. Dazu zählt laut Begründung beispielsweise die Fraunhofer Gesellschaft oder die Max-Planck-Gesellschaft. Dies stellt aber wohl nur eine Verdeutlichung und keine tatsächliche Erweiterung des Kreises der berechtigten Stellen dar. Denn derartige Forschungseinrichtungen fallen auch schon unter den aktuellen Wortlaut als „sonstige Einrichtungen mit Aufgabe unabhängiger wissenschaftlicher Forschung“.

Sogar wortgleich bleiben die Zweckbestimmungen des § 303e Abs. 2 SGB V-E. Damit erfolgt hier nach dem aktuellen Stand des Entwurfs keine Konkretisierung, wie weit die Zweckbindung insbesondere in Bezug auf wissenschaftliche Vorhaben reichen soll, wodurch verbleibende Zweifel bestehen bleiben (s.o. B. II. 4. b. und III. 3.).

Eine erhebliche Konkretisierung und auch einige Änderungen wurden in § 303e Abs. 3 SGB V-E hinsichtlich des Antragsverfahrens einer nutzungsberechtigten Stelle vorgenommen. Neu ist, dass gemäß § 303e Abs. 3 S. 1 SGB V-E alle Voraussetzungen der Absätze 1 und 2 geprüft werden sollen, also auch, ob die Datenverarbeitung einer nutzungsberechtigten Stelle für deren Aufgabenerfüllung erforderlich ist. Dies war zuvor nicht vom ausdrücklichen Prüfprogramm nach § 303e Abs. 3 S. 1 SGB V umfasst. Zudem ist in § 303e Abs. 3 S. 2 SGB V-E nun ausdrücklich und für alle nutzungsberechtigten Stellen eine Plausibilitätsprüfung anstelle einer Erforderlichkeitsprüfung hinsichtlich des Datenumfangs vorgesehen, so dass einem Konflikt mit der Forschungsfreiheit sachgerecht vorgebeugt wird (dazu C. III. 1. e)).

Eine Erforderlichkeitsprüfung erfolgt nach § 303e Abs. 4 Nr. 1 SGB V-E weiterhin bei der Frage, ob der Zugang zu Einzelangaben gewährt wird. Hierbei ist nach § 303e Abs. 4 Nr. 2 SGB V-E durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Datennutzung auf das erforderliche Maß beschränkt bleibt und keine Kopien der Einzeldaten möglich sind. Hierzu zählt nach § 5 Abs. 5 S. 4 DaTraV-E die Möglichkeit eines Fernzugangs, soweit dies technisch umsetzbar ist. Aktuell ist hier nach § 5 Abs. 5 S. 3 DaTraV nur ein Zugang an einem Gastarbeitsplatz bei der Datenaufbereitungsstelle möglich.

§ 303e Abs. 5 SGB V-E statuiert zudem ein Verbot der Zweckentfremdung, der Datenweitergabe und vor allem der Reidentifikation durch Nutzungsberechtigte. Diese Regelungen finden sich bislang nicht in dieser Klarheit in den §§ 303a ff. SGB V (s.o. B. III. 1. c)). § 303c Abs. 2 S. 2 SGB V gebietet zwar auch jetzt schon, dass eine Reidentifikation nicht möglich sein soll, was sich jedoch primär an die Vertrauensstelle richtet und nach dem Wortlaut vor allem auf organisatorische Maßnahmen zur Verhinderung der Reidentifikation abzielt. Ein ausdrückliches Reidentifikationsverbot, das sich direkt an nutzungsberechtigte Stellen richtet, enthält bislang nur die Nutzungsordnung der Datenaufbereitungsstelle.²³⁵

Dieses Verbot soll in § 307c Abs. 1 SGB V-E flankiert werden mit einer Strafvorschrift für die vorsätzliche (vgl. § 15 StGB) Reidentifikation von Versicherten. § 307c Abs. 2 SGB V-E enthält eine Qualifikation für eine Reidentifikation gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht. Gemäß § 307c Abs. 3 SGB V-E handelt es sich hierbei um ein (absolutes) Antragsdelikt, wobei der Betroffene, das Forschungsdatenzentrum und die zuständige Datenschutzaufsichtsbehörde antragsberechtigt sein sollen.

Mit § 303e Abs. 6 SGB V-E soll eine Vorschrift zur Kommunikation des Forschungsdatenzentrums mit der Datenschutzaufsicht eingeführt werden. Soweit die Datenschutzaufsichtsbehörde Datenschutzrechtsverstöße der nutzungsberechtigten Stelle feststellt, ist die Möglichkeit der Sperrung dieser Stelle vorgesehen. Die Dauer der Sperre beträgt stets zwei Jahre.

Zudem fände sich die Entgeltregelung für die Arbeit des DIMDI künftig in § 303f SGB V-E. Hiernach wird das DIMDI selbst ermächtigt, einen Entgeltkatalog festzusetzen und nicht mehr wie bisher nach § 303e Abs. 2 S. 4 SGB V das BMG durch Rechtsverordnung.

²³⁵ Informationssystem Versorgungsdaten (Datentransparenz): Nutzungsordnung, Version 01-05-000, S. 3, abrufbar unter <https://www.dimdi.de/static/.downloads/deutsch/versorgungsdaten-nutzungsordnung.pdf>, abgerufen am 24.6.2019.

bb) Kabinettsentwurf

Hinzu kommt ein am 10.7.2019 vorgestellter Kabinettsentwurf,²³⁶ der ebenfalls die §§ 303a ff. SGB V betrifft und in einigen Punkten vom Referentenentwurf abweicht.²³⁷

Inhaltlich im Wesentlichen unverändert gegenüber dem Referentenentwurf bleibt dabei § 303a SGB V-KE. Insbesondere die Entscheidungen, den Spitzenverband Bund der Krankenkassen als Datensammelstelle einzusetzen und die Datenaufbereitungsstelle in Forschungsdatenzentrum umzubenennen, wurden beibehalten. Leicht spezifiziert wurde dagegen die Verordnungsermächtigung in § 303a Abs. 4 SGB V-KE.

Vor allem durch sprachlich-redaktionelle Präzisierungen sind die §§ 303b, 303c und 303d SGB V-KE leicht abgewandelt worden. So wurde beispielsweise in § 303b SGB V-KE das Übermittlungsverfahren von der Datensammelstelle an das Forschungsdatenzentrum und die Vertrauensstelle genauer dargestellt, ohne jedoch erkennbar inhaltliche Änderungen vorzunehmen.

Weiterentwicklungen gegenüber dem Referentenentwurf wurden dagegen bei § 303e SGB V-KE vorgenommen. § 303e Abs. 1 SGB V-KE gibt nun am Anfang ein klares Prüfprogramm für das Forschungsdatenzentrum vor. Die nutzungsberechtigten Stellen bleiben jedoch unverändert. Änderungen ergeben sich bei der Regelung zur Zweckbindung in § 303e Abs. 2 SGB V-KE. Hier wurde das „insbesondere“ aus der bisherigen Fassung gestrichen, so dass die Liste der zulässigen Zwecke hiernach als abschließend zu verstehen sein wird. Zudem wurde § 303e Abs. 2 Nr. 4 SGB V-KE um das Wort „Forschung“ ergänzt. Letzterem wird zwar wohl auch nur klarstellender Charakter zukommen. Doch angesichts der Zweifel, wie weit die Zweckbindung im Bereich der Forschung reicht (s.o. B. III. 3.), dürfte dies als Signal für ein weites Verständnis zugunsten der Nutzungsberechtigung verschiedener Forscher zu werten sein.

Beibehalten wurde die Beschränkung der Erforderlichkeitsprüfung auf eine Plausibilitätsprüfung in § 303e Abs. 3 SGB V-KE. Spezifiziert wurde die Art der Datenbereitstellung, nämlich einerseits „anonymisiert und aggregiert“ nach § 303e Abs. 3 SGB V-KE oder andererseits als „pseudonymisierte Einzeldatensätze [...] ohne Sichtbarmachung der Pseudonyme“ nach

²³⁶ Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation vom 10.7.2019, abrufbar unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/Digitale-Versorgung-Gesetz_DVG_Kabinett.pdf, abgerufen am 10.7.2019.

²³⁷ §§ des Kabinettsentwurfs werden gekennzeichnet mit SGB V-KE.

§ 303e Abs. 4 SGB V-KE. Während dies jedoch wohl vor allem nur eine sprachliche Präzisierung darstellen soll, werden in § 303e Abs. 4 SGB V-KE auch zusätzliche Voraussetzungen für die Bereitstellung von Einzeldatensätzen geschaffen. § 303e Abs. 4 S. 2 Nr. 1 SGB V-KE setzt voraus, dass die die Daten empfangende Person auf Seiten der nutzungsberechtigten Stellen einer Geheimhaltungspflicht nach § 203 StGB unterliegt. Ist dies nicht der Fall, so muss sich die empfangende Person nach § 303e Abs. 4 S. 3 SGB V-KE zusätzlich zur Geheimhaltung verpflichten. Dabei soll nach § 303e Abs. 4 S. 4 SGB V-KE das Verpflichtungsgesetz in Teilen entsprechend gelten. Zudem ist nun auch hier eine ausdrückliche Begrenzung der Erforderlichkeit auf eine Plausibilitätsprüfung vorgesehen.

Das strafbewährte Verbot der vorsätzlichen Identifikation von Versicherten nach § 303e Abs. 5 S. 4 SGB V-KE i.V.m. § 307b Abs. 1 SGB V-KE bleibt grundsätzlich erhalten. Neu wird in § 303e Abs. 5 S. 3 SGB V-KE vorgesehen, dass unbeabsichtigte Identifikationen dem Forschungsdatenzentrum zu melden sind.

b) Regelungsebene des Datenumfangs

Bei einer möglichen Neuregelung hinsichtlich des Datenumfangs der Datentransparenz i.S.d. §§ 303a ff. SGB V sollte vorsorglich eher von einem streng verstandenen Parlamentsvorbehalt ausgegangen werden. Denn es ist nicht mit letzter Sicherheit zu prognostizieren, inwieweit eine Verlagerung von Zulässigkeitsstatbeständen auf die Ebene einer Exekutivverordnung einer verfassungsrechtlichen Überprüfung standhielte (s.o. B. III. 6.).²³⁸ Zwar lässt sich gut vertreten, dass es hier bei der Frage des Datenumfangs ausreichend ist, wenn der Gesetzgeber diesen lediglich umreißt und sodann durch eine Verordnung konkretisieren lässt. Das Gebot der Normklarheit legt jedoch nahe, auf allzu komplizierte Verweisungen gänzlich zu verzichten.²³⁹ Es bietet sich an, in den §§ 303a ff. SGB V die zu erhebenden Daten möglichst genau zu definieren, um sodann im Rahmen einer Verordnungsermächtigung vor allem Einzelfragen der Erhebung der Daten zu regeln und bezüglich des Umfangs der Daten lediglich Konkretisierungen vorzunehmen. § 303b Abs. 1 SGB V-E verfolgt hier bereits einen relativ pragmatischen Ansatz, zumal dort eine Aufzählung der zu erhebenden Daten erfolgt. Hieraus wird sowohl für

²³⁸ Vgl. Kingreen/Kühling, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 12, abrufbar unter https://www.ber-telsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019.

²³⁹ Kingreen/Kühling, in: Kingreen/Kühling (Hrsg.), Gesundheitsdatenschutzrecht, 2015, S. 453.

nutzungsberechtigte Stellen als auch für potentielle Betroffene bzw. die Versicherten wesentlich leichter ersichtlich, welche Daten erhoben werden sollen. Dem Gebot der Normklarheit wird damit deutlich besser Rechnung getragen, als es nach bisheriger Rechtslage der Fall ist (s.o. B. III. 6.). Gleiches gilt für § 303b Abs. 1 S. 1 Nrn. 1 bis 5 SGB V-KE.

c) Integration von Institutionskennzeichen, Betriebsgeheimnis

Zu erwägen ist, die jeweiligen Institutionskennzeichen der Leistungserbringer mit in den Datensatz der Datentransparenz aufzunehmen. Die damit möglichen Rückschlüsse auf bestimmte Krankenhäuser oder Arztpraxen müssen in zweifacher Hinsicht überprüft werden. Zunächst kann bei dem Rückschluss auf einzelne Arztpraxen auch das Recht auf informationelle Selbstbestimmung des Arztes betroffen sein. Wesentlich relevanter dürfte aber die Frage sein, inwieweit Betriebs- und Geschäftsgeheimnisse von Leistungsträgern, z.B. von Krankenhäusern, betroffen sind. Auch die Betriebs- und Geschäftsgeheimnisse der Krankenkassen als Leistungsträger können umfasst sein. Diese unterfallen dem Schutz des Art. 12 Abs. 1 GG.²⁴⁰

Soweit im Datensatz der Versorgungsdaten Informationen zu Art und Umfang der Leistungserbringung und vor allem zu den berechneten Entgelten eines bestimmten Leistungserbringers vorkommen, ist der Schutzbereich der Berufsfreiheit eröffnet.²⁴¹ Bei Art. 12 Abs. 1 GG ist ein einfacher Gesetzesvorbehalt zu beachten. Wenn der Gesetzgeber also die Erfassung der Institutionskennzeichen für die Versorgungsforschung für erforderlich hält, kann in den §§ 303a ff. SGB V eine Rechtsgrundlage für einen möglichen Eingriff geschaffen werden. § 303b Abs. 1 S. 1 SGB V-E, der als Berufsausübungsregel zu verstehen ist, enthält eine solche Rechtsgrundlage. Dies wurde in § 303b Abs. 1 S. 1 Nr. 5 SGB V-KE übernommen. Dort müssten zur verfassungsrechtlichen Rechtfertigung des Eingriffs ausreichende Sicherungsmechanismen vorgesehen werden, die insbesondere verhindern, dass Wettbewerber auf die Betriebs- und Geschäftsgeheimnisse zugreifen können.²⁴²

²⁴⁰ Vgl. BVerfG, Beschl. v. 14.3.2006 – 1 BvR 2111/03, Rn. 84.

²⁴¹ Kingreen/Kühling, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 20, abrufbar unter https://www.ber-telsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019.

²⁴² Kingreen/Kühling, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, Rechtsgutachten, 2017, S. 4, 22, abrufbar unter https://www.ber-telsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku_hling.pdf, abgerufen am 24.6.2019.

Hier ist bislang lediglich eine Pseudonymisierung der Angaben zu den Leistungserbringern nach § 303b Abs. 2 S. 3 SGB V-E bzw. § 303b Abs. 3 S. 2 SGB V-KE vorgesehen. Ob diese ausreicht, hängt davon ab, inwieweit für eine nutzungsberechtigte Stelle Rückschlüsse darauf möglich sind, welches Pseudonym welchem Leistungserbringer zuzuschreiben ist. Soweit dies möglich scheint, gilt es einerseits zu vermeiden, dass Einzelangaben aus dem Datensatz, die Betriebs- und Geschäftsgeheimnisse darstellen (z.B. Angaben zu den verrechneten Entgelten), veröffentlicht werden. Da aber selbst in den Situationen, in denen eine nutzungsberechtigte Stelle auf Einzeldatensätze zugreifen kann, lediglich aggregierte Ergebnismengen die Datenaufbereitungsstelle verlassen, scheint hier kein großes Risiko gegeben zu sein, dass es zu Veröffentlichungen von Einzelangaben kommt.

Darüber hinaus muss sichergestellt werden, dass Konkurrenten der Leistungserbringer die Daten nicht zum Zweck der Aufdeckung von Betriebs- und Geschäftsgeheimnissen nutzen. Denkbare Szenario wäre ein nutzungsberechtigter Forscher, der zugleich Arzt bei einer konkurrierenden Klinik ist. Auch die Betriebs- und Geschäftsgeheimnisse der Leistungsträger müssen geschützt werden.

Der Gefahr des Missbrauchs der im Rahmen der Datentransparenz bereitgestellten Daten, die auch Betriebs- und Geschäftsgeheimnisse beinhalten können, zu begegnen, könnte mit einem an die nutzungsberechtigte Stelle gerichteten Verbot der Ausspähung von Geschäftsgeheimnissen konkurrierender Leistungserbringer begegnet werden, das mit einer wirksamen strafrechtlichen Sanktionsdrohung durchgesetzt werden könnte. Systematisch könnte § 303e SGB V für das Verbot einen geeigneten Regelungsort darstellen. Die Vorschrift könnte wie folgt formuliert werden:

„Die Verarbeitung der bereit gestellten Daten zum Zwecke der unbefugten Identifizierung von Leistungserbringern oder Leistungsträgern sowie zur bewussten Verschaffung von Kenntnissen über fremde Betriebs- und Geschäftsgeheimnisse ist untersagt.“

§ 307b SGB V böte sodann Raum für eine wie folgt lautende Strafandrohung:

„Wer die ihm im Rahmen der Datentransparenz zur Verfügung gestellten Daten nutzt, um sich oder einem Dritten bewusst Kenntnis von fremden Betriebs- und Geschäftsgeheimnissen zu verschaffen oder ein solches Geheimnis zu nutzen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unbefugt bestimmte Leistungserbringer oder Leistungsträger identifiziert.“

Die Tatbestandsmerkmale „bewusst“ und „unbefugt“ sollen berechnigte Forschungsinteressen ausnehmen.

In der DaTraV könnte sodann ergänzend folgende Regelung vorgesehen werden:

„Rechtfertigen Tatsachen die Annahme, dass der Antragsteller gegen dieses Verbot verstößt, so kann der Antrag abgelehnt oder nur eingeschränkt bewilligt werden.“

Die Datenaufbereitungsstelle wird so in die Lage versetzt, geeignete Maßnahmen zu ergreifen, um unzuverlässige Antragsteller auszuschließen. Die Einräumung eines weiten Ermessensspielraums der Behörde sorgt für die erforderliche Flexibilität in der Handhabung und einen unbürokratischen Antragsprozess. Insbesondere sollte vermieden werden, die Behörde durch einen vorgeschriebenen Prüfprozess, der über eine bloße Evidenzkontrolle hinausgeht, zu überfordern.

d) Fragen der Zweckbindung und Öffnung für die Forschung

Der in Art. 5 Abs. 1 lit. b DS-GVO normierte Zweckbindungsgrundsatz ist einer der Kernbestandteile des europäischen Datenschutzrechts.²⁴³ In § 303e Abs. 2 SGB V definiert der deutsche Gesetzgeber die Zwecke, zu denen eine Verarbeitung der Versorgungsdaten durch nutzungsberechtigte Stellen möglich ist. Wie die Ausführungen zur derzeitigen Rechtslage zeigen, können dabei bereits nach aktueller Rechtslage wissenschaftliche Vorhaben in erheblichem Maße durchgeführt werden (s.o. B. III. 3.). In der Praxis werden dagegen nur wenige Anträge gestellt werden. Umso mehr hat der Gesetzgeber die Möglichkeit, die Zweckbestimmungen des § 303e Abs. 2 SGB V zu präzisieren und dadurch einerseits verbleibende Zweifel auszuräumen und andererseits ein Signal für die Öffnung der Versorgungsdaten für die Wissenschaft zu senden.

Das betrifft zunächst die allgemeine Frage, ob der Katalog des § 303e Abs. 2 SGB V abschließend ist oder nicht (s.o. B. II. 4. b)). Hier sollte eine Klarstellung erfolgen. Der Referentenentwurf behält in § 303e Abs. 2 SGB V-E das „insbesondere“ bei und ersetzt dafür die Formulierung „dem Katalog des Absatz 2 entspricht“ in § 303e Abs. 3 S. 1 SGB V durch „prüft das Vorliegen der Voraussetzungen nach Absatz 1 und 2“ (§ 303e Abs. 3 S. 1 SGB V-E). Dies würde eine begrüßenswerte Klarstellung zugunsten eines nicht abschließenden Kataloges bedeuten. Ebenso denkbar wäre aber auch eine Klarstellung in die entgegengesetzte Stoßrichtung,

²⁴³ Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 20.

indem das „insbesondere“ ganz weggelassen wird. Diesen Ansatz verfolgt § 303e Abs. 2 SGB V-KE.

Klarstellungsbedarf besteht auch hinsichtlich der Frage, welche wissenschaftlichen Vorhaben von der Zweckbestimmung umfasst sind. Nach dem der vorliegenden Bearbeitung zugrunde liegenden Verständnis gibt es bereits de lege lata keinen Grund, bestimmte Vorhaben – wie beispielsweise im Zuge einer Promotion oder Habilitation – auszuschließen (s.o. B. III. 3.).

Da die Praxis der Datenaufbereitungsstelle jedoch gerade solchen Vorhaben den Zugriff verweigert, sollte der Gesetzgeber hier seinen Willen klar zum Ausdruck bringen. Die bloße Aufnahme der Förderung der wissenschaftlichen Erschließung der Daten als Aufgabe der Datenaufbereitungsstelle in § 303d Abs. 3 Nr. 10 SGB V-E ist zwar begrüßenswert, genügt aber nicht. Eine Ergänzung des § 303e Abs. 2 SGB V könnte die obige Rechtsfrage abschließend klären. So ist folgende Formulierung des § 303e Abs. 2 Nr. 4 SGB möglich:

„4. Längsschnittanalysen über längere Zeiträume, Analysen von Behandlungsabläufen, Analysen des Versorgungsgeschehens zum Erkennen von Fehlentwicklungen und von Ansatzpunkten für Reformen (Über-, Unter- und Fehlversorgung), insbesondere im Rahmen unabhängiger wissenschaftlicher Forschung; hierzu zählen auch Vorhaben, die im Rahmen der Erstellung wissenschaftlicher Qualifikationsschriften wie der Promotion oder Habilitation erfolgen,“

Die in § 303e Abs. 2 Nr. 5 SGB V-KE erfolgte Klarstellung mit dem Wortlaut „Forschung, insbesondere für Längsschnittanalysen über längere Zeiträume, Analysen von Behandlungsabläufen oder Analysen des Versorgungsgeschehens“ geht bereits in die beschriebene Richtung. Allein aus der Auslegung dieser Norm mit Blick auf die besondere Betonung der Forschung sollte klar werden, dass sämtliche Forschungsvorhaben umfasst sind, insbesondere auch im Zuge einer Promotion oder Habilitation. Damit dies aber auch von der Datenaufbereitungsstelle bzw. dem Forschungsdatenzentrum so umgesetzt wird, ist zumindest auf der Ebene der DaTraV eine weitere Klarstellung möglich. Alternativ könnte das BMG auch von aufsichtsrechtlichen Maßnahmen gegenüber der Datenaufbereitungsstelle Gebrauch machen. Eine Klarstellung in der DaTraV könnte in § 5 Abs. 3 Nr. 2 verankert werden und wie folgt lauten:

„2. der angegebene Zweck der Datenverarbeitung und Datennutzung (Nutzungszweck) dem Katalog nach § 303e Absatz 2 des Fünften Buches Sozialgesetzbuch entspricht, worunter insbesondere auch Forschungsvorhaben fallen, die im Rahmen der Erstellung

wissenschaftlicher Qualifikationsschriften wie der Promotion oder Habilitation erfolgen,“

e) **Erforderlichkeitsprüfung**

Der Grundsatz der Erforderlichkeit war bereits im Hessischen Datenschutzgesetz von 1970²⁴⁴ als erste datenschutzrechtliche Kodifikation verankert und stellt damit einen seit Jahrzehnten gewachsenen Grundsatz dar. Vor Inkrafttreten der DS-GVO war er Bestandteil des deutschen Datenschutzrechts nach § 3a BDSG a.F. Als Ausprägung des Grundsatzes der Datenminimierung findet er sich nun auch in Art. 5 Abs. 1 lit. c DS-GVO wieder. Soweit ein Verarbeitungsvorgang im Rahmen der §§ 303a ff. SGB V personenbezogene Daten betrifft, ist dieser Grundsatz demnach auch von dem deutschen Gesetzgeber zu beachten, zumal eine Erforderlichkeitsprüfung auch ein sinnvolles Instrument zur Abwehr eines stets bestehenden Missbrauchspotentials darstellt. Die Begriffe „Datensparsamkeit“ bzw. „Erforderlichkeit“ sind vor allem aber als der eigentlich selbstverständliche Grundsatz zu verstehen, dass ein Grundrechtseingriff auf das notwendige Maß beschränkt bleiben muss (dazu unten auch C. IV. 1.).

Anders als noch unter dem BDSG a.F. orientiert sich im aktuellen europäischen Rechtsrahmen der Erforderlichkeitsgrundsatz stärker an der Zweckbindung.²⁴⁵ Es geht daher vorliegend um die Frage, in welchem Maße eine Datenverarbeitung zur Erreichung des in § 303e Abs. 2 SGB V definierten Zwecks erforderlich ist. Bei der hier anzustellenden Güterabwägung sind die Wissenschaftsfreiheit und das Allgemeininteresse an einer effektiven Versorgung mit einzubeziehen.

Die Erforderlichkeitsprüfung hinsichtlich des Datenumfanges in § 303e Abs. 3 S. 1 SGB V ist bereits de lege lata wegen der Freiheit der Wissenschaft inhaltlich auf eine Plausibilitätsprüfung zu beschränken, zumindest soweit die nutzungsberechtigte Stelle Träger dieses Grundrechts ist (s.o. B. III. 2.). De lege ferenda ist insoweit eine Klarstellung sinnvoll. Die Formulierung in § 303e Abs. 3 S. 2 SGB V-E, es sei „nachvollziehbar darzulegen, dass Umfang und Struktur der beantragten Daten erforderlich“ sind, verfolgt dabei den richtigen Ansatz. Hier wird deutlich, dass die nutzungsberechtigte Stelle zwar darlegen muss, warum sie den gewähl-

²⁴⁴ Abrufbar unter <http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1>, dort § 3 Abs. 2; siehe auch Leeb/Liebhaber, JuS 2018, 534, 534 f.

²⁴⁵ Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rn. 55 ff.

ten Datenumfang für die Zweckerreichung für erforderlich hält. Aus der Formulierung „nachvollziehbar darlegen“ ergibt sich, dass die Datenaufbereitungsstelle (bzw. künftig gegebenenfalls das Forschungsdatenzentrum) hier nur den Datenzugang verweigern kann, wenn die angeforderten Daten zur Zweckerreichung offensichtlich ungeeignet sind oder viel zu weit greifen. Der Kabinettsentwurf behält mit § 303e Abs. 3 und 4 SGB V-KE dieselbe sinnvolle Richtung bei. Inhaltlich zwingend ist dies zwar nur für Grundrechtsträger der Wissenschaftsfreiheit wie Hochschulen i.S.v. § 303e Abs. 1 Nr. 8 SGB V. Regelungstechnisch ist es jedoch zur Vermeidung einer unnötigen Komplexität in der Verfahrenspraxis zweckmäßig, die Plausibilitätsprüfung auch für andere berechnigte Stellen (z.B. Krankenkassen nach § 303e Abs. 1 Nr. 3 SGB V) einzuführen, wie im Referentenentwurf vorgesehen.

f) Risikoabwägung und prozedurale Ausdifferenzierung

Zur Diskussion steht eine prozedurale Ausdifferenzierung des Antragsverfahrens nach § 303e SGB V, die nach der Art der nutzungsberechnigten Stelle unterschiedlich leicht und weitreichend Einsicht in den Datensatz der Versorgungsdaten gewährt. Denkbar wäre es etwa, einen „Circle of Trust“ festzulegen, bei dem drei Stufen bestehen.

Ausgestalten könnte man einen solchen beispielsweise, indem man eine erste Stufe von besonders vertrauenswürdigen Nutzungsberechnigten festlegt. Kriterium hierfür könnte sein, dass diese Berechnigten öffentliche Stellen sein müssen, die dem Sozialgeheimnis unterliegen und ausreichende technische Schutzvorrichtungen vorweisen können. Für diese Stellen auf der ersten Stufe würde dann das Verfahren deutlich verkürzt, die Risikoabwägung seitens der Datenaufbereitungsstelle nach § 303c Abs. 2 S. 2 SGB V i.V.m. § 5 Abs. 3 Nr. 5 DaTraV zugunsten der Annahme eines niedrigen Risikos weitgehend vorweggenommen. Die Stellen könnten Zugriff sowohl auf Ergebnismengen als auch auf Einzeldatensätze nehmen (siehe hierzu oben B. III. 1. b)).

Auf der zweiten Stufe würden nach diesem Modell Stellen stehen, die zwar nicht dem Sozialgeheimnis unterliegen, die aber ein ausreichendes Datenschutzkonzept vorweisen können und möglicherweise eine Selbstverpflichtung zur Achtung hoher Datenschutzstandards eingegangen sind. Hierzu könnten etwa Wissenschaftler von Hochschulen und sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung i.S.v. § 303e Abs. 1 Nr. 8 SGB V zählen, soweit sie die genannten Bedingungen erfüllen. Auf dieser zweiten Stufe könnte dann das Verfahren wie bisher (siehe hierzu oben B. III. 4.) verlaufen. Es könnte also ebenfalls neben Ergebnismengen die Arbeit mit Einzeldatensätzen ermöglicht werden, soweit dies erforderlich

ist. Jedoch müsste bei der Bereitstellung der Ergebnisse am Ende stets eine ausführliche Abwägung des Reidentifikationsrisikos seitens der Datenaufbereitungsstelle (wie bei § 303c Abs. 2 S. 2 SGB V i.V.m. § 5 Abs. 3 Nr. 5 DaTraV bereits jetzt vorgegeben) vorgenommen werden.

Auf Stufe drei würden dann Stellen stehen, die nicht dem Sozialgeheimnis unterliegen und die die Voraussetzungen der zweiten Stufe nicht erfüllen. Hier wäre dann lediglich der Zugang zu tatsächlich anonymen Ergebnismengen möglich.

Positiv zu bewerten ist an derartigen Überlegungen, dass sie zu einer Vereinfachung und Beschleunigung des Verfahrens führen könnten. Aus datenschutzrechtlicher Sicht scheinen sie nicht zwingend notwendig. Eine gesetzliche Festlegung von Kriterien zur besseren Handhabung der Risikoabwägung durch die Datenaufbereitungsstelle ist jedoch durchaus zweckmäßig.

Bislang ist weder in der aktuellen Gesetzgebung (s.o. B. III. 4.) noch im Referentenentwurf eine solche Differenzierung angelegt. Soweit vom Gesetzgeber gewünscht, könnte eine solche Regelung normsystematisch sinnvoll an § 303e SGB V gekoppelt werden. In der aktuellen Struktur wäre dazu eine Neufassung des § 303e Abs. 3 SGB V, in der Systematik des Referentenentwurfs in einem neuen Absatz zwischen § 303e Abs. 3 und 4 SGB V-E notwendig.

Im Kabinettsentwurf ist in § 303e Abs. 4 S. 3 und 4 SGB V-KE eine zweistufige Differenzierung im Sinne der vorstehenden Überlegungen integriert. Geheimhaltungspflichtige Personen auf Seiten der nutzungsberechtigten Stellen bekommen ohne weitere Voraussetzungen Zugriff. Alle weiteren Personen müssen noch zur Geheimhaltung verpflichtet werden. Sollte eine weitergehende Ausdifferenzierung gewünscht sein, so könnte dies auch auf der Verordnungsebene in der DaTraV vorgenommen werden. § 303a Abs. 4 Nr. 4 SGB V-KE sieht hier bereits eine ausreichende Verordnungsermächtigung vor.

g) Zur Verwendung der Begriffe „anonymisiert“ und „pseudonymisiert“

Es wurde bereits dargestellt, wie der Begriff anonymer Daten i.S.d. DS-GVO zu verstehen ist (siehe hierzu oben B. I. 2. b) aa)). Wichtig ist hierbei, dass Anonymität nach der DS-GVO nicht gleichzusetzen ist mit absoluter Anonymität, also der absoluten Unmöglichkeit der Reidentifikation für jeden erdenklichen Verarbeiter. Eine Einschränkung wird einerseits durch das Wahrscheinlichkeitskriterium vorgenommen. Es darf demnach ein geringes Restrisiko der Reidentifikation verbleiben und die Daten können dennoch als anonym qualifiziert werden. Auch der

EuGH²⁴⁶ hat deutlich gemacht, dass der Unterscheidung von personenbezogenen und anonymen Daten kein absoluter Personenbezugsbegriff zugrunde liegt. Es kommt also stets auf die Möglichkeit zur Reidentifizierung des jeweiligen Verantwortlichen an. Wissen und Mittel Dritter sind nur mit einzubeziehen, wenn rechtliche Mittel bestehen, um das Wissen zu erlangen.²⁴⁷ Ob Daten aggregiert sind oder nicht, hat dabei unter Zugrundelegung des aufgezeigten Verständnisses nach der DS-GVO zunächst keine direkte Auswirkung auf die Frage, ob diese anonym oder personenbezogen sind. Aggregierte Daten als Aussagen über Personengruppen weisen in der Regel keinen Personenbezug auf.²⁴⁸ Etwas anderes kann auch hier nur gelten, wenn die Aussage über eine Gruppe auf einzelne Personen „durchschlägt“.²⁴⁹ Soweit keine personenbezogenen Daten vorliegen, greift aber bei aggregierten Daten auch nicht die oben beschriebene Vorfeldwirkung (s.o. C. I. 2.) aus dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Denn auch diese Rechtsprechung des BVerfG knüpft an den Personenbezug an.²⁵⁰

Der Begriff der pseudonymisierten Daten ist ein Unterfall personenbezogener Daten. Die Pseudonymisierung von Daten stellt lediglich eine Sicherungsmaßnahme dar, bei der eine Identifizierung der Daten nicht mehr unmittelbar, sondern nur noch über eine Zuordnungsregel möglich ist.²⁵¹

Gerade auch für gesetzgeberische Erwägungen auf mitgliedstaatlicher Ebene stellt sich die Frage, ob auch solche Verfahren nach der DS-GVO rein begrifflich eine Pseudonymisierung darstellen, die nicht rückführbare Pseudonyme generieren, die allein der Datenzusammenführung dienen und auch mit Zusatzwissen nicht zur Herstellung des Personenbezugs genutzt werden können (sog. Hash-Verfahren).

Art. 4 Nr. 5 DS-GVO definiert die Pseudonymisierung als „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

²⁴⁶ EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779 – Breyer = ZD 2016, 24 m. Anm. Kühling/Klar.

²⁴⁷ Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 253 ff.

²⁴⁸ Gola, in: Gola (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 4 Rn. 8 f.

²⁴⁹ Klar/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 Rn. 15; Gola, in: Gola (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 4 Rn. 8.

²⁵⁰ BVerfG, Beschl. v. 13.6.2007, 1 BvR 1550/03 u.a. = BVerfGE 118, 168 = DStRE 2007, 1196, 1200 f.

²⁵¹ Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 266 f.

organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (siehe hierzu bereits B. I. 2. b) bb)).

Die Daten müssen also weiterhin einer Person zuordenbar sein, allerdings explizit unter Hinzuziehung von gesondert aufbewahrten und technisch-organisatorischen Maßnahmen unterliegenden Zusatzinformationen. Nimmt man den Wortlaut des Art. 4 Nr. 5 DS-GVO ernst, so muss zumindest irgendjemandem die Identifizierung der betroffenen Person gerade durch Verwendung dieser Zusatzinformationen – also beispielsweise durch eine Zuordnungsregel oder durch eine Liste der Pseudonyme – möglich sein. Steht also tatsächlich ein Verfahren in Rede, das es vollkommen unmöglich macht, die „Pseudonymisierung“ umzukehren und wieder eine Zuordnung zu erzielen, so passt der Begriff der Pseudonymisierung nach Art. 4 Nr. 5 DS-GVO vom Wortlaut her nicht. Denn eine derartige Hash-Funktion ist gerade dazu konzipiert, zwar eine Zuordnung des Klarnamens bzw. des Eingabewerts zum Hash-Wert bzw. zum „Pseudonym“ zu ermöglichen. Eine umgekehrte Zuordnung vom Hash-Wert zur natürlichen Person soll dagegen nicht möglich sein. Es soll sich um ein Einwegverfahren handeln.

Dabei kann jedoch kein Algorithmus absolute Sicherheit garantieren, gerade auch mit Blick auf kommende Entwicklungen. So sind die früher gängigen und als sicher angesehenen Hash-Verfahren MD5 und SHA-1 inzwischen bei gesteigerter Rechnerleistung rückrechenbar.²⁵² Hier kann also gerade wieder ein Bezug vom Hash-Wert zur Person hergestellt werden. Bei lebensnaher Betrachtung ist es demnach nicht auszuschließen, dass alle Hash-Verfahren mit ausreichend Rechnerleistung zu irgendeinem zukünftigen Zeitpunkt entschlüsselbar sein werden. Nimmt man den Telos des Art. 4 Nr. 5 DS-GVO hinzu, der in Art. 32 Abs. 1 lit. a DS-GVO und in Erwägungsgrund 28 S. 1 der DS-GVO zum Ausdruck kommt, dass es sich bei der Pseudonymisierung vor allem um einen Sicherheitsmechanismus handeln soll, so ist es dennoch vertretbar, ein Hash-Verfahren als Pseudonymisierung zu bezeichnen. Denn ein Hash-Verfahren ist eine Sicherungsmaßnahme, die bei einem funktionierenden Verfahren sogar noch größeren Schutz für Betroffene gewährleistet als bei einer herkömmlichen Pseudonymisierung. Insgesamt verbleiben jedoch Zweifel, ob Hash-Verfahren unter den Wortlaut des Art. 4 Nr. 5 DS-GVO fallen. Wenn der Gesetzgeber ein solches Verfahren anordnen will, ohne dabei Gefahr zu laufen, mit der DS-GVO in begrifflichem Widerspruch zu stehen, können al-

²⁵² Siehe exemplarisch *Projekt 29*, Meldung vom 6.9.2017, abrufbar unter <https://www.projekt29.de/sha-1-und-md5-hashing-veraltet-und-unsicher/>, zuletzt abgerufen am 19.7.2019.

ternativ andere Formulierungen gewählt werden. Beispielsweise könnte der Begriff der „Verschlüsselung“ aufgegriffen werden, der nach Art. 32 Abs. 1 lit. a DS-GVO ebenfalls eine Sicherungsmaßnahme darstellt. Der Begriff wird dabei jedoch nicht von der DS-GVO definiert und weist gewisse Überschneidungen zur Pseudonymisierung auf.²⁵³

Eine präzise Formulierung ist wie folgt möglich: „die Daten sind derart zu verschlüsseln, dass ein Rückschluss auf die Identität durch eine direkte Umkehrung des Verschlüsselungsprozesses nach dem jeweiligen Stand der Technik ausgeschlossen ist“.

Die im Kabinetentwurf in § 303c Abs. 2 SGB V-KE verwendete Formulierung des „schlüsselabhängige[n] Verfahren[s] zur Pseudonymisierung“, bei dem „aus dem Pseudonym aber nicht auf das Versichertenkennzeichen oder die Identität des Versicherten geschlossen werden kann“ bringt ebenfalls klar zum Ausdruck, worum es gehen soll. Bei einer engen Lesart des Wortlauts des Art. 4 Nr. 5 DS-GVO ergibt sich allerdings ein gewisser Widerspruch, da dort gerade Voraussetzung ist, dass auf die Identität des Betroffenen geschlossen werden kann.

Ob bei einem nach aktuellem Stand der Technik sicherer gestalteten Hash-Verfahren nicht bereits eine Anonymisierung vorliegt, ist eine andere Frage und richtet sich nach den allgemeinen Kriterien (siehe hierzu B. I. 2. und B. III. 1.).²⁵⁴ Dabei geht es jeweils um die Möglichkeit des konkreten Datenverarbeiters, die betroffene Person zu identifizieren – egal ob durch eine Zuordnungsregel oder eine andere Art der Reidentifikation (siehe hierzu B. III. 1. a)). Pseudonymisierung und Anonymisierung schließen sich demnach keineswegs aus, denn es kommt auf die Sichtweise des jeweiligen Datenverarbeiters an. Für denjenigen, der in Besitz des Schlüssels bzw. der Zusatzinformation ist, stellen pseudonymisierte Daten stets personenbezogene Daten dar. Zeitgleich können eben jene Daten für einen Dritten als anonym angesehen werden, soweit für diesen keine Möglichkeit zur Identifizierung besteht, weder durch eine Zuordnung von Pseudonymen, noch durch Hinzuziehung sonstiger Informationen.²⁵⁵

Vom Bayerischen Verwaltungsgerichtshof wurde – zwar noch zur alten Rechtslage vor der DS-GVO – zumindest das in diesem Verfahren konkret in Rede stehende Hash-Verfahren SHA-

²⁵³ Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 269.

²⁵⁴ Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 270.

²⁵⁵ So im Fall EuGH, Urt. v. 19.10.2016, C-582/14, ECLI:EU:C:2016:779 – Breyer = ZD 2016, 24 m. Anm. Kühling/Klar.

256 als nicht ausreichend zur Herstellung von Anonymität bewertet.²⁵⁶ Dort hatte sich das Bayerische Landesamt für Datenschutzaufsicht mit dieser Ansicht durchgesetzt.²⁵⁷ Von Anonymität wird bei „gehashten“ personenbezogenen Daten unter Berücksichtigung dieser Aufsichtspraxis und ersten Rechtsprechungstendenz also nur im Ausnahmefall auszugehen sein.

Auch in den §§ 303a ff. SGB V und in der DaTraV kommen die Begriffe „anonymisiert“ (§ 303e Abs. 3 S. 2 SGB V und § 5 Abs. 4, 5 DaTraV) und „pseudonymisiert“ (z.B. § 303e Abs. 3 S. 3 SGB V und § 5 Abs. 5 DaTraV) vor. Soweit hingegen die zuständige Datenaufbereitungsstelle unter „anonymisiert“ eine absolute Anonymisierung versteht, wäre dies unter Berücksichtigung ihrer Aufgabe der Verhinderung einer Reidentifikation nach § 303c Abs. 2 S. 2 SGB V durchaus verständlich.

Bei einer Neuregelung könnte der Gesetzgeber vor diesem Hintergrund klarstellen, was unter „anonymisiert“ zu verstehen ist. Sinnvoll wäre dabei eine Verweisung auf den Anonymitätsbegriff der DS-GVO, um insoweit kein abweichendes Regelungsregime zu schaffen. Zweckmäßig wäre daher eine Formulierung wie „derart anonymisierte Angaben im Sinne des Erwägungsgrunds 26 der Datenschutzgrundverordnung 2016/679“. Gegebenenfalls wäre eine Präzisierung denkbar, die unmittelbar Bezug nimmt auf S. 5 des Erwägungsgrunds. Diese könnte wie folgt formuliert werden: „derart anonymisierte Angaben, d.h. personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann im Sinne des Erwägungsgrunds 26 der Datenschutzgrundverordnung 2016/679“. Eine absolute Anonymität zu fordern, könnte zwar mit einer Formulierung wie „derart anonymisierte Angaben, dass eine Identifizierung von Versicherten für jedermann unmöglich ist“, verfolgt werden.²⁵⁸ Damit würde der deutsche Gesetzgeber jedoch Regelungen außerhalb des Anwendungsbereichs der DS-GVO parallel zu dieser treffen, was zumindest rechtspolitisch sehr fraglich ist.

²⁵⁶ BayVGH, Beschl. v. 26.9.2018 – 5 CS 18.1157 = NVwZ 2019, 171; siehe auch zur Entscheidung in der Vorinstanz VG Bayreuth, Beschluss vom 08.05.2018 - B 1 S 18.105 = K&R 2018, 524 m. Anm. *Nacimiento/Küll* = ZD 2018, 382 m. Anm. *Felber*.

²⁵⁷ BayLDA, 8. Tätigkeitsbericht 2017/2018, S. 58 ff., abrufbar unter https://www.lda.bayern.de/media/baylda_report_08.pdf, zuletzt abgerufen am 18.7.2019.

²⁵⁸ Problematisch wäre vor diesem Hintergrund dann § 5 Abs. 5 DaTraV-E, der von „anonymisierten Einzelangaben“ spricht. Die Arbeit mit Einzeldatensätzen findet immer am gesamten Datensatz statt, zumindest solange keine repräsentativen Stichproben möglich sind. Die Herstellung absoluter Anonymität hierbei scheint schwierig.

h) Verbot der Reidentifikation und Sanktionen

Verbesserungspotenzial besteht ferner hinsichtlich der Handhabung des Reidentifikationsverbots. Dieses sollte nicht nur als Aufgabe der Datenaufbereitungsstelle in § 303c Abs. 2 S. 2 SGB V definiert werden, sondern auch ausdrücklich an die nutzungsberechtigten Stellen gerichtet sein. Die bloße Formulierung eines Reidentifikationsverbots in der Nutzungsordnung der Datenaufbereitungsstelle scheint unzulänglich (siehe hierzu oben B. III. 1. c)).

§ 303e Abs. 5 S. 2 SGB V-E enthält bereits ein solches Verbot, das in dieser oder vergleichbarer Form übernommen werden sollte. Im Entwurf sind als weitere Sicherungsmaßnahmen eine Sperre nutzungsberechtigter Stellen für zwei Jahre (§ 303e Abs. 6 S. 2 SGB V-E) und ein Straftatbestand (§ 307c SGB V-E) vorgesehen (s.o. C. III. 1. a)). In Bezug auf § 303e Abs. 6 S. 2 SGB V-E sollte möglicherweise abgewogen werden, ob eine Sperrung von stets zwei Jahren nicht zu unflexibel ist. Es könnte ein gestufter Sperrzeitraum nach Schwere des Verstoßes festgelegt werden. Der Kabinettsentwurf übernimmt die Systematik der Sanktionen fast deckungsgleich, wobei hier nun ein flexiblerer Sperrzeitraum von „bis zu zwei Jahren“ vorgesehen ist.

Im Übrigen ist diese Art des sanktionsbewährten Reidentifikationsverbots eine sehr sinnvolle Möglichkeit, um die Verarbeitung der Versorgungsdaten datenschutzrechtskonform auszugestalten. Entscheidend ist dabei, dass der durch die Sanktionsdrohungen abgesicherte hohe Sicherheitsstandard mit in die Risikoabwägung einbezogen werden kann. So könnten Daten mit einer sehr geringen Reidentifikationswahrscheinlichkeit eher bereitgestellt werden, zumal die Verantwortlichen ohnehin zumeist kein Interesse an einer Reidentifikation haben dürften und sich – soweit dies umgesetzt wird – künftig zusätzlich einer Strafandrohung ausgesetzt sehen. In der praktischen Umsetzung ist hierzu wichtig, dass die Zugriffe auf die Versorgungsdaten hinreichend protokolliert werden, um ex post Verstöße feststellen und sanktionieren zu können. Zur Absicherung könnte insoweit auch eine Regelung zur Protokollierung der Datenzugriffe in die §§ 303a ff. SGB V oder in die DaTraV selbst aufgenommen werden, anstatt dies der praktischen Umsetzung des Regelwerks zu überlassen.

i) Verknüpfung mit weiteren Sozialdaten oder Behandlungsdaten

Zudem stellt sich die Frage, inwieweit der Datensatz der Versorgungsdaten i.S.d. §§ 303a ff. SGB V datenschutzrechtskonform um andere Sozialdaten als die der Krankenkassen oder sonstige Daten aus dem Gesundheitssektor erweitert werden könnte. Denkbar ist zunächst, die Sozialdaten der Renten- und Unfallversicherungen mit einzubeziehen. Ein zweiter Ansatzpunkt

wären die „Behandlungsdaten“ der Patienten, die beispielsweise auf der elektronischen Patientenakte gespeichert sind.

Der Gedanke der Integration weiterer Sozialdaten ist dabei durchaus sinnvoll, zumindest soweit sie für die Versorgungs- und Gesundheitsforschung relevante Informationen umfassen. Da es sich bei den Daten der Renten- und Sozialversicherung ebenfalls um Sozialdaten handelt (s.o. A. III. 1. b)), dürften sich hier aus datenschutzrechtlicher Perspektive kaum wesentliche Unterschiede zum Datentransparenzsystem der gesetzlichen Krankenkassen in den §§ 303a ff. SGB V ergeben. Soweit der Gesetzgeber auf die Erweiterung des Umfangs der Versorgungsdaten abzielt, wären prima facie in dem für die §§ 303a ff. SGB V als zulässig erarbeiteten Rahmen vergleichbare Regelungen auch im SGB VI und VII denkbar. Regelungstechnisch wäre es zweckmäßig, hierfür bei § 274 SGB VI (z.B. in einen neuen § 274a SGB VI) und in den §§ 199 ff. SGB VII (z.B. in einem neuen § 206a SGB VII) Zulässigkeitstatbestände zu schaffen, die klarstellen, welche Daten erhoben werden sollen und bezüglich des Verfahrens umfassend auf die §§ 303a ff. SGB V und auch die dortigen Verfahrensweisen zur Gewährleistung des Datenschutzes zu verweisen. Dort müsste jeweils auch eine Verordnungsermächtigung verankert werden, so dass die Regelungen der DaTraV auch für die Daten der Renten- und Unfallversicherung gelten. In die gesetzgeberische Abwägung – vor dem Hintergrund der grundrechtlichen Anforderungen – mit einzubeziehen ist dabei, dass mit einem steigenden Datenvolumen auch das Reidentifikations- und Missbrauchsrisiko an Gewicht gewinnt. Es müsste also größter Wert auf einen hohen Datenschutzstandard gelegt werden. Umso sinnvoller scheinen Regelungen wie Strafvorschriften und vor allem Reidentifikationsverbote (s.o. C. III. 1. h)). Inwieweit technische Maßnahmen, wie beispielsweise die Pseudonymisierungsverfahren (insbesondere die Zuordnung zu periodenübergreifenden Pseudonymen), bei mehreren Datenquellen gleich sicher gestaltet werden können, ist ebenfalls in die Überlegungen einzubeziehen. Was die Behandlungsdaten angeht, so stellt sich die Situation anders dar. Mit den Behandlungsdaten sind diejenigen Daten gemeint, die bei der Untersuchung eines Patienten entstehen und möglicherweise künftig in dessen elektronischer Patientenakte gespeichert werden. Diese Daten reichen weiter als die bloße Diagnose, die an den Leistungsträger zur Abrechnung übermittelt wird und somit ohnehin schon zur Verfügung steht. Auch Untersuchungswerte, Arztbriefe oder Testergebnisse können je nach Ausgestaltung umfasst sein. Dabei entspringen die Daten unmittelbar aus dem Verhältnis des Leistungserbringers zum Versicherten und werden nicht im Rahmen der Leistungsabrechnung nach den §§ 295 f. SGB V an die Leistungsträger übermittelt. Eine Erhebung der Daten über die Leistungsträger ist mithin ausgeschlossen. Die

Leistungserbringer dagegen unterliegen der ärztlichen Schweigepflicht. Zweckmäßig schiene demnach nur eine Übermittlung der Behandlungsdaten durch die Versicherten selbst, also mithilfe einer Einwilligung oder eines Zulässigkeitsstatbestands in Verbindung mit einer Zustimmung. Hier kann auf die Ausführungen zur Datenspende verwiesen werden (dazu unter C. IV. 3.).

j) Zwischenfazit

Eine weitere Öffnung der Versorgungsdaten für die Wissenschaft, auch in der Praxis der Datenaufbereitungsstelle, ist positiv zu bewerten und durch die überwölbenden Vorgaben der Datenschutzordnung in grundrechtlicher Hinsicht und vor dem Hintergrund der DS-GVO nicht ausgeschlossen. Datenschutzrechtlich bieten die §§ 303a ff. SGB V hierzu weitestgehend bereits einen passenden Rahmen. Defizitär scheinen derzeit eher die Vollständigkeit des Datensatzes und die Kapazitäten des DIMDI zur tatsächlichen Bearbeitung von Forschungsvorhaben, vor allem falls eine Gesetzesänderung tatsächlich zu einer Zunahme der Anträge führen sollte. Zudem bestehen stellenweise Unsicherheiten hinsichtlich der Anonymität, die regelmäßig zu einer im Zweifel zu strengen Anwendung der §§ 303a ff. SGB V zulasten der Datenverarbeitung führen. Hier kann eine Konkretisierung durch den Gesetzgeber hin zu einem erleichterten Zugriff für die Wissenschaft auf den Datensatz einen Rahmen für das Abwägungsergebnis der Datenaufbereitungsstelle vorgeben. Das ließe sich einerseits bereits über eine Konkretisierung der Zweckbestimmung in § 303e Abs. 2 SGB V erreichen. Diese bietet zwar bereits Raum für wissenschaftliche Analysen. Die ausdrückliche Formulierung einer weiten Zweckbestimmung wäre dennoch erstrebenswert. Andererseits sollte beachtet werden, dass Anonymität im Verständnis der DS-GVO nicht gleichzusetzen ist mit absoluter Anonymität, so dass nicht jeder Vorgang der Bereitstellung von Versorgungsdaten zwangsläufig unter das unionale Datenschutzregime fällt. Eine Klarstellung, dass der SGB-Gesetzgeber in den §§ 303a ff. SGB V vom gleichen Verständnis der Anonymität ausgeht wie Erwägungsgrund 26 der DS-GVO ist empfehlenswert (s.o. C. III. 1. g)). Soweit Gesetzesänderungen die Verarbeitung personenbezogener Daten betreffen, müssen sich diese jedoch innerhalb der Vorgaben der DS-GVO bewegen. Durch die weiten Öffnungsklauseln gibt die DS-GVO dem nationalen Gesetzgeber im Bereich der §§ 303a ff. SGB V jedoch einen erheblichen Spielraum (s.o. A. III. 3. und B. II. 5. b)).

Auf grundrechtlicher Ebene stehen dabei dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG die Wissenschaftsfreiheit aus Art. 5 Abs. 3 S. 1 GG und

die grundrechtlich geschützte Gesundheit der Versicherten aus Art. 2 Abs. 2 S. 1 GG entgegen. Die § 303a ff. SGB V müssen hier den Rahmen für eine interessengerechte Abwägung schaffen. Zur Wahrung des Rechts auf informationelle Selbstbestimmung muss bei einer Novellierung der Datentransparenzregelungen auch weiter eine hinreichende Sicherung vor einer missbräuchlichen Verwendung der Versorgungsdaten im deutschen Recht verankert sein. In Kombination mit technisch-organisatorischen Maßnahmen der Datenaufbereitungsstelle, die die Identifizierung Versicherter verhindern sollen, sind sanktionsbewehrte Verbote ein taugliches Mittel zur Missbrauchsprävention. Insbesondere können die Sanktionen eine Abwägung zugunsten der Herausgabe von Daten positiv beeinflussen und stellen damit eine empfehlenswerte Neuerung dar (s.o. C. III. 1. h)).

Dabei sollten vorsorglich alle Änderungen, die potenziell einen Zulässigkeitstatbestand für einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, soweit möglich auf der Ebene der §§ 303a ff. SGB V und nicht in der DaTraV angesiedelt werden. Auf Verordnungsebene können lediglich weitere Konkretisierungen stattfinden. Zu beachten ist dabei das Gebot der Normklarheit, das auch fordert, dass allzu komplizierte Verweisungen zu unterlassen sind.

Eine Integration von Institutionskennzeichen der Leistungsträger ist unter den obigen Bedingungen (C. III. 1. c)) bei gleichzeitiger Wahrung des Betriebs- und Geschäftsgeheimnisses möglich. Ein Fernzugang wie in § 5 Abs. 5 S. 4 DaTraV-E vorgesehen, ist eine Möglichkeit, die Praxistauglichkeit der Datentransparenz zu erhöhen. Dies gilt freilich nur, soweit sich ein solcher Fernzugang technisch ausreichend sicher und praktikabel umsetzen lässt. Wichtig sind bei der Umsetzung des Fernzugangs, wie auch gegebenenfalls bei Beibehaltung der Zugriffsmöglichkeit auf Einzeldatensätze nur an Gastarbeitsplätzen, dass Zugriffe der Nutzungsberechtigten protokolliert werden, so dass im Falle eines Datenschutzrechtsverstoßes die Sanktionen auch praktische Wirksamkeit entfalten können.

2. Gesetzgeberischer Klarstellungs- und Anpassungsbedarf im SGB X

Es empfehlen sich im Anschluss an die obigen Ausführungen (B. III. 7.) zudem einige gesetzgeberische Klarstellungen und Anpassungen im SGB X.

a) § 76 Abs. 2 SGB X

Vor dem Hintergrund der oben gefundenen Ergebnisse stellt sich die Frage, ob es zweckmäßig ist, einen Ausnahmetatbestand in § 76 Abs. 2 SGB X für Datenübermittlungen nach

§ 75 SGB X vorzusehen. Da die betroffene Person über den Schutz des § 203 StGB uneingeschränkt disponieren, insbesondere einen Arzt auch von der Schweigepflicht entbinden kann, ist schon nach dem Wortlaut des § 76 SGB X bei entsprechender Schweigepflichtentbindung durch die betroffene Person (Patient) eine Übermittlung stets zulässig. Es könnte daher klarstellend eine Ausnahme in § 76 Abs. 2 SGB X für den Fall aufgenommen werden, dass die betroffene Person in die Datenübermittlung eingewilligt hat. Keine besondere Schutzbedürftigkeit besteht ferner, wenn die Stelle, an die Daten übermittelt werden, selbst dem Sozialgeheimnis oder einem Berufsgeheimnis unterliegt. Eine darüber hinausgehende Ausnahme müsste die besondere Bedeutung des von der berufs- und strafrechtlichen Schweigepflicht geschützten Vertrauensverhältnisses berücksichtigen, um den Anforderungen der Berufsfreiheit aus Art. 12 GG gerecht zu werden.

Da § 75 Abs. 1 S. 1 a.E. SGB X für die Zulässigkeit einer Datenübermittlung bereits fordert, dass „schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse der betroffenen Person erheblich überwiegt“, kann die besondere Schutzwürdigkeit der Daten bereits durch diese Interessenabwägung Berücksichtigung finden. Soweit im Einzelfall die Daten eine Identifizierung der betroffenen Person nicht zulassen, ist schon fraglich, ob ein Geheimnis im Sinne des § 203 Abs. 1 StGB vorliegt. Ist das nicht der Fall, so hätte der Berufsgeheimnisträger die Daten selbst ebenfalls übermitteln dürfen, so dass auch § 76 Abs. 1 SGB X einer Übermittlung nicht entgegensteht. Je unwahrscheinlicher eine Identifizierung der betroffenen Person ist, etwa weil die Daten pseudonymisiert übermittelt werden, desto weniger wird der verlängerte Berufsgeheimnisschutz beeinträchtigt und desto eher können Forschungsinteressen gegenüber dem Geheimhaltungsinteresse überwiegen.

Denkbar wäre daher die Schaffung eines Ausnahmetatbestandes in Art. 76 Abs. 2 SGB X als neue Nr. 4 der Norm, der seinerseits drei Fallgruppen abbilden könnte:

„4. im Rahmen des Art. 75 SGB X soweit,

a) die betroffene Person eingewilligt hat,

b) die Stelle, an die die Daten übermittelt werden, selbst einer umfassenden beruflichen Schweigepflicht oder dem Sozialgeheimnis unterliegt, oder

c) das Interesse an der Datenverarbeitung das Geheimhaltungsinteresse der betroffenen Person auch unter Berücksichtigung der besonderen Schutzbedürftigkeit der übermittelten Daten erheblich überwiegt, was insbesondere der Fall

sein kann, wenn eine Identifizierung der betroffenen Person aufgrund der Beschaffenheit der Daten unwahrscheinlich ist.“

b) § 78 SGB X

Es empfiehlt sich eine gesetzgeberische Klarstellung durch Aufnahme einer Ausnahme in § 78 SGB X. Normsystematisch würde sich insoweit die Ergänzung um einen Absatz 5 wie folgt anbieten:

„Die Absätze 1 bis 4 finden keine Anwendung, soweit die Daten auf Veranlassung der betroffenen Person übermittelt werden und diese anstelle der Übermittlung an den Empfänger auch die Herausgabe einer Datenkopie an sich selbst hätte verlangen können.“

IV. Bewertung der Reformvorschläge des Deutschen Ethikrates de lege ferenda

Da die Reformvorschläge des Deutschen Ethikrates eine Debatte über die Kompatibilität des derzeitigen Rechtsrahmens mit den technisch zur Verfügung stehenden Möglichkeiten durch Big-Data ausgelöst haben, sollen wesentliche Punkte aus den Vorschlägen abschließend analysiert und bewertet werden.

1. Abkehr vom Grundsatz der Datensparsamkeit bzw. der Datenminimierung?

Die Feststellung des Deutschen Ethikrats, dass die Grundsätze der Datensparsamkeit und Datenminimierung in „augenfälligem Widerspruch zu Big-Data“ stünden,²⁵⁹ erscheint nur auf den ersten Blick einleuchtend.²⁶⁰ Zwar ist es – wie der Terminus bereits nahelegt – ein Wesensmerkmal von Big-Data-Anwendungen, dass mit großen Datenmengen gearbeitet wird. Der Grundsatz der Datenminimierung steht dem jedoch nicht entgegen. Er besagt gerade nicht, dass nur kleine Mengen an personenbezogenen Daten verarbeitet werden dürfen. Vielmehr statuiert er den eigentlich selbstverständlichen Grundsatz, dass ein Grundrechtseingriff auf das notwendige Maß beschränkt bleibt. Sofern es einen plausiblen Zweck gibt, mit großen Datenmengen

²⁵⁹ *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 16.

²⁶⁰ So auch *Ohrtmann/Schwiering*, NJW 2014, 2984, 2985.

zu arbeiten, kann dies nach einer Abwägung der widerstreitenden Interessen ohne weiteres gerechtfertigt sein. Sicherlich sind Szenarien vorstellbar, bei denen das Datenschutzrecht hinderlich ist aus Sicht des Datenverarbeiters. Nichts anders gilt aber in der Offline-Welt beispielsweise für das Grundrecht auf körperliche Unversehrtheit etwa bei medizinischen Studien: Die gewonnenen Daten einer Studie wären sehr viel aussagekräftiger, wenn verpflichtend alle betroffenen Patienten daran teilnehmen müssten. Gleichwohl wird hier das Individualinteresse der Patienten höher gewichtet. Aufgabe des Rechtssystems ist es, Interessen zu einem vernünftigen Ausgleich zu bringen. Dies gilt auch für die Zulässigkeit von Big-Data-Analysen großer Mengen personenbezogener Daten. Der gegenwärtige Rechtsrahmen ist insoweit sehr flexibel, denn er bietet neben der Möglichkeit der Einwilligung auch einen sehr offen formulierten Zulässigkeitstatbestand der berechtigten Interessen in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO, der letztlich auf eine Interessenabwägung hinausläuft. Immer dann, wenn also das Interesse einer Datenverarbeitung gleich oder höher zu gewichten ist als das Interesse am Privatsphärenschutz der betroffenen Personen, darf die Datenverarbeitung erfolgen. Ist dies nicht der Fall, hat sie zu unterbleiben. Es ist nicht ersichtlich, weshalb diese sehr sinnvolle Systematik im Big-Data-Umfeld nicht ebenfalls gelten sollte.

Eine andere Frage ist, wie die konkreten Interessen gewichtet werden und ob nicht die derzeitige aufsichtsbehördliche Praxis und Rechtsprechung zu einer latenten Übergewichtung von Datenschutzinteressen neigen. Den eigentlich selbstverständlichen Grundsatz der Datenminimierung deshalb in Frage zu stellen, geht hingegen fehl. Angesichts seiner unionsrechtlichen Determination stieße trotz vorhandener Öffnungsklauseln seine Relativierung auch schnell an die Grenzen der EU-Datenschutzgrundrechte und der DS-GVO (sowie des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG).

2. Abkehr vom Grundsatz der Zweckbindung im Allgemeinen?

In einem Widerspruch zu den Möglichkeiten von Big-Data-Anwendung steht – zumindest scheinbar – auch der Zweckbindungsgrundsatz. Dieser für das Datenschutzrecht in der gegenwärtigen Form geradezu konstitutive Grundsatz kann nicht relativiert werden. Denn für den Privatsphärenschutz einer Person ist es entscheidend, zu welchen Zwecken eine Datenverarbeitung erfolgt. Daher ist dieser Grundsatz auch in besonderer Weise grundrechtssensibel. Der Zweckbindungsgrundsatz blieb auch bei der jüngsten Neuordnung der europäischen Datenschutzordnung erhalten (Art. 5 Abs. 1 lit. b DS-GVO). Ansätze, die auf eine Abkehr von diesem Grundsatz abzielen, haben ungeachtet der damit verbundenen unionsprimärrechtlichen

und verfassungsrechtlichen Schwierigkeiten auch politisch mittelfristig keine Aussicht auf eine Realisierung. Eine Umsetzung derartiger Vorschläge erscheint auch weder notwendig noch zweckmäßig. Im Umgang mit Big-Data-Anwendungen können und müssen vielmehr die Instrumente, die der gegenwärtige Rechtsrahmen bietet, sachgerecht angewendet werden. Insbesondere der sehr offen gehaltene Tatbestand des Art. 6 Abs. 4 DS-GVO zur Zweckänderung bietet die dafür erforderlichen normativen Ansätze. Es liegt nun an der Aufsichtspraxis und Rechtsprechung, die gegebenen Möglichkeiten auszugestalten. Eine Grundsatzdebatte, die die Pfadabhängigkeiten des über Jahrzehnte gewachsenen Datenschutzrechtssystems nicht berücksichtigt, führt hingegen gerade in der sich schnell wandelnden digitalen Welt nicht weiter.

3. Die Möglichkeit einer zweckungebundenen Datenspende im Besonderen

Versicherte, die freiwillig sie betreffende Gesundheitsdaten zum Zweck der medizinischen Forschung zur Verfügung stellen möchten, soll das Datenschutzrecht diesen Wunsch nicht verwehren. Insoweit hat jeder Versicherte die Möglichkeit, entsprechende Einwilligungen zu erteilen. Dabei ist oftmals jedoch die Bestimmtheit der Einwilligungserklärungen problematisch, wenn die Zwecke sehr allgemein gehalten werden, wie etwa die Einwilligung in die Verarbeitung zu jeglichen Zwecken, die der medizinischen Forschung dienen. Die Frage, unter welchen Voraussetzungen eine derartige Einwilligung hinreichend bestimmt ist, führt zu Rechtsunsicherheiten. Um diesem Problem zu begegnen, könnten klarere gesetzliche Leitlinien, inwiefern die Zustimmung einer Person zur Nutzung ihrer Daten zu Forschungszwecken eine darauf gestützte Datenverarbeitung zulässig ist, zweckdienlich sein. Insbesondere der Deutsche Ethikrat hat hierzu – wie oben ausführlich dargestellt (s.o. A. II. 3.) – die Einführung einer umfassenden Datenspende für Forschungszwecke vorgeschlagen.

Um im nationalen Recht entsprechende Regelungen zur Schaffung einer entsprechenden Datenspende treffen zu können, müssen sich die entsprechenden Empfehlungen (dazu d) im Rahmen des unionsrechtlichen (dazu a) und verfassungsrechtlichen Rahmens (dazu b) halten und insbesondere auch die Rechte Dritte wahren (dazu c).

a) Unionsrechtlicher Rahmen

Grundsätzlich sind die Voraussetzungen einer wirksamen Einwilligung vollständig auf unionaler Ebene durch die DS-GVO determiniert. Die umfassenden Öffnungsklauseln zu Gesundheitsdaten zielen jedoch insbesondere auf die Frage der Zulässigkeit der Verarbeitung ab und

ermöglichen es so den Mitgliedstaaten, im materiellen Datenschutzrecht eigene Zulässigkeitstatbestände zu schaffen. Da in Art. 6 DS-GVO die Einwilligung nur als ein Zulässigkeitstatbestand unter vielen aufgezählt wird, spricht das systematische Verständnis der Norm für die Möglichkeit der Mitgliedstaaten, auch die Voraussetzungen und Wirkungen einer Einwilligung abweichend zu regeln, soweit ihnen die DS-GVO einen materiellen Handlungsspielraum eröffnet. Auch wenn nicht ausgeschlossen scheint, dass der EuGH mit dem Ziel, eine größtmögliche Harmonisierung durch den „effet utile“ (Art. 4 Abs. 3 EUV) der DS-GVO sicherzustellen, künftig innerhalb der Öffnungsklauseln die weiteren Vorgaben der DS-GVO für durch den nationalen Gesetzgeber nicht disponibel erachten wird, sprechen jedenfalls für die materiell-rechtlichen Vorgaben die besseren Argumente für die hier vertretene Auffassung. Gleichwohl verbleibt insoweit das Restrisiko der Unanwendbarkeit entsprechender Normen mit der Folge weiter steigender Rechtsunsicherheit.

b) Verfassungsrechtlicher Rahmen

Das Grundgesetz stellt nach der Rechtsprechung des Bundesverfassungsgerichts besonders strenge Anforderungen an die Normenklarheit im Bereich des Datenschutzrechts.²⁶¹ Eine Regelung der Datenspende zu Zwecken der medizinischen und pharmakologischen Forschung sowie der Versorgungsforschung muss daher den rechtsstaatlichen Anforderungen an die Normenklarheit genügen, sofern sie einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.²⁶² Richtigerweise stellt das Einverständnis mit der Verarbeitung der eigenen Daten selbst jedoch keinen (gerechtfertigten) Eingriff in das Recht auf informationelle Selbstbestimmung dar, sondern ist der Konzeption des Rechts auf informationelle Selbstbestimmung folgend vielmehr gerade eine Freiheitswahrnehmung des Einzelnen.²⁶³ Das Grundrecht auf informationelle Selbstbestimmung beschränkt also nicht nur die Möglichkeiten der Datenverarbeitung, es fordert vielmehr geradezu hinreichende Optionen, die Verarbeitung der eigenen Daten auch zu erlauben. Es schützt den Grundrechtsberechtigten daher nicht nur negativ vor der Verarbeitung seiner Daten, sondern ermöglicht ihm positiv auch die Freigabe seiner Daten.

²⁶¹ Kritisch dazu *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 73 f. m.w.N.

²⁶² BVerfG, Beschluss vom 23.2.2007 - 1 BvR 2368/06 = NVwZ 2007, 688, 690.

²⁶³ *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 497.

c) Berücksichtigung der Rechte Dritter

Denkbar erscheint es, dass in besonderen Fällen auch die Interessen Dritter, insbesondere der Angehörigen von Patienten, betroffen sein können.²⁶⁴ Dies ist etwa bei Daten über vererbare Krankheiten anzunehmen. Hier können neben dem Patienten auch dessen Angehörige betroffene Personen sein, wenn sie identifizierbar sind. Dies hat zur Folge, dass eine Einwilligung des Patienten in die Verarbeitung dieser Daten als Legitimationsgrundlage nicht ausreichen kann, wenn sich die Daten auch auf Angehörige beziehen. Solange die Angehörigen jedoch nur identifizierbar sind, nicht aber identifiziert werden, ist ein Überwiegen der berechtigten Forschungsinteressen der Regelfall, so dass als Zulässigkeitstatbestand insoweit vor allem Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO in Betracht kommt. Informationspflichten, insbesondere über das Widerspruchsrecht der mitbetroffenen Angehörigen nach Art. 21 DS-GVO sind dann ebenfalls gemäß Art. 11 Abs. 1 DS-GVO entbehrlich. Die Mitbetroffenheit von Angehörigen wird bei der Verarbeitung von Gesundheitsdaten also erst dann wirklich relevant, wenn die Angehörigen auch tatsächlich mit in die Datei aufgenommen werden, etwa um über die Wahrscheinlichkeit einer Vererbbarkeit von Krankheiten zu forschen. Die reine Mitbetroffenheit von Angehörigen hat ansonsten keine erheblichen praktischen Auswirkungen.

d) Handlungsempfehlung

Um größtmögliche Rechtssicherheit herzustellen, könnte sich anstelle der Modifikation der Vorgaben zur Einwilligung auch die Schaffung eines gesetzlichen Zulässigkeitstatbestandes für die medizinische Forschung anbieten. Auf diese Weise ließe sich das Konzept einer umfassenden Datenspende am sichersten unionsrechtskonform umsetzen, wenn man den Zulässigkeitstatbestand unter den Vorbehalt der Zustimmung der betroffenen Person stellt. Insoweit könnte zwar angenommen werden, dass letztlich die Vorgaben der Einwilligung unterlaufen werden, wenn die Anforderungen an die Zustimmung im Rahmen des gesetzlichen Zulässigkeitstatbestandes niedriger sind als diejenigen für eine wirksame Einwilligung. Dem ließe sich jedoch entgegen halten, dass es dem nationalen Gesetzgeber wohl unbenommen wäre, einen vollumfänglichen gesetzlichen Zulässigkeitstatbestand für Zwecke der medizinischen Forschung vorzusehen, soweit nicht zwingende Interessen des Betroffenen entgegenstehen. Inso-

²⁶⁴ *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2018, S. 267.

weit muss erst recht bei einem zusätzlichen Zustimmungsvorbehalt ein entsprechender Zulässigkeitsstatbestand möglich sein, da der betroffenen Person insoweit mehr Einwirkungsmöglichkeiten eingeräumt werden als ohne. Bei einer Zustimmung der betroffenen Person können auch keine zwingenden Interessen der betroffenen Person entgegenstehen. Entscheidend ist dafür, dass die Zustimmung in freiwilliger und informierter Weise erteilt wird. Diese an die Einwilligung angelehnten Voraussetzungen könnten im Gesetz näher ausgestaltet werden, indem etwa eine Musterzustimmungserklärung in das Gesetz selbst oder in eine Rechtsverordnung aufgenommen wird, um so die notwendige Rechtssicherheit zu garantieren. Damit könnte der Gesetzgeber letztlich ein „Standardmodell“ schaffen, das neben das Instrument der Einwilligung tritt und den Fall abdeckt, dass einzelne Personen ihre Daten allgemein für die medizinische Forschung zur Verfügung stellen möchten, ohne sich im Detail Gedanken machen zu wollen, für welche konkreten Anwendungsbereiche in der Forschung diese gelten soll. Damit werden die mit der Einwilligung einhergehenden Rechtsunsicherheiten und Schwierigkeiten bei der Formulierung rechtswirksamer Einwilligungserklärungen vermieden. Die Eingriffstiefe in die Rechte der betroffenen Person ist nicht besonders groß, da sie insgesamt zustimmen muss und daneben mit der Einwilligung auch weiterhin alle bestehenden Möglichkeiten der graduellen Abstufungen bei der Freigabe der eigenen Daten nutzen kann (von vollständiger Veröffentlichung gemäß Art. 9 Abs. 2 lit. e DS-GVO als zweckungebundene Freigabe an einen unbestimmten Personenkreis bis zu einer sehr eng gefassten Zweckbestimmung, etwa für eine bestimmte Studie).

In verfassungsrechtlicher Hinsicht muss insbesondere die Normenklarheit eines gesetzlichen Zulässigkeitsstatbestandes sichergestellt werden, denn es handelt sich insoweit um eine gesetzliche Legitimationsgrundlage. Aufgrund der sachlichen Nähe zur Einwilligung sind die Anforderungen insoweit allerdings nicht allzu hoch anzusetzen. Zweckmäßig – aber auch ausreichend – erscheint es, wenn der Begriff der medizinischen Forschung näher definiert wird, ohne vollständig auf unbestimmte Rechtsbegriffe zu verzichten und eine gewisse Offenheit zu erhalten. Es sollte jedoch seitens des Gesetzgebers klargestellt werden, welche Formen der Forschung umfasst sein sollen, insbesondere im Hinblick auf die Frage etwaiger Publikationspflichten oder auch die Verfolgung von primär finanziellen Interessen bei einem Forschungsprojekt.

Gesetzessystematisch wird eine Regelung in einem eigenständigen Gesundheitsdatenspendengesetz (GDSG) den breit gestreuten Normen im Gesundheitsdatenschutzrecht am ehesten gerecht. Eine Gesetzgebungskompetenz könnte sich aus Art. 74 Abs. 1 Nr. 13 GG ableiten lassen.

Demnach hat der Bund einen Kompetenztitel im Rahmen der konkurrierenden Gesetzgebung zur Förderung der wissenschaftlichen Forschung. Die Förderung der wissenschaftlichen Forschung umfasst die Regelung finanzieller, organisatorischer und planerischer Maßnahmen zur Forschungsförderung.²⁶⁵ Dies bezieht sich richtigerweise auch auf die Schaffung eines sicheren Rechtsrahmens zur Datenverarbeitung, um damit die Forschung anhand von Gesundheitsdaten zu fördern. Eine bundeseinheitliche Regelung ist auch zur Wahrung der Rechtseinheit im Sinne des Art. 72 Abs. 2 GG erforderlich, da nur auf der Basis konsistenter Einwilligungen Forschungsdaten aus dem gesamten Bundesgebiet rechtssicher verarbeitet werden können. Gleichwohl verbleiben insoweit Risiken, die einmal mehr Anlass geben sollten, die Schaffung eines einheitlichen (konkurrierenden) Gesetzgebungstitel für dem Bund im Bereich des Datenschutzrechts zu erwägen.²⁶⁶ Die horizontale Bedeutung des Datenschutzes in vielen Bereichen erfordert einen bundeseinheitlichen Ansatz, auch um die Komplexität beim Zusammenspiel verschiedener Normenwerke im Mehrebenensystem zu reduzieren.

4. Ergänzende Einführung eines Konzepts der Datensouveränität?

Es wurde bereits darauf hingewiesen, dass der verfassungsgerichtlichen Konzeption des deutschen Datenschutzgrundrechts als Recht auf informationelle Selbstbestimmung dem Grunde nach eine Datensouveränität immanent ist (s.o. B.V.4.). Kerninstrument, das eine stärkere Akzentuierung der Selbstbestimmung im Sinne einer Legitimierung von Datenverarbeitungsprozessen im Gesundheitswesen durch den Betroffenen, also den Patienten, ermöglicht, ist dabei die Einwilligung. Anhand der Datenspende wurde exemplarisch aufgezeigt, wie diese insoweit ertüchtigt werden kann, gerade auch in der Abwandlung einer flankierenden gesetzlichen Regelung im Verbund mit einer Zustimmung. Andere Normbereiche – etwa die Vorgaben zur elektronischen Patientenakte – können identifiziert werden, in denen ähnliche Gestaltungsmöglichkeiten für den Gesetzgeber bestehen und durchaus genutzt werden sollten.

Im Übrigen bedarf es eines neuen Konzeptes der Datensouveränität jedoch nicht und die „Flughöhe“ des Konzepts ist jedenfalls für die Steuerungsansätze in den Sozialgesetzbüchern zu hoch, um dies allgemein zu verankern. Vielmehr muss es in der Form der stärkeren Akzentu-

²⁶⁵ Maunz in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, 86. EL Januar 2019, Art. 74 Rn. 179 m.w.N.; Seiler in: Epping/Hillgruber (Hrsg.), BeckOK Grundgesetz, 41. Edition, Stand: 15.02.2019, Art. 74 Rn. 54.

²⁶⁶ So auch Kircher, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 252; zur föderalen Gemengelage bereits Kingreen/Kühling, JZ 2015, 213, 214.

ierung der verfassungsrechtlichen Selbstbestimmung als Legitimationsquelle für Datenverarbeitungsprozesse in den einzelnen Regelungsbereichen konkret verwirklicht und gleichsam „klein gearbeitet“ werden, um so inhaltlich das berechtigte Interesse an einer größeren „Datensouveränität“ im Sinne einer informationellen Selbstbestimmung zu gewährleisten.

D. Zusammenfassung der Ergebnisse; Handlungsempfehlungen mit konkreten Vorschlägen für Gesetzesänderungen

I. Hintergrund, Stoßrichtung und Eingrenzung der Untersuchung

1. Zunehmende Big-Data-Anwendungen; Reformvorschläge des Deutschen Ethikrates

1. Hauptanlass des vorliegenden Rechtsgutachtens ist die zunehmende Verwendung von Big-Data-Analysen im Gesundheitswesen, die eine Fülle datenschutzrechtlicher Fragen aufwirft.
2. Unter dem Begriff des Gesundheitswesens wird dabei allgemein – und auch vorliegend – die Organisation der Gesundheitsversorgung durch die gesetzliche und private Krankenversicherung verstanden.
3. Das Gutachten fokussiert dabei die Regelungen der gesetzlichen Krankenkassen und daher den Umgang mit Sozialdaten. Darunter sind gemäß § 67 Abs. 2 SGB X sämtliche personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO zu verstehen, allerdings nur, soweit sie von den in § 35 SGB I aufgezählten Stellen, insbesondere den Leistungsträgern erhoben, verarbeitet und genutzt werden.
4. Weiterer Anstoß der Untersuchung sind die Reformvorschläge, die der Deutsche Ethikrat für die Fortentwicklung des Datenschutzrechts in einem Gutachten Ende 2017 unterbreitet hat. Der Deutsche Ethikrat adressiert – wie auch das vorliegende Gutachten – die Frage, ob das geltende Gesundheitsdatenschutzrecht den Herausforderungen von Big-Data-Anwendungen gerecht wird, diese unter Wahrung eines angemessenen Datenschutzes ermöglicht oder ob Anpassungen de lege ferenda erforderlich sind.

2. Stoßrichtung der Untersuchung

5. Vor diesem Hintergrund untersucht das Rechtsgutachten den Regelungsrahmen für Big-Data-Anwendungen auf verschiedenen Ebenen: Insbesondere anlässlich der Vorschläge des Deutschen Ethikrates wurde auf einer sehr prinzipiellen „Meta-Ebene“ der Frage nachgegangen, ob es einer fundamentalen Neuausrichtung des (Gesundheits-) Datenschutzrechts im Zeitalter von Big-Data-Anwendungen bedarf. Auf einer deutlich spezifischeren normativen Ebene wurden einzelne für den Datenschutz und Big-Data-Anwendungen im Gesundheitswesen zentrale Paragraphen des SGB V und SGB X auf ihre Zweckmäßigkeit hin betrachtet. Schließlich wurden, gleichsam auf einer „Micro-Ebene“, dabei auch sehr genaue Untersuchungen zur spezifischen Funktionsweise der Normen angestellt. Daraus wurden sodann jeweils mögliche Änderungsvorschläge de lege ferenda entwickelt. Auf der Detailebene wurde zudem umfassend die Idee einer Datenspende geprüft und normativ verortet.
6. Nicht weiter nachgegangen wurden gleichsam auf einer „Mezzo-Ebene“ angesiedelte systematische Fragen, ob und wie das Datenschutzrecht im Gesundheitswesen durch eine grundlegende Neustrukturierung der relevanten Normen im SGB V und SGB X verbessert werden könnte bzw. ob und inwiefern gegebenenfalls der Detaillierungsgrad der Regelungen zurückgefahren werden sollte. Gleichwohl weisen die Ergebnisse des vorliegenden Gutachtens darauf hin, dass

eine systematische Vereinfachung und stärkere Rückführung auf allgemeine datenschutzrechtliche Grundanforderungen unter Zurückdrängung komplexitätsreicher Detailregelungen sinnvoll sein dürfte, wobei insoweit Näheres einer eigenen Untersuchung vorbehalten bliebe.

3. Definition von „Big Data“

7. Unter „Big Data“ werden im Gutachten als Sammel- oder Oberbegriff solche Anwendungen, Applikationen oder Analyseprogramme verstanden, die eine außerordentlich große und gegebenenfalls heterogene Datenmenge innerhalb kurzer Zeit (oder in Echtzeit) auswerten. Als Kernmerkmale werden häufig die „drei Vs“ genannt: volume (Menge), velocity (Geschwindigkeit/Echtzeit) und variety (unterschiedliche Daten). Hinzu kommen teilweise noch validity (Richtigkeit bzw. Wahrheitsgehalt der Daten) oder alternativ veracity (Genauigkeit) und value (wirtschaftlicher Wert), so dass man auch von „fünf Vs“ sprechen kann. Eine außergewöhnlich hohe Trennschärfe bietet der Begriff damit nicht und kann schon gar nicht als rechtliche Definition verstanden werden.
8. Jedoch treten im Rahmen von Big-Data-Anwendungen in der Regel eine Reihe von Besonderheiten auf, die sodann (datenschutz-)rechtliche Fragestellungen aufwerfen. Hierzu zählt vor allem die Vorgehensweise, dass – anders als bei vielen herkömmlichen Analysetechniken – nicht gezielt nach der Antwort auf eine bestimmte Fragestellung gesucht wird, sondern die Anwendung ergebnisoffen nach Mustern und Zusammenhängen sucht, woraus sich gänzlich neue Erkenntnisse ergeben können. Durch das Aufzeigen von Korrelationen kann die Big-Data-Anwendung so oftmals dazu beitragen, die richtigen Fragen überhaupt erst zu stellen. Dementsprechend groß sind die Hoffnungen, die in verschiedensten Lebensbereichen – insbesondere auch im Gesundheitssektor – in Big-Data-Techniken gesetzt werden. Demgegenüber stehen jedoch die Risiken, die mit der systematischen Auswertung solch großer Datenmengen einhergehen. Die Persönlichkeitsrechtsverletzungen bei einer Big-Data-Anwendung werden in der Regel Folgen für eine große Zahl von Betroffenen entfalten. Werden darüber hinaus auch noch sensible Daten (wie Gesundheitsdaten) verarbeitet, können Datenschutzrechtsverstöße besonders schwer wiegen.
9. Unter Gesundheitsdaten sind dabei nach Art. 4 Nr. 15 DS-GVO „personenbezogene Daten, die sich auf den körperlichen oder geistigen Gesundheitszustand einer natürlichen Person, einschließlich der Erbringung von Gesundheitsleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“ zu verstehen. Der Begriff ist grundsätzlich weit auszulegen.

4. Big-Data-Anwendungen in der Realwelt von SGB V und SGB X

10. Big-Data-Anwendungen kommen innerhalb der gesetzlichen Krankenkassen in verschiedenen Anwendungsgebieten zum Einsatz. Relevante Zielsetzungen entspringen vor allem den Bereichen der Finanzen, der Steuerung oder teils des Marketings und des Vertriebs. Dabei kommen Big-Data-Anwendungen in den Anwendungsfeldern Versorgung und Marktanalyse deutlich stärker zum Einsatz als in den Bereichen des Personals, des Rechts und der Finanzen. Die

größten Datenquellen stellen neben den Stamm- und Abrechnungsdaten auch gesetzliche Quellen wie amtliche Statistiken und die im Zuge der Datentransparenz i.S.d. §§ 303a ff. SGB V zugänglichen Datensätze dar.

11. Das andere große Anwendungsfeld bildet die medizinische und pharmakologische Forschung sowie die Versorgungsforschung mit den Sozialdaten. Daneben eröffnet § 287 SGB V in Ergänzung zu den Vorschriften der §§ 67c Abs. 5 sowie 75 SGB X den Zugriff auch für die Entwicklung eigener Forschungsprojekte der Krankenkassen.
12. Diese sektorspezifischen Vorgaben sind auch weiterhin die zentralen Steuerungsnormen, da die an sich auf Vollharmonisierung angelegte Datenschutz-Grundverordnung durch weit gefasste Öffnungsklauseln gerade im Gesundheitswesen (insbesondere mit Art. 9 Abs. 2 lit. h DS-GVO) geprägt ist. Allerdings werden die Regelungen im SGB V und SGB X durch die allgemeinen Bestimmungen der DS-GVO vorgesteuert, insbesondere zur Definition des Begriffs des personenbezogenen Datums einschließlich pseudonymer Daten und in Abgrenzung zu anonymisierten Daten.

II. Der rechtliche Handlungsrahmen im geltenden Recht

1. Der Anwendungsbereich des Datenschutzrechts

a) Begriff des personenbezogenen Datums in Abgrenzung zu anonymen Daten

13. Das Datenschutzrecht als Schutzordnung der Privatsphäre von natürlichen Personen ist nämlich nur anwendbar, soweit es um Daten geht, die sich auf die betroffene Person beziehen, einschließlich pseudonymer, nicht aber anonymer Daten. Art. 4 Nr. 1 DS-GVO umfasst ohne Einschränkung „alle Informationen“, die sich auf eine Person beziehen und ist daher grundsätzlich weit zu verstehen. Die Informationen müssen sich auf eine identifizierte oder identifizierbare Person beziehen. Von einer identifizierten Person ist auszugehen, wenn die Identität der Person unmittelbar aus der Information selbst folgt.
14. Dagegen ist eine Person identifizierbar, wenn die Information zwar für sich genommen nicht ausreicht, um sie einer Person zuzuordnen, dies aber gelingt, sobald die Information mit weiteren Informationen, die für den Verantwortlichen verfügbar sind, verknüpft wird. So bestimmt Art. 4 Nr. 1 DS-GVO, dass eine Person dann identifizierbar ist, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
15. Nach Erwägungsgrund 26 der DS-GVO sind bei der Frage, ob eine Person identifizierbar ist, alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Frage, welche Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, sind nach Erwägungsgrund 26 der DS-GVO alle über die betreffende Person bekannten oder ermittelbaren Informationen sowie alle objektiven

Faktoren heranzuziehen, wie z.B. die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand.

16. Nach verbindlicher Ansicht des EuGH sind dabei alle rechtlichen Mittel zu berücksichtigen, die legaler Weise bestehen, um sich die Daten des Dritten verfügbar zu machen, auch wenn dies über den Umweg staatlicher Behörden erfolgt. Gesetzlich verbotene Möglichkeiten haben dagegen außer Betracht zu bleiben.
17. Es wurde näher dargelegt, dass vor diesem Hintergrund Institutionskennzeichen und mit diesem verknüpfte Daten als personenbeziehbar zu qualifizieren sind.

b) Pseudonymisieren

18. Die DS-GVO definiert in Art. 4 Nr. 5 das Pseudonymisieren als die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Eine Pseudonymisierung stellt daher keine Anonymisierung, sondern – wie Art. 32 Abs. 1 lit. a DS-GVO verdeutlicht – eine bloße Sicherungsmaßnahme dar. Das Ziel der Pseudonymisierung besteht nach Erwägungsgrund 28 der DS-GVO darin, die Risiken für betroffene Personen zu senken und den Verantwortlichen und Auftragsverarbeiter bei der Einhaltung der Datenschutzpflichten zu unterstützen.

2. Zentrale Datenschutzgrundsätze

19. Wichtige, auch im Gesundheitssektor relevante Konzepte, die im Rahmen des Gutachtens zur Orientierung näher erläutert wurden, sind sodann die zentralen Datenschutzgrundsätze der Datensparsamkeit bzw. Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO), der Zweckbestimmung bzw. -begrenzung (Art. 5 Abs. 1 lit. b DS-GVOs), das Erforderlichkeitsprinzip (vgl. Art. 6 Abs. 1 UAbs. 1 lit. b bis f DS-GVO) sowie die Voraussetzungen für eine wirksame Einwilligung (Art. 6 Abs. 1 UAbs. 1 DS-GVO; Art. 4 Nr. 11 DS-GVO; Art. 7 DS-GVO; Art. 9 Abs. 2 lit. a DS-GVO).

III. Bewertung der Reformvorschläge des Deutschen Ethikrates

20. Die Vorschläge des Deutschen Ethikrates sind vor dem Hintergrund der Ausführungen im Gutachten im Ergebnis differenziert zu bewerten.

1. Ergänzende Einführung eines Konzepts der Datensouveränität?

21. Das Plädoyer des Deutschen Ethikrates für die stärkere Ausrichtung an einem „neuartigen“ Konzept einer „Datensouveränität“ ist wenig zielführend.
22. So ist der verfassungsgerichtlichen Konzeption des deutschen Datenschutzgrundrechts als Recht auf informationelle Selbstbestimmung dem Grunde nach bereits eine Datensouveränität immanent.

23. Kerninstrument, das eine stärkere Akzentuierung der Selbstbestimmung im Sinne einer Legitimierung von Datenverarbeitungsprozessen im Gesundheitswesen durch den Betroffenen, also den Versicherten bzw. Patienten, ermöglicht, ist dabei die Einwilligung.
24. Anhand der Datenspende wurde exemplarisch aufgezeigt, wie diese insoweit ertüchtigt werden kann.
25. Andere Normbereiche – etwa die Vorgaben zur elektronischen Patientenakte – können identifiziert werden, in denen ähnliche Gestaltungsmöglichkeiten für den Gesetzgeber bestehen und durchaus genutzt werden sollten.
26. Im Übrigen bedarf es eines neuen Konzeptes der Datensouveränität jedoch nicht und die „Flughöhe“ des Konzepts ist jedenfalls für die Steuerungsansätze in den Sozialgesetzbüchern zu hoch, um dies allgemein zu verankern. Vielmehr muss es in der Form der stärkeren Akzentuierung der verfassungsrechtlichen Selbstbestimmung als Legitimationsquelle für Datenverarbeitungsprozesse in den einzelnen Regelungsbereichen konkret verwirklicht und gleichsam „klein gearbeitet“ werden, um so inhaltlich das berechtigte Interesse an einer größeren „Datensouveränität“ im Sinne einer informationellen Selbstbestimmung zu gewährleisten.

2. Abkehr vom Grundsatz der Datensparsamkeit bzw. der Datenminimierung?

27. Hinsichtlich der Grundsätze der Datensparsamkeit bzw. der Datenminimierung besteht kein legislativer Anpassungsbedarf.
28. Eine andere Frage ist, wie die konkreten Interessen gewichtet werden und ob nicht die derzeitige aufsichtsbehördliche Praxis und Rechtsprechung zu einer latenten Übergewichtung von Datenschutzinteressen neigen. Hier ist die weitere Entwicklung unter der Herrschaft der DS-GVO abzuwarten, die durchaus einen vernünftigen Ausgleich ermöglicht.
29. Den Grundsatz der Datenminimierung als Kernelement der Traditionen der Datenschutzgesetzgebung in Frage zu stellen, geht jedenfalls fehl. Angesichts seiner unionsrechtlichen Determination stieße trotz vorhandener Öffnungsklauseln seine Relativierung auch schnell an die Grenzen der DS-GVO sowie der EU-Datenschutzgrundrechte (und des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG).

3. Abkehr vom Grundsatz der Zweckbindung im Allgemeinen?

30. Dasselbe gilt für die Idee einer Abkehr vom Grundsatz der Zweckbindung. Eine Umsetzung dieses Vorschlags ist ebenfalls weder notwendig noch zweckmäßig.
31. Im Umgang mit Big-Data-Anwendungen können und müssen vielmehr die Instrumente, die der gegenwärtige Rechtsrahmen bietet, sachgerecht angewendet werden. Insbesondere der sehr offen gehaltene Tatbestand des Art. 6 Abs. 4 DS-GVO zur Zweckänderung bietet – auch soweit Gesundheitsdaten betroffen sind – die dafür erforderlichen normativen Ansätze. In der praktischen Bedeutung kommt Art. 6 Abs. 4 DS-GVO daher eine ähnliche Funktion wie einem gesetzlichen Zulässigkeitstatbestand zu.
32. Es liegt nun an der Aufsichtspraxis und Rechtsprechung, die gegebenen Möglichkeiten auszugestalten.

33. Eine Grundsatzdebatte, die die Pfadabhängigkeiten des über Jahrzehnte gewachsenen Datenschutzrechtssystems nicht berücksichtigt, führt hingegen gerade in der sich schnell wandelnden digitalen Welt nicht weiter.

4. Die Möglichkeit einer zweckungebundenen Datenspende im Besonderen

34. Zielführend ist dagegen der Anstoß zur konkreten Erleichterung einer möglichst weitreichenden zweckungebundenen Datenspende, die als Zweck sämtliche denkbaren Verarbeitungsszenarien im Rahmen der medizinischen Forschung ermöglicht.
35. Diese ist zwar schon jetzt grundsätzlich im Rahmen einer Einwilligung rechtlich möglich. Gegebenenfalls könnten die Einwilligungsbedingungen insoweit sektorspezifisch erleichtert werden.
36. Um größtmögliche Rechtssicherheit herzustellen, bietet sich die Schaffung eines gesetzlichen Zulässigkeitstatbestandes für die medizinische und pharmakologische Forschung und gegebenenfalls auch Versorgungsforschung an. Dies schließt die Möglichkeit der Beschränkung auf einen spezifischen Adressatenkreis, namentlich Forscher, ein. Auf diese Weise ließe sich das Konzept einer umfassenden Datenspende am sichersten unionsrechtskonform umsetzen, wenn man den Zulässigkeitstatbestand unter den Vorbehalt der Zustimmung der betroffenen Person stellt. In verfassungsrechtlicher Hinsicht muss insbesondere die Normenklarheit eines gesetzlichen Zulässigkeitstatbestandes sichergestellt werden. Zweckmäßig – aber auch ausreichend – ist es, wenn der Begriff der medizinischen und pharmakologischen Forschung und Versorgungsforschung näher definiert wird, ohne vollständig auf unbestimmte Rechtsbegriffe zu verzichten und eine gewisse Offenheit zu erhalten. Es sollte jedoch seitens des Gesetzgebers klar gestellt werden, welche Formen der Forschung umfasst sein sollen.
37. Gesetzessystematisch wird eine Regelung in einem eigenständigen Gesundheitsdatenspendegesetz (GDSG) den breit gestreuten Normen im Gesundheitsdatenschutzrecht am ehesten gerecht.

IV. Konkrete Gesetzgebungsempfehlungen hinsichtlich der Datentransparenz gemäß den §§ 303a ff. SGB V und im § 76 SGB X

38. Über diese teils sehr breiten Vorschläge des Deutschen Ethikrates hinaus hat die Analyse der Verbesserungsoptionen im SGB V (und SGB X) vor dem Hintergrund der durch den Referententwurf (SGB V-E) bereits angestoßenen Reformdebatte folgende Ergebnisse erzielt.

1. Datenumfang auf der Ebene eines formellen Gesetzes

39. Bei einer möglichen Neuregelung der Datentransparenz i.S.d. §§ 303a ff. SGB V sollte vorsorglich eher von einem streng verstandenen Parlamentsvorbehalt ausgegangen werden.
40. Das Gebot der Normenklarheit legt nahe, auf allzu komplizierte Verweisungen gänzlich zu verzichten.
41. Es bietet sich an, in den §§ 303a ff. SGB V die zu erhebenden Daten möglichst genau zu definieren, um sodann im Rahmen einer Verordnungsermächtigung vor allem Einzelfragen der

Erhebung der Daten zu regeln und bezüglich des Umfangs der Daten lediglich Konkretisierungen vorzunehmen.

42. § 303b Abs. 1 SGB V-E und § 303b Abs. 1 S. 1 SGB V-KE verfolgen hier bereits einen relativ pragmatischen Ansatz, zumal dort eine Aufzählung der zu erhebenden Daten erfolgt.

2. Schutz der Betriebs- und Geschäftsgeheimnisse

43. Es muss sichergestellt werden, dass Konkurrenten der Leistungserbringer die Daten nicht zum Zweck der Aufdeckung von Betriebs- und Geschäftsgeheimnissen nutzen. Auch die Betriebs- und Geschäftsgeheimnisse der Leistungsträger sind angemessen zu schützen.
44. Hierzu könnte im SGB V eine Regelung ergänzt werden. Beispielsweise könnte in § 303d SGB V ein Satz eingefügt werden, der besagt, dass es auch Aufgabe der Datenaufbereitungsstelle ist, zu verhindern, dass Konkurrenten von Leistungserbringern oder Leistungsträgern zum Zweck der Aufdeckung von Betriebs- und Geschäftsgeheimnissen und nicht bloß zu Forschungszwecken Daten verarbeiten.
45. Dies sollte dann sinnvollerweise (ähnlich wie bei der Reidentifikation) mit einem an die nutzungsberechtigte Stelle gerichteten Verbot der Ausspähung von Geschäftsgeheimnissen konkurrierender Leistungserbringer gekoppelt werden und könnte in § 303e SGB V-E wie folgt angefügt werden:

„Die Verarbeitung der bereit gestellten Daten zum Zwecke der unbefugten Identifizierung von Leistungserbringern oder Leistungsträgern sowie zur bewussten Verschaffung von Kenntnissen über fremde Betriebs- und Geschäftsgeheimnisse ist untersagt.“

46. Sodann könnte § 307b SGB V um einen hierzu korrelierenden Straftatbestand ergänzt werden:
- „Wer die ihm im Rahmen der Datentransparenz zur Verfügung gestellten Daten nutzt, um sich oder einem Dritten bewusst Kenntnis von fremden Betriebs- und Geschäftsgeheimnissen zu verschaffen oder ein solches Geheimnis zu nutzen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unbefugt bestimmte Leistungserbringer oder Leistungsträger identifiziert.“*

Die Tatbestandsmerkmale „bewusst“ und „unbefugt“ sollen berechnete Forschungsinteressen ausnehmen.

47. In der DaTraV könnte sodann ergänzend folgende Regelung vorgesehen werden:

„Rechtfertigen Tatsachen die Annahme, dass der Antragsteller sich über dieses Verbot hinwegsetzt, so kann der Antrag abgelehnt oder nur eingeschränkt bewilligt werden.“

Die Datenaufbereitungsstelle wird so in die Lage versetzt, geeignete Maßnahmen zu ergreifen, um unzuverlässige Antragsteller auszuschließen. Die Einräumung eines weiten Ermessensspielraums der Behörde sorgt für die erforderliche Flexibilität in der Handhabung und einen unbürokratischen Antragsprozess. Insbesondere sollte vermieden werden, die Behörde durch einen vorgeschriebenen Prüfprozess, der über eine bloße Evidenzkontrolle hinausgeht, zu überfordern.

3. Zweckbindung und Öffnung für die Forschung

a) Klarstellung hinsichtlich des Katalogs des § 303e Abs. 2 SGB V

48. Die Frage, ob der Katalog des § 303e Abs. 2 SGB V abschließend ist, sollte im Gesetz beantwortet werden. Der Referentenentwurf behält in § 303e Abs. 2 SGB V-E das „insbesondere“ bei und ersetzt dafür die Formulierung „dem Katalog des Absatz 2 entspricht“ in § 303e Abs. 3 S. 1 SGB V durch „prüft das Vorliegen der Voraussetzungen nach Absatz 1 und 2“ (§ 303e Abs. 3 S. 1 SGB V-E). Dies würde eine begrüßenswerte Klarstellung zugunsten eines nicht abschließenden Kataloges bedeuten. Ebenso denkbar ist aber auch eine Klarstellung in die entgegengesetzte Stoßrichtung, indem das „insbesondere“ ganz weggelassen wird. Diesen Ansatz verfolgt § 303e Abs. 2 SGB V-KE.

b) Klarstellung bezüglich des Umfangs der Zweckbindung in der Wissenschaft

49. Klarstellungsbedarf besteht auch hinsichtlich der Frage, welche wissenschaftlichen Vorhaben von der Zweckbestimmung umfasst sind. Eine Ergänzung des § 303e Abs. 2 SGB V könnte die Rechtsfrage abschließend klären. So ist folgende Formulierung des § 303e Abs. 2 Nr. 4 SGB V möglich:

„4. Längsschnittanalysen über längere Zeiträume, Analysen von Behandlungsabläufen, Analysen des Versorgungsgeschehens zum Erkennen von Fehlentwicklungen und von Ansatzpunkten für Reformen (Über-, Unter- und Fehlversorgung), insbesondere im Rahmen unabhängiger wissenschaftlicher Forschung; hierzu zählen auch Vorhaben, die im Rahmen der Erstellung wissenschaftlicher Qualifikationsschriften wie der Promotion oder Habilitation erfolgen,“

50. Die in § 303e Abs. 2 Nr. 5 SGB V-KE erfolgte Klarstellung mit dem Wortlaut „Forschung, insbesondere für Längsschnittanalysen über längere Zeiträume, Analysen von Behandlungsabläufen oder Analysen des Versorgungsgeschehens“ geht bereits in die beschriebene Richtung. Um letzte Zweifel zu beseitigen, könnte aber dennoch folgende Klarstellung in der DaTraV in § 5 Abs. 3 Nr. 2 verankert werden:

„2. der angegebene Zweck der Datenverarbeitung und Datennutzung (Nutzungszweck) dem Katalog nach § 303e Absatz 2 des Fünften Buches Sozialgesetzbuch entspricht, worunter insbesondere auch Forschungsvorhaben fallen, die im Rahmen der Erstellung wissenschaftlicher Qualifikationsschriften wie der Promotion oder Habilitation erfolgen,“

4. Erforderlichkeitsprüfung

51. Die Erforderlichkeitsprüfung hinsichtlich des Datenumfangs in § 303e Abs. 3 S. 1 SGB V ist bereits de lege lata wegen der Freiheit der Wissenschaft inhaltlich auf eine Plausibilitätsprüfung zu beschränken, zumindest soweit die nutzungsberechtigte Stelle Träger dieses Grundrechts ist.

52. De lege ferenda ist insoweit eine Klarstellung sinnvoll.

53. Die Formulierung in § 303e Abs. 3 S. 2 SGB V-E, es sei „nachvollziehbar darzulegen, dass Umfang und Struktur der beantragten Daten erforderlich“ sind, verfolgt dabei den richtigen Ansatz. Hier wird deutlich, dass die nutzungsberechtigte Stelle zwar darlegen muss, warum sie den gewählten Datenumfang für die Zweckerreichung für erforderlich hält. Aus der Formulierung „nachvollziehbar darlegen“ ergibt sich aber, dass die Datenaufbereitungsstelle (bzw. künftig gegebenenfalls das Forschungsdatenzentrum) hier nur den Datenzugang verweigern kann, wenn die angeforderten Daten zur Zweckerreichung offensichtlich ungeeignet sind oder viel zu weit greifen. Der Kabinettsentwurf behält mit § 303e Abs. 3 und 4 SGB V-KE die selbe sinnvolle Richtung bei. Inhaltlich zwingend ist dies zwar nur für Grundrechtsträger der Wissenschaftsfreiheit wie Hochschulen i.S.v. § 303e Abs. 1 Nr. 8 SGB V. Regelungstechnisch ist es jedoch zur Vermeidung einer unnötigen Komplexität in der Verfahrenspraxis zweckmäßig, die Plausibilitätsprüfung auch für andere berechnigte Stellen (z.B. Krankenkassen nach § 303e Abs. 1 Nr. 3 SGB V) einzuführen, wie es im Referentenentwurf vorgesehen ist.

5. Risikoabwägung und prozedurale Ausdifferenzierung

54. Zur Diskussion steht eine prozedurale Ausdifferenzierung des Antragsverfahrens nach § 303e SGB V, die nach der Art der nutzungsberechnigten Stelle unterschiedlich leicht und weitreichend Einsicht in den Datensatz der Versorgungsdaten gewährt. Denkbar wäre es etwa, einen „Circle of Trust“ festzulegen, bei dem drei Stufen bestehen.
55. Ausgestalten könnte man einen solchen beispielsweise, indem man eine erste Stufe von besonders vertrauenswürdigen Nutzungsberechnigten festlegt. Kriterium hierfür könnte sein, dass diese Berechnigten öffentliche Stellen sein müssen, die dem Sozialgeheimnis unterliegen und ausreichende technische Schutzvorrichtungen vorweisen können. Für diese Stellen auf der ersten Stufe würde dann das Verfahren deutlich verkürzt, die Risikoabwägung seitens der Datenaufbereitungsstelle nach § 303c Abs. 2 S. 2 SGB V i.V.m. § 5 Abs. 3 Nr. 5 DaTraV zugunsten der Annahme eines niedrigen Risikos weitgehend vorweggenommen. Die Stellen könnten Zugriff sowohl auf Ergebnismengen als auch auf Einzeldatensätze erhalten.
56. Auf der zweiten Stufe würden nach diesem Modell Stellen stehen, die zwar nicht dem Sozialgeheimnis unterliegen, die aber ein ausreichendes Datenschutzkonzept vorweisen können und möglicherweise eine Selbstverpflichtung zur Achtung hoher Datenschutzstandards eingegangen sind. Hierzu könnten etwa Wissenschaftler von Hochschulen und sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung i.S.v. § 303e Abs. 1 Nr. 8 SGB V zählen, soweit sie die genannten Bedingungen erfüllen. Auf dieser zweiten Stufe könnte dann das Verfahren wie bisher verlaufen. Es könnte also ebenfalls neben Ergebnismengen die Arbeit mit Einzeldatensätzen ermöglicht werden, soweit dies erforderlich ist. Jedoch müsste bei der Bereitstellung der Ergebnisse am Ende stets eine ausführliche Abwägung des Reidentifikationsrisikos seitens der Datenaufbereitungsstelle (wie bei § 303c Abs. 2 S. 2 SGB V i.V.m. § 5 Abs. 3 Nr. 5 DaTraV bereits jetzt vorgegeben) vorgenommen werden.
57. Auf der dritten Stufe würden dann Stellen stehen, die nicht dem Sozialgeheimnis unterliegen und die die Voraussetzungen der zweiten Stufe nicht erfüllen. Hier wäre dann lediglich der Zugang zu tatsächlich anonymen Ergebnismengen möglich.

58. Normsystematisch sinnvoll könnte eine solche Regelung an § 303e SGB V gekoppelt werden. In der aktuellen Struktur wäre dazu eine Neufassung des § 303e Abs. 3 SGB V in der Systematik des Referentenentwurfs in einem neuen Absatz zwischen § 303e Abs. 3 und 4 SGB V-E notwendig. Alternativ könnte dies auch auf Verordnungsebene in der DaTraV geregelt bzw. im Vergleich zum Kabinettsentwurf weiter ausdifferenziert werden.

6. Zur Verwendung der Begriffe „anonymisiert“ und „pseudonymisiert“

59. Bei einer Neuregelung könnte der Gesetzgeber klarstellen, was unter „anonymisiert“ zu verstehen ist. Sinnvoll wäre dabei eine Verweisung auf den Anonymitätsbegriff der DS-GVO, um insoweit kein abweichendes Regelungsregime zu schaffen. Zweckmäßig wäre daher eine Formulierung wie *„derart anonymisierte Angaben im Sinne des Erwägungsgrunds 26 der Datenschutzgrundverordnung 2016/679“*. Gegebenenfalls wäre eine Präzisierung des Anonymitätsbegriffs denkbar, die unmittelbar Bezug nimmt auf S. 5 des Erwägungsgrunds. Diese könnte wie folgt formuliert werden:

„derart anonymisierte Angaben, d.h. personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann im Sinne des Erwägungsgrunds 26 der Datenschutz-Grundverordnung 2016/679“.

Eine absolute Anonymität zu fordern, könnte zwar mit einer Formulierung wie *„derart anonymisierte Angaben, dass eine Identifizierung von Versicherten für jedermann unmöglich ist“*, verfolgt werden. Damit würde der deutsche Gesetzgeber jedoch Regelungen außerhalb des Anwendungsbereichs der DS-GVO parallel zu dieser treffen, was zumindest rechtspolitisch sehr fraglich ist.

60. Ob Daten aggregiert sind oder nicht hat dabei unter Zugrundelegung des aufgezeigten Verständnisses nach der DS-GVO zunächst keine direkte Auswirkung auf die Frage, ob diese anonym oder personenbezogen sind. Aggregierte Daten als Aussagen über Personengruppen weisen in der Regel keinen Personenbezug auf. Etwas anderes kann hier nur gelten, wenn die Aussage über eine Gruppe auf einzelne Personen „durchschlägt“. Soweit keine personenbezogenen Daten vorliegen, greift aber bei aggregierten Daten auch nicht die oben beschriebene Vorfeldwirkung (s.o. C. I. 2.) aus dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.
61. Soweit im Zuge der §§ 303a ff. SGB V ein Verfahren durchgeführt wird, das nicht rückführbare Pseudonyme erzeugt, die allein der Datenzusammenführung dienen und auch mit Zusatzwissen nicht zur Herstellung des Personenbezugs genutzt werden können, kann begrifflich weiter von einem Pseudonymisierungsverfahren i.S.v. Art. 4 Nr. 5 DS-GVO gesprochen werden. Zwar kann bei einem strengen Wortlautverständnis der Norm vertreten werden, dass keine Pseudonymisierung vorliegt, soweit bei einem Verfahren nicht durch gesondert aufbewahrtes Zusatzwissen vom Pseudonym auf die Identität der Person geschlossen werden kann. Doch Sinn und Zweck der Pseudonymisierung als Sicherungsmaßnahme rechtfertigen bei lebensnaher Betrachtung ein weiteres Verständnis (siehe hierzu C. III. 1. g)). Um letzten begrifflichen Zweifeln vorzubeugen, kann alternativ der Begriff der *„Verschlüsselung“* aufgegriffen werden, der nach Art. 32 Abs. 1 lit. a DS-GVO ebenfalls eine Sicherungsmaßnahme darstellt, nicht

von der DS-GVO definiert wird und Überschneidungen zur Pseudonymisierung aufweist. Eine präzise Formulierung scheint wie folgt möglich: „*die Daten sind derart zu verschlüsseln, dass ein Rückschluss auf die Identität durch eine direkte Umkehrung des Verschlüsselungsprozesses nach dem jeweiligen Stand der Technik ausgeschlossen ist*“. Ob die Daten nach dem Verfahren im Einzelfall und aus Sicht des jeweiligen Verantwortlichen als anonym zu betrachten sind, richtet sich nach den allgemeinen Kriterien (siehe hierzu B. I. 2. und B. III. 1.).

7. Normierung eines Verbots der Reidentifikation

62. Verbesserungspotenzial besteht ferner hinsichtlich der Handhabung des Reidentifikationsverbots. Dieses sollte nicht nur als Aufgabe der Datenaufbereitungsstelle in § 303c Abs. 2 S. 2 SGB V definiert werden, sondern auch ausdrücklich an die nutzungsberechtigten Stellen gerichtet sein.
63. § 303e Abs. 5 S. 2 SGB V-E und § 303e Abs. 5 SGB V-KE enthalten bereits ein solches Verbot, das in dieser oder vergleichbarer Form übernommen werden sollte.

8. Sanktionen für Datenschutzrechtsverstöße

64. In den Entwürfen sind als weitere Sicherungsmaßnahmen eine Sperre nutzungsberechtigter Stellen für (bis zu) zwei Jahre (§ 303e Abs. 6 S. 2 SGB V-E bzw. § 303e Abs. 6 S. 2 SGB V-KE) und ein Straftatbestand (§ 307c SGB V-E bzw. § 307b Abs. 1 SGB V-KE) vorgesehen.

a) Sperren von nutzungsberechtigten Stellen nach § 303e Abs. 6 S. 2 SGB V-E

65. In Bezug auf § 303e Abs. 6 S. 2 SGB V-E sollte möglicherweise abgewogen werden, ob eine Sperrung von stets zwei Jahren nicht zu unflexibel ist. Es könnte ein gestufter Sperrzeitraum nach Schwere des Verstoßes festgelegt werden. § 303e Abs. 6 S. 2 SGB V-KE ermöglicht hier angemessenere Sperren von bis zu zwei Jahren. Im Übrigen ist eine derartige „milde“ Sanktion sehr sinnvoll.

b) Straftatbestand für die vorsätzliche Reidentifikation von Versicherten

66. Die Art des sanktionsbewährten Reidentifikationsverbots, wie es in § 307c SGB V-E oder § 307b Abs. 1 SGB V-KE als Straftatbestand vorgesehen ist, stellt eine sinnvolle Möglichkeit dar, um die Verarbeitung der Versorgungsdaten datenschutzrechtskonform auszugestalten. Entscheidend ist dabei, dass der durch die Sanktionsdrohungen abgesicherte hohe Sicherheitsstandard mit in die Risikoabwägung einbezogen werden kann. So könnten Daten mit einer sehr geringen Wahrscheinlichkeit der Reidentifikation eher bereitgestellt werden, zumal die Verantwortlichen ohnehin zumeist kein Interesse an einer Reidentifikation haben dürften und sich – soweit dies umgesetzt wird – künftig zusätzlich einer Strafandrohung ausgesetzt sehen.

c) Protokollierung der Datenzugriffe

67. In der praktischen Umsetzung ist es ferner wichtig, dass die Zugriffe auf die Versorgungsdaten hinreichend protokolliert werden, um ex post Verstöße feststellen und sanktionieren zu können.
68. Zur Absicherung könnte insoweit auch eine Regelung zur Protokollierung der Datenzugriffe in die DaTraV aufgenommen werden, anstatt dies der praktischen Umsetzung des Regelwerks zu überlassen.

9. Gesetzgeberischer Klarstellungs- und Anpassungsbedarf im SGB X

a) § 76 Abs. 2 SGB X

69. Art. 76 Abs. 1 SGB X verlängert die ärztliche Schweigepflicht dahingehend, dass Sozialgeheimnisträger Daten, die ursprünglich unter dem besonderen Schutz der ärztlichen Schweigepflicht standen, nur dann an Dritte übermitteln dürfen, wenn auch der Berufsgeheimnisträger selbst sie weitergeben hätte dürfen. Da die betroffene Person über den Schutz des § 203 StGB uneingeschränkt disponieren kann, insbesondere einen Arzt auch von der Schweigepflicht entbinden kann, ist schon nach dem Wortlaut des § 75 SGB X bei entsprechender Schweigepflichtentbindung durch die betroffene Person (Patient) eine Übermittlung stets zulässig. Ist der Empfänger der Daten selbst an eine berufliche Schweigepflicht gebunden, so wird das Berufsgeheimnis hinreichend geschützt, so dass der besondere Schutz des Art. 76 Abs. 1 SGB X nicht erforderlich ist. Im Übrigen kann im Einzelfall das Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Person überwiegen, insbesondere wenn aufgrund der Beschaffenheit der Daten eine Identifizierung unwahrscheinlich ist.

70. Es empfiehlt sich daher eine Ergänzung in § 76 Abs. 2 SGB X wie folgt:

„4. im Rahmen des Art. 75 SGB X soweit,

a) die betroffene Person eingewilligt hat,

b) die Stelle, an die die Daten übermittelt werden, selbst einer umfassenden beruflichen Schweigepflicht oder dem Sozialgeheimnis unterliegt, oder

c) das Interesse an der Datenverarbeitung das Geheimhaltungsinteresse der betroffenen Person auch unter Berücksichtigung der besonderen Schutzbedürftigkeit der übermittelten Daten erheblich überwiegt, was insbesondere der Fall sein kann, wenn eine Identifizierung der betroffenen Person aufgrund der Beschaffenheit der Daten unwahrscheinlich ist.“

b) § 78 SGB X

71. Es empfiehlt sich eine gesetzgeberische Klarstellung durch Aufnahme einer Ausnahme in § 78 SGB X. Normsystematisch würde sich insoweit die Ergänzung um einen Absatz 5 wie folgt anbieten:

„Die Absätze 1 bis 4 finden keine Anwendung, soweit die Daten auf Veranlassung der betroffenen Person übermittelt werden und diese anstelle der Übermittlung an den Empfänger auch die Herausgabe einer Datenkopie an sich selbst hätte verlangen können.“

Regensburg, den 4. September 2019

Prof. Dr. Jürgen Kühling, LL.M.