Prof. Dr. Matthias Bäcker, LL.M.
Trützschlerstr. 11
68199 Mannheim

Mannheim, den 2. Mai 2022

Sozialgericht Frankfurt a.M.
Gutleutstr. 136
60327 Frankfurt a.M.

Antrag auf Erlass einer einstweiligen Anordnung

des Herrn ...,
...
– Antragsteller –

g e g e n

AOK Hessen,
Basler Str. 2, 61352 Bad Homburg
– Antragsgegnerin –

Namens und in beigefügter Vollmacht des Antragstellers **(Anlage 1)** beantrage ich,

> der Antragsgegnerin im Wege einer einstweiligen Anordnung die Übermittlung der den Antragsteller betreffenden in § 303b Abs. 1 SGB V und § 3 Abs. 1 DaTraV bezeichneten Daten für die Berichtsjahre 2019 und 2021 an den Spitzenverband Bund der Krankenkassen vorläufig zu untersagen,

Ich rege an, zur Klärung unionsrechtlicher Zweifelsfragen bereits im Verfahren zum Erlass einer einstweiligen Anordnung ein beschleunigtes Vorabentscheidungsverfahren bei dem Gerichtshof der Europäischen Union durchzuführen (Art. 267 AEUV, Art. 23a EuGH-Satzung, Art. 105 f. EuGH-Verfahrensordnung).

Hierzu rege ich an, dem Gerichtshof die folgenden Fragen vorzulegen:

1. Sind Art. 2 Abs. 1 und Abs. 2 lit. a der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden: DSGVO) so auszulegen, dass eine Übermittlung pseudonymisierter Gesundheitsdaten durch eine Krankenkasse an eine Datensammelstelle mit dem Ziel, die Daten im Rahmen eines Datentransparenzverfahrens für Zwecke der medizinischen Forschung, der Planung, Analyse und Evaluation der Gesundheitsversorgung im System der gesetzlichen Krankenversicherung sowie der Gesundheitsberichterstattung verfügbar zu machen, wie sie in § 303b Abs. 1 Satz 1 SGB V vorgesehen ist, in den sachlichen Anwendungsbereich der DSGVO fällt, obwohl die Festlegung der Gesundheitspolitik, die Organisation des Gesundheitswesens und die medizinische Versorgung gemäß Art. 168 Abs. 7 Satz 1 und 2 AEUV in der Verantwortung der Mitgliedstaaten liegen?

2. Falls Frage 1 zu bejahen ist: Stehen die aus Art. 5 Abs. 1 lit. f DSGVO im Lichte von Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: GRCh) folgenden Anforderungen an die Gewährleistung der Vertraulichkeit und Integrität personenbezogener

Daten mitgliedstaatlichen Regelungen zur Zusammenführung, Bevorratung und Nutzung von Gesundheitsdaten gesetzlich krankenversicherter Personen wie §§ 303a ff. SGB V entgegen, wenn

a) zunächst die Krankenkassen die Daten für einen Berichtszeitraum von einem Jahr an eine zentrale Datensammelstelle zu übermitteln haben, die jedes Datum eindeutig einer bestimmten, durch ein kassenübergreifendes Lieferpseudonym gekennzeichneten Person zuordnen kann,

b) die Daten nach einer Weiterübermittlung durch die Datensammelstelle für bis zu dreißig Jahre bei einem zentralen Forschungsdatenzentrum unter einem dauerhaften Pseudonym je versicherter Person gespeichert werden, ohne dass sich in den Rechtsgrundlagen der Datenspeicherung nähere Vorgaben zur technischen und organisatorischen Sicherung der Daten fänden, die über den allgemeinen Schutzstandard von Art. 24, Art. 25 und Art. 32 DSGVO hinausgingen,

c) das Forschungsdatenzentrum die Daten bestimmten nutzungsberechtigten Stellen gegebenenfalls auch in Form pseudonymisierter Einzeldatensätze zur Verfügung stellen darf, wobei es lediglich zu prüfen hat, ob ein Nutzungsberechtigter in seinem Zugangsantrag „nachvollziehbar dargelegt“ hat, dass diese Nutzung für einen gesetzlich zulässigen Nutzungszweck erforderlich ist?

3. Falls Frage 1 zu bejahen ist: Ist das Widerspruchsrecht des Art. 21 Abs. 1 DSGVO im Rahmen eines gestuften Verfahrens der Datensammlung, Datenspeicherung und Datenbereitstellung, wie es in §§ 303a ff. SGB V angelegt wird, bereits auf die erste Stufe der Datenübermittlung von der Krankenkasse an die Datensammelstelle anzuwenden, wenn die Krankenkasse zur Datenübermittlung gesetzlich verpflichtet ist, die Nutzung der bei dem Forschungsdatenzentrum gespeicherten Daten hingegen von einer Ermessensentscheidung der nutzungsberechtigten Stellen abhängt?

4. Falls Frage 1 zu bejahen ist: Ist das Widerspruchsrecht des Art. 21 Abs. 6 DSGVO im Rahmen eines gestuften Verfahrens der Datensammlung, Datenspeicherung und Datenbereitstellung, wie es in §§ 303a ff. SGB V angelegt wird, bereits auf die erste Stufe der Datenübermittlung von der Krankenkasse an die Datensammelstelle anzuwenden, wenn die

Krankenkasse und die Datensammelstelle mit den übermittelten Daten selbst keine Forschungszwecke verfolgen, die Übermittlung aber einer Bereitstellung der Daten zu Forschungszwecken dient?

5. Falls Frage 3 und/oder Frage 4 zu bejahen sind:

   a) Ist Art. 21 Abs. 1 und/oder Abs. 6 DSGVO so auszulegen, dass eine betroffene Person die sie betreffende Verarbeitung von Gesundheitsdaten zu Zwecken der Gesundheitsversorgung, der Gesundheitsberichterstattung und/oder der Forschung im Rahmen eines Datentransparenzverfahrens, wie es §§ 303a ff. SGB V vorsehen, durch einen Widerspruch generell, also unabhängig von einer Erforderlichkeitsprüfung und Interessenabwägung hinsichtlich einzelner Auswertungsprojekte, unterbinden kann?

   b) Falls kein generelles Widerspruchsrecht besteht: Ist der mitgliedstaatliche Gesetzgeber aufgrund von Art. 21 Abs. 1 und/oder Abs. 6 DSGVO verpflichtet, ein auf die einzelnen Datenbereitstellungen bezogenes Widerspruchsverfahren einzurichten, damit die betroffene Person von ihrem Widerspruchsrecht im Einzelfall tatsächlich wirksam Gebrauch machen kann?

6. Falls Frage 3 und/oder Frage 4 zu verneinen sind: Sind Art. 6 Abs. 3 Satz 3 und 4 und Art. 9 Abs. 2 lit. h, i und j DSGVO im Lichte von Art. 7 und 8 GRCh so auszulegen, dass ein mitgliedstaatlicher Gesetzgeber, wenn er ein Datentransparenzverfahren wie in §§ 303a ff. SGB V vorgesehen schafft, den betroffenen Versicherten generell oder für den Fall einer besonderen individuellen Betroffenheit das Recht einräumen muss, der Verarbeitung sie betreffender personenbezogener Daten im Rahmen des Datentransparenzverfahrens generell oder hinsichtlich bestimmter Datenbereitstellungen zu widersprechen?

7. Falls Frage 3 zu bejahen ist: Ist Art. 18 Abs. 2 DSGVO so auszulegen, dass ein die Verarbeitung von Daten, deren Verarbeitung nach Art. 18 Abs. 1 lit. d DSGVO wegen eines Widerspruchs der betroffenen Person vorläufig eingeschränkt ist, ausnahmsweise rechtfertigendes wichtiges öffentliches Interesse nur dann besteht, wenn die Verarbeitung eilbedürftig ist, sodass nicht abgewartet werden kann, bis feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen?

8. Falls Frage 2 und/oder Frage 6 zu bejahen sind: Ist Art. 5 Abs. 1 lit. a DSGVO oder eine andere Vorschrift der Verordnung im Lichte von Art. 8 und Art. 47 GRCh so auszulegen, dass eine betroffene Person von einem für eine bevorstehende Datenverarbeitung Verantwortlichen verlangen kann, eine bevorstehende rechtswidrige Datenverarbeitung zu unterlassen, obwohl die DSGVO keine ausdrückliche Regelung über einen vorbeugenden Unterlassungsanspruch der betroffenen Person enthält?

Gliederung

A. Vorbemerkung: Verfahrensgegenstand und aufgeworfene Rechtsfragen im Überblick

Der Antragsteller wendet sich dagegen, dass die Antragsgegnerin im Rahmen des sogenannten Datentransparenzverfahrens ihn betreffende Daten an den Spitzenverband Bund der Krankenkassen übermittelt. Gegenstand dieses Verfahrens ist die zentrale Zusammenführung zahlreicher Gesundheitsdaten über alle gesetzlich krankenversicherten Personen in Deutschland. Die zusammengeführten Daten stehen für Auswertungen zu den Zwecken der medizinischen Forschung, der Planung, Analyse und Evaluation der Gesundheitsversorgung im System der gesetzlichen Krankenversicherung sowie der Gesundheitsberichterstattung bereit.

Der vorliegende Antrag zielt nicht darauf ab, das Datentransparenzverfahren ersatzlos zu beseitigen. Der Antragsteller stellt nicht in Frage, dass dieses Verfahren legitimen und gewichtigen Zielen dient. Die gesetzliche Ausgestaltung des Datentransparenzverfahrens weist jedoch gravierende Mängel auf. Wegen dieser Mängel verletzen die Rechtsgrundlagen des Verfahrens in ihrer gegenwärtigen Form sowohl Verfassungsrecht als auch Unionsrecht und sind deshalb unanwendbar. Darüber hinaus ist im Rahmen des Datentransparenzverfahrens der besonderen Vulnerabilität des Antragstellers Rechnung zu tragen, der an einer seltenen schweren Krankheit leidet.

Die Rechtsgrundlagen des Datentransparenzverfahrens sind mangelhaft, weil sie die Sicherheit der verarbeiteten Gesundheitsdaten gegen unbefugte Zugriffe nur unzureichend gewährleisten. Da diese Daten nach ihrer Art und ihrem Umfang außerordentlich sensibel sind, ist ein besonders hoher Sicherheitsstandard unabdingbar. Die gesetzlichen Regelungen begründen hingegen erhebliche Sicherheitsrisiken, indem sie zum einen für die Zusammenführung und Bevorratung der Daten eine riskante Zentralisierung vorschreiben oder zumindest ermöglichen, zum anderen keine hinreichend strengen Anforderungen an die Bereitstellung der Daten für konkrete Auswertungsprojekte errichten.

Zudem steht dem Antragsteller aufgrund seiner besonderen Situation ein Widerspruchsrecht gegen die Verarbeitung der ihn betreffenden Gesundheitsdaten im Datentransparenzverfahren zu. Von diesem Recht hat er gegenüber der Antragsgegnerin vorprozessual erfolglos Gebrauch gemacht. Dem Antragsteller ist nicht zumutbar, die Übermittlung und Weiterverarbeitung der ihn betreffenden Gesundheitsdaten und die damit

verbundenen schwerwiegenden Risiken gegen seinen Willen auch nur vorläufig hinzunehmen.

Der Antragsteller regt an, vor der Entscheidung über seinen Antrag die im vorliegenden Verfahren aufgeworfenen Grundsatzfragen des europäischen Datenschutzrechts durch ein (beschleunigtes) Vorabentscheidungsverfahren vor dem Gerichtshof der Europäischen Union verbindlich klären zu lassen.

B. Sachverhalt

I. Das Datentransparenzverfahren nach §§ 303a ff. SGB V

Die Regelungen über das Datentransparenzverfahren in §§ 303a ff. SGB V verfolgen das Ziel, Gesundheitsdaten der in der gesetzlichen Krankenversicherung pflichtversicherten Personen für Zwecke der medizinischen Forschung, der Planung, Analyse und Evaluation der Gesundheitsversorgung im System der gesetzlichen Krankenversicherung sowie der Gesundheitsberichterstattung verfügbar zu machen. Dazu wurden diese Regelungen durch das Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz) vom 9. Dezember 2019 (BGBl I S. 2562) grundlegend überarbeitet. Die gesetzlichen Regelungen werden durch die auf § 303a Abs. 1 Satz 2 SGB V gestützte Verordnung zur Umsetzung der Vorschriften über die Datentransparenz (Datentransparenzverordnung – DaTraV) vom 19. Juni 2020 ergänzt.

Die zur Verfügung zu stellenden Datenkategorien werden in § 303b Abs. 1 SGB V und § 3 DaTraV im Einzelnen bezeichnet. Hierzu zählen zum einen bestimmte Basisangaben zu der betroffenen Person (Geburtsjahr, Geschlecht, Postleitzahl des Wohnorts, Vitalstatus und ggfs. Sterbedatum). Zum anderen sind Angaben zum Versicherungsverhältnis sowie Kosten- und Leistungsdaten verschiedener Leistungserbringer bereitzustellen. Diese Daten schließen etwa ärztliche Diagnosen, durchgeführte Behandlungen, verordnete Arzneimittel oder Informationen zur Inanspruchnahme von Krankengeld ein.

Die Daten werden zum Schutz der betroffenen Personen in einem mehrstufigen Verfahren bereitgestellt. An den Verarbeitungsschritten sind unterschiedliche Stellen beteiligt.

Zunächst übermitteln die Krankenkassen die Daten nach § 303b Abs. 1 SGB V an den Spitzenverband Bund der Krankenkassen als Datensammelstelle. Sie verbinden die Daten mit einem jährlich wechselnden (§ 5 Abs. 2 Satz 2 DaTraV) Lieferpseudonym, das für das jeweilige Berichtsjahr eine kassenübergreifende eindeutige Identifizierung der betroffenen Person ermöglicht. Der Spitzenverband führt gemäß § 303b Abs. 2 SGB V i.V.m. § 4 DaTraV die Daten zusammen, prüft sie auf Vollständigkeit, Plausibilität und Konsistenz und klärt gegebenenfalls Auffälligkeiten mit der zuliefernden Krankenkasse.

Anschließend übermittelt der Spitzenverband gemäß § 303b Abs. 3 SGB V zum einen an das Bundesinstitut für Arzneimittel und Medizinprodukte als

Forschungsdatenzentrum (§ 2 Abs. 2 DaTraV) die angelieferten Daten, jedoch nicht das Lieferpseudonym. Stattdessen kennzeichnet er jeden Einzeldatensatz mit einer individuellen Arbeitsnummer, die gemäß § 4 Abs. 4 DaTraV keinen Rückschluss auf das Lieferpseudonym zulassen darf. Zudem sind die Angaben zu den Leistungserbringern vor der Übermittlung an das Bundesinstitut für Arzneimittel und Medizinprodukte zu pseudonymisieren. Zum anderen übermittelt der Spitzenverband an das Robert Koch-Institut als Vertrauensstelle (§ 2 Abs. 1 DaTraV) eine Liste mit den Lieferpseudonymen und den jeweils zugehörigen Arbeitsnummern.

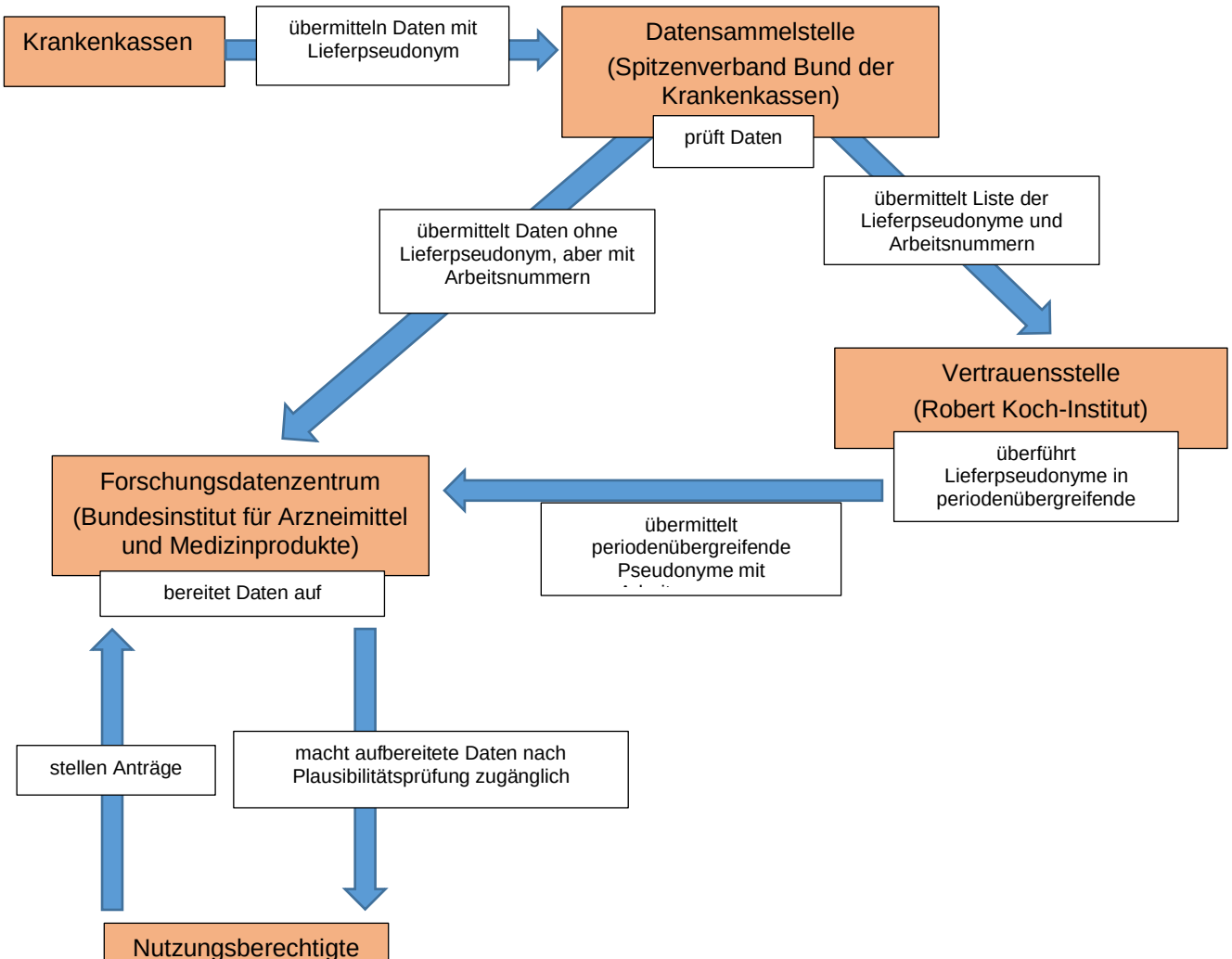
Das Robert Koch-Institut überführt gemäß § 303c SGB V i.V.m. § 6 DaTraV die ihm übermittelten Lieferpseudonyme in periodenübergreifende Pseudonyme. Die periodenübergreifenden Pseudonyme ermöglichen es, die Daten dauerhaft einer bestimmten versicherten Person zuzuordnen, um auf dieser Grundlage beispielsweise medizinische Langzeitstudien oder Längsschnittanalysen durchführen zu können. Die Pseudonymisierung ist so zu gestalten, dass einerseits für alle Lieferpseudonyme einer versicherten Person immer dasselbe periodenübergreifende Pseudonym erstellt wird, andererseits aus dem periodenübergreifenden Pseudonym nicht auf das Lieferpseudonym oder die Identität der versicherten Person geschlossen werden kann. Sodann übermittelt das Robert Koch-Institut dem Bundesinstitut für Arzneimittel und Medizinprodukte eine Liste der periodenübergreifenden Pseudonyme und der jeweils zugehörigen Arbeitsnummern. Anschließend hat es Lieferpseudonyme, Arbeitsnummern und periodenübergreifende Pseudonyme zu löschen.

Die weitere Verarbeitung der pseudonymisierten Gesundheitsdaten liegt bei dem Forschungsdatenzentrum, also dem Bundesinstitut für Arzneimittel und Medizinprodukte. Dieses darf die versichertenbezogenen Einzeldatensätze nach § 303d Abs. 3 SGB V maximal 30 Jahre lang aufbewahren. Die Aufgaben des Forschungsdatenzentrums sind im Einzelnen in § 303d Abs. 1 SGB V aufgezählt. Für das vorliegende Verfahren primär bedeutsam ist die in § 303e SGB V i.V.m. §§ 7 ff. DaTraV näher geregelte Bereitstellung der Daten. § 303e Abs. 1 SGB V zählt die Nutzungsberechtigten, § 303e Abs. 2 SGB V die zulässigen Nutzungszwecke auf. Auf einen hinreichend substantiierten Antrag eines Nutzungsberechtigten (§ 7 DaTraV) übermittelt das Forschungsdatenzentrum nach einer Antragsprüfung (§ 8 DaTraV) die entsprechend den Anforderungen des Nutzungsberechtigten ausgewählten Daten gemäß § 303e Abs. 3 Satz 3 und 4 SGB V i.V.m. § 10 Abs. 1 Nr. 1 und 2 DaTraV grundsätzlich in anonymisierter und aggregierter Form. Daneben ist insbesondere – nicht notwendigerweise ausschließlich – für

Forschungszwecke gemäß § 303e Abs. 4 Satz 1 SGB V i.V.m. § 10 Abs. 1 Nr. 3, Abs. 2 DaTraV auch eine Bereitstellung pseudonymisierter Einzeldatensätze zulässig. Hierbei bestehen spezifische Anforderungen an Verfahren, Organisation und Technik der Datenverarbeitung (keine Sichtbarmachung der Pseudonyme, Verarbeitung in einer gesicherten physischen oder virtuellen Umgebung unter Kontrolle des Forschungsdatenzentrums, Bereitstellung nur an besonders zur Geheimhaltung verpflichtete Personen, Beschränkung der Datenverarbeitung auf das erforderliche Maß). Vor einer Bereitstellung hat das Forschungsdatenzentrum gemäß § 303d Abs. 1 Nr. 5 SGB V i.V.m. § 10 Abs. 3 DaTraV das spezifische Risiko einer Reidentifikation der betroffenen Personen durch den Empfänger zu bewerten und dieses Risiko durch geeignete Maßnahmen zu minimieren.

Die Weiterverarbeitung der bereitgestellten Daten durch die Nutzungsberechtigten ist schließlich in § 303e Abs. 5 SGB geregelt. Insbesondere unterliegen die Daten einer grundsätzlich strengen Zweckbindung und dürfen die Nutzungsberechtigten keinen Bezug zu Personen, Leistungserbringern oder Leistungsträgern herstellen.

Die für das vorliegende Verfahren bedeutsamen Verfahrensschritte und beteiligten Stellen lassen sich wie folgt graphisch darstellen:



Das Datentransparenzverfahren soll in diesem Jahr anlaufen. Gemäß § 12 Abs. 3 Satz 1 Nr. 1 DaTraV haben die Krankenkassen spätestens zum 1. Oktober 2022 die Daten für das Berichtsjahr 2021 und, soweit vorhanden, für das Berichtsjahr 2019 an die Datensammelstelle zu übermitteln. Nach Auskunft des Spitzenverbands Bund der Krankenkassen sollen die Krankenkassen mit den Datenübermittlungen an die Datensammelstelle ab dem 1. August 2022 beginnen.

II. Situation des Antragstellers

Der am ... geborene Antragsteller ist bei der Antragsgegnerin in der gesetzlichen Krankenversicherung pflichtversichert (Krankenversicherungsnr. ...).

Der Antragsteller leidet an einer angeborenen schweren Blutgerinnungsstörung (Schwere Hämophilie A, ICD-10 Code D66, umgangssprachlich mitunter als „Bluterkrankheit“ bezeichnet). Hierbei handelt es sich um eine seltene Krankheit. Sie tritt bei etwa einem von 5.000 männlichen Neugeborenen auf, wobei etwa die Hälfte der Erkrankten an der schweren Form leidet,

> vgl. https://www.dhg.de/blutungskrankheiten/haemophilie.html (letzter Abruf am 2. Mai 2022).

Die Blutgerinnungsstörung des Antragstellers muss durch Dauermedikation mit einem Blutgerinnungsmittel behandelt werden, das der Antragsteller aufgrund ärztlicher Verordnung von einer nahe seiner Wohnung gelegenen Apotheke bezieht. Aufgrund seiner Erkrankung gilt der Antragsteller als schwerwiegend chronisch krank im Sinne der sogenannten Chroniker-Richtlinie des Gemeinsamen Bundesausschusses. Zudem liegen bei ihm eine Schwerbehinderung mit einem Grad der Behinderung von 70 sowie eine Gehbehinderung vor, die auf einer hämophiliebedingten Polyarthrose der Ellbogen-, Knie- und Sprunggelenke beruht.

Darüber hinaus leidet der Antragsteller an einer rezidivierenden depressiven Störung (ICD-10 Code F33.1). Außerdem wurde bei ihm eine kombinierte Persönlichkeitsstörung diagnostiziert (ICD-10 Code F61). Wegen seiner psychischen Erkrankung befand er sich von ... bis ... in ambulanter und von ... bis ... in therapeutischer Behandlung. Der Antragsteller hat im ... eine neue Therapie aufgenommen.

III. Verfahrensgeschichte

Mit Schreiben vom 1. März 2022 **(Anlage 2)** forderte der Antragsteller die Antragsgegnerin auf, von einer Übermittlung ihn betreffender personenbezogener Daten an die Datensammelstelle abzusehen. Zur Begründung berief sich der Antragsteller zum einen auf verschiedene Sicherheitsmängel des Datentransparenzverfahrens, die durch die gesetzliche und verordnungsrechtliche Gestaltung dieses Verfahrens angelegt würden. Zum anderen widersprach der Antragsteller der Datenübermittlung unter Berufung auf Art. 21 Abs. 1 und 6 DSGVO und unter Verweis auf seine besondere Situation.

Die Antragsgegnerin erwiderte hierauf mit Schreiben vom 8. März 2022 **(Anlage 3)**. Darin führte sie aus, die Datenverarbeitungen im Datentransparenzverfahren beruhten auf einer hinreichenden Rechtsgrundlage und ein Widerspruchsrecht bestehe generell nicht.

Der Antragsteller legte gegen die aus dem Schreiben vom 8. März 2022 hervorgehende Ablehnung seines Unterlassungsbegehrens mit Schreiben vom 15. März 2022 **(Anlage 4)** Widerspruch (§ 83 SGG) ein. Zur Begründung bezog er sich auf sein Schreiben vom 1. März 2022. Zudem forderte er die Antragsgegnerin auf, bis zu einer bestands- bzw. rechtskräftigen Entscheidung über den von ihm nach Art. 21 Abs. 1 DSGVO erklärten (datenschutzrechtlichen) Widerspruch die Verarbeitung der ihn betreffenden Daten im Datentransparenzverfahren gemäß Art. 18 Abs. 1 lit. d DSGVO einzuschränken, also die Daten einstweilen nicht an die Datensammelstelle zu übermitteln. Der Antragsteller ersuchte die Antragsgegnerin, ihm die Einschränkung der Verarbeitung sowie die aufschiebende Wirkung seines (prozessrechtlichen) Widerspruchs zu bestätigen.

Die Antragsgegnerin antwortete mit Schreiben vom 12. April 2022 **(Anlage 5)**, bei ihrem Schreiben vom 8. März 2022 habe es sich nicht um einen Verwaltungsakt gehandelt. Die Datenübermittlung an die Datensammelstelle sei nach Art. 18 Abs. 2 DSGVO zulässig.

Der Antragsteller forderte die Antragsgegnerin mit Schreiben vom 19. April 2022 **(Anlage 6)** auf, den am 15. März 2022 eingelegten (prozessrechtlichen) Widerspruch zu bearbeiten.

C. Zulässigkeit des Antrags

Der Antrag ist als Antrag auf Erlass einer Sicherungsanordnung nach § 86b Abs. 2 Satz 1 SGG statthaft. Ein vorrangig zu erhebender Eilantrag nach § 86b Abs. 1 SGG ist zumindest teilweise nicht statthaft, im Übrigen jedenfalls nicht zielführend.

Der Antragsteller begehrt von der Antragsgegnerin das vorläufige Unterlassen einer Datenübermittlung. Dieses Begehren stützt er auf zwei unterschiedliche Rechtsgründe, die verfahrensrechtlich unterschiedlich zu behandeln sind.

Erstens beruft sich der Antragsteller darauf, dass die Rechtsgrundlagen der Datenübermittlung gegen höherrangiges Recht verstoßen und darum unanwendbar sind. Insoweit verlangt der Antragsteller von der Antragsgegnerin das schlichte Unterlassen eines rechtswidrigen Realakts. Ein Verwaltungsakt, gegen den im Verfahren nach § 86b Abs. 1 SGG vorgegangen werden könnte, steht mit Blick auf diesen Rechtsgrund des Begehrens des Antragstellers nicht in Rede.

Zweitens stützt sich der Antragsteller auf sein Widerspruchsrecht aus Art. 21 Abs. 1 und Abs. 6 DSGVO, also ein datenschutzrechtliches Betroffenenrecht. Hiermit verknüpft ist sein weiteres Recht auf Einschränkung der Verarbeitung aus Art. 18 Abs. 1 lit. d DSGVO. Nach einer auch in der Rechtsprechung verbreiteten Auffassung ist über das Bestehen eines geltend gemachten Betroffenenrechts durch Verwaltungsakt zu entscheiden. Hieraus werden prozessual unterschiedliche Folgerungen gezogen. Im Ergebnis scheidet allerdings nach allen Auffassungen ein Verfahren nach § 86b Abs. 1 SGG hier aus.

Teilweise wird angenommen, die betroffene Person, die ein Betroffenenrecht erfolglos geltend gemacht habe, müsse ihr Begehren mit einem Verpflichtungswiderspruch und einer Verpflichtungsklage weiterverfolgen,

> so zum Auskunftsrecht des Art. 15 DSGVO BVerwG, Urteil vom 16. September 2020 – 6 C 10.19 –, juris, Rn. 12.

Auf der Grundlage dieser Auffassung kommt ein Antrag nach § 86b Abs. 1 SGG hier von vornherein nicht in Betracht. In der Verpflichtungssituation richtet sich der einstweilige Rechtsschutz allein nach § 86b Abs. 2 SGG.

Nach anderer Auffassung soll in der Weigerung, ein Betroffenenrecht zu erfüllen, ein belastender Verwaltungsakt liegen, gegen den ein Anfechtungswiderspruch und eine Anfechtungsklage statthaft seien,

> so zum Anspruch auf Datenlöschung aus Art. 17 DSGVO BSG, Urteil vom 18. Dezember 2018 – B 1 KR 31/17 R –, BeckRS 2018, 33790, Rn. 11; LSG Nordrhein-Westfalen, Urteil vom 24. Juli 2020 – L 21 AS 196/19 –, BeckRS 2020, 40729, Rn. 19.

Auf dieser Grundlage scheint hier auf den ersten Blick der Anwendungsbereich von § 86b Abs. 1 SGG eröffnet zu sein. Der von dem Antragsteller am 15. März 2022 erhobene Widerspruch hätte dabei gemäß § 86a Abs. 1 Satz 1 SGG sogar bereits von Gesetzes wegen aufschiebende Wirkung, sodass es eines gerichtlichen Eilrechtsschutzes insoweit nicht bedürfte.

Jedoch hilft eine denkbare aufschiebende Wirkung des Widerspruchs der Beschwer des Antragstellers, die das vorliegende Verfahren beheben soll, nicht ab. Dem Antragsteller geht es nicht (allein) darum, die Ablehnung seines Antrags zu beseitigen, sondern (vor allem) die Datenübermittlung an die Datensammelstelle zu verhindern. Dieses Ziel erreicht er nicht schon, wenn sein auf der Grundlage von Art. 21 Abs. 1 und Abs. 6 DSGVO geltend gemachter (datenschutzrechtlicher) Widerspruch nicht zurückgewiesen wird beziehungsweise wenn die Zurückweisung wegen der aufschiebenden Wirkung seines (prozessrechtlichen) Widerspruchs einstweilen ausgesetzt ist. Die Antragsgegnerin muss dieses Betroffenenrecht vielmehr durch ein konkretes Unterlassen erfüllen, indem sie von einer Datenübermittlung absieht. Dem Antragsteller geht es also um eine Leistung. Da die Datenübermittlung nicht auf der Zurückweisung des (datenschutzrechtlichen) Widerspruchs des Antragstellers, sondern auf den gesetzlichen Regelungen in §§ 303a ff. SGB V beruht, kann er dieses Begehren durch die aufschiebende Wirkung seines (prozessrechtlichen) Widerspruchs ebenso wenig erreichen wie in der Hauptsache durch eine bloße Anfechtungsklage. In der Hauptsache wäre daher gemäß § 54 Abs. 4 SGG eine mit der Anfechtungsklage verbundene (unechte) Leistungsklage statthaft. Im Eilverfahren ist das von dem Antragsteller verfolgte Leistungsbegehren durch einen Antrag nach § 86b Abs. 2 Satz 1 SGG abzubilden.

Der Antrag ist zulässig. Der Antragsteller ist analog § 54 Abs. 1 Satz 2 SGG klagebefugt, da die gesetzlich angeordnete Datenübermittlung in seine Grundrechte aus Art. 7 und Art. 8 GRCh sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreift und eine Grundrechtsverletzung zumindest möglich ist.

Dementsprechend ist auch zumindest möglich, dass der Antragsteller von der Antragsgegnerin verlangen kann, die Datenübermittlung zu unterlassen.

Das für den von dem Antragsteller begehrten vorbeugenden Rechtsschutz erforderliche qualifizierte Rechtsschutzinteresse besteht. Die Datenübermittlung, gegen die sich der Antragsteller wendet, ist gesetzlich spätestens zu einem bestimmten Stichtag vorgesehen und darum konkret absehbar. Der Antragsteller kann nicht auf einen nachträglichen Rechtsschutz verwiesen werden, da dieser für ihn mit unzumutbaren Nachteilen verbunden wäre. In der gesetzlich vorgesehenen Datenübermittlung liegt gegenüber dem Antragsteller ein Grundrechtseingriff, der sich im Rahmen eines nachträglichen Rechtsschutzverfahrens nicht mehr rückgängig machen ließe. Zudem könnte der Antragsteller durch einen nachträglichen Rechtsschutz die ihn belastenden Folgen der Datenübermittlung nicht mehr zuverlässig ausräumen.

Die Antragsgegnerin hat, sobald sie die Daten an die Datensammelstelle übermittelt hat, auf die weitere Datenverarbeitung keinen Einfluss mehr. Das Ziel des Antragstellers, dass es zu einer Datenübermittlung und zu den daran anschließenden Datenverarbeitungsschritten gar nicht erst kommt, ließe sich auf dem Weg über einen nachträglichen Rechtsschutz von vornherein nicht erreichen.

Ein nachträglicher Rechtsschutz, der die Datenverarbeitung vorläufig stoppt, käme darum von vornherein nur gegenüber den anderen am Datentransparenzverfahren beteiligten Stellen in Betracht. Hierzu müsste der Antragsteller von einer dieser Stellen die Löschung der ihn betreffenden Daten verlangen. Dies ist dem Antragsteller jedoch nicht zumutbar, da er so seine Rechte nicht hinreichend wirksam verteidigen könnte.

Zum einen wäre ein derartiges Löschungsbegehren faktisch erheblich erschwert. In den Datenbeständen der Datensammelstelle, der Vertrauensstelle und des Forschungsdatenzentrums ist der Antragsteller nur anhand von Pseudonymen identifizierbar, die ihm nicht bekannt sind. Um einen Löschungsanspruch überhaupt substantiieren zu können, müsste sich der Antragsteller zunächst das Pseudonym beschaffen, unter dem seine Daten in dem jeweiligen Datenbestand gespeichert sind. Hierzu müsste er sich mindestens an eine weitere, gegebenenfalls an mehrere Stellen wenden. Um beispielsweise gegenüber dem Forschungsdatenzentrum die zu löschenden Daten zu bezeichnen, müsste sich der Antragsteller zunächst bei der Antragsgegnerin das Lieferpseudonym beschaffen, unter dem die Antragsgegnerin die Daten an die Datensammelstelle übermittelt hat.

Anschließend müsste der Antragsteller durch die Vertrauensstelle aus dem Lieferpseudonym das periodenübergreifende Pseudonym berechnen lassen, unter dem die Daten bei dem Forschungsdatenzentrum gespeichert sind. Ein solches Vorgehen wäre sehr aufwändig und könnte schlimmstenfalls ein erhebliches Sicherheitsrisiko begründen. Der Antragsteller müsste sich insbesondere gegenüber der Vertrauensstelle und nachfolgend dem Forschungsdatenzentrum identifizieren, obwohl diese Stellen seine Identität gerade nicht kennen sollen.

Zum anderen könnte der Antragsteller durch einen nachträglichen Rechtsschutz nicht verhindern, dass bis zur gerichtlichen Entscheidung die ihn betreffenden Daten im Rahmen des Datentransparenzverfahrens verarbeitet werden. Der Antragsteller wendet sich gegen die bevorstehende Datenübermittlung aber gerade, weil nach seiner Auffassung das Datentransparenzverfahren unzumutbare Sicherheitsrisiken begründet und die Datenverarbeitung ihm nicht gegen seinen Willen zugemutet werden kann. Mit einem Verweis auf einen nachträglichen Rechtsschutz würde dem Antragsteller angesonnen, gerade die Rechtsbeeinträchtigungen und Grundrechtsgefährdungen, gegen die er sich wendet, für einen nicht genau absehbaren gerichtlichen Entscheidungszeitraum irreversibel hinzunehmen.

D. Anordnungsanspruch

Dem Antragsteller steht der für den Erlass einer einstweiligen Anordnung erforderliche Anordnungsanspruch zu. Er hat einen Anspruch gegen die Antragsgegnerin, die Datenübermittlung an die Datensammelstelle zu unterlassen. Dieser Anspruch ergibt sich aus drei voneinander unabhängigen Rechtsgründen.

Erstens ist die Datenübermittlung an die Datensammelstelle nur zulässig, wenn es für sie eine mit höherrangigem Recht vereinbare Rechtsgrundlage gibt (unten I). Die Regelungen über das Datentransparenzverfahren gewährleisten jedoch die Sicherheit der in diesem Verfahren verarbeiteten Daten nur unzureichend. Daher ist die Erlaubnisregelung in § 303b Abs. 1 SGB V sowohl unionsrechts- als auch verfassungswidrig und darum unanwendbar. Hieraus folgt ein Unterlassungsanspruch des Antragstellers (unten II).

Zweitens steht dem Antragsteller ein Recht zum Widerspruch gegen die Datenübermittlung zu, von dem er mit seinem Schreiben vom 1. März 2022 wirksam Gebrauch gemacht hat. Aufgrund des Widerspruchs ist die Datenübermittlung unzulässig. Sollte ein Widerspruchsrecht nicht bestehen, so müsste es zur Wahrung des Verhältnismäßigkeitsgrundsatzes geschaffen werden. In diesem Fall verstießen die Rechtsgrundlagen des Datentransparenzverfahrens gegen höherrangiges Recht und wären unanwendbar, woraus sich wiederum ein Unterlassungsanspruch des Antragstellers ergäbe (unten III).

Drittens kann der Antragsteller von der Antragsgegnerin verlangen, dass diese die Datenübermittlung zumindest so lange unterlässt, bis die Berechtigung seines Widerspruchs abschließend geklärt ist (unten IV).

I. Erfordernis einer unionsrechts- und verfassungskonformen gesetzlichen Übermittlungserlaubnis

Die Datenübermittlung von der Antragsgegnerin an den Spitzenverband Bund der Krankenkassen hat personenbezogene Daten des Antragstellers zum Gegenstand und bedarf darum einer gesetzlichen Übermittlungserlaubnis, die höherrangigem Recht genügt.

Für das vorliegende Verfahren sind als Quellen höherrangigen Rechts maßgeblich zum einen das in der DSGVO geregelte allgemeine europäische Datenschutzrecht, das im Lichte der Unionsgrundrechte aus Art. 7 und Art. 8 GRCh auszulegen ist, zum anderen das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung.

Erstens fällt die in § 303b Abs. 1 Satz 1 SGB V i.V.m. § 3 DaTraV vorgesehene Datenübermittlung gemäß Art. 2 Abs. 1 DSGVO in den Anwendungsbereich des allgemeinen europäischen Datenschutzrechts.

Die Voraussetzungen des Art. 2 Abs. 1 DSGVO liegen vor. Gemäß § 303b Abs. 1 Satz 1 SGB V übermitteln die Krankenkassen dem Spitzenverband personenbezogene Daten. Hieran ändert die Pseudonymisierung durch das Lieferpseudonym nichts, da pseudonyme Daten zumindest für die Stelle, die das Pseudonym der betroffenen Person zuordnen kann, personenbezogen sind,

> statt aller Klar/Kühling, in: Kühling/Buchner, DSGVO/BDSG, Art. 4 Nr. 5 DSGVO Rn. 11 f.

Auch wenn § 303b Abs. 1 Satz 1 SGB V dies nicht ausdrücklich regelt, wird die Datenübermittlung zudem immer automatisiert erfolgen.

Die in § 303b Abs. 1 Satz 1 SGB V i.V.m. § 3 DaTraV vorgesehene Datenübermittlung unterfällt keinem der Ausnahmetatbestände vom sachlichen Anwendungsbereich des allgemeinen europäischen Datenschutzrechts in Art. 2 Abs. 2 DSGVO. Insbesondere handelt es sich nicht im Sinne von Art. 2 Abs. 2 lit. a DSGVO um eine Datenverarbeitung im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

Zwar hat das Bundessozialgericht bislang offengelassen, ob die DSGVO Datenverarbeitungen im Bereich der gesetzlichen Krankenversicherung erfasst. Dies sei fraglich, weil die Festlegung der Gesundheitspolitik, die Organisation des Gesundheitswesens und die medizinische Versorgung nach Art. 168 Abs. 7 Satz 1 und 2 AEUV in der Verantwortung der Mitgliedstaaten lägen,

> BSG, Urteil vom 20. Januar 2021 – B 1 KR 7/20 R –, juris, Rn. 28.

Auf der Grundlage der jüngeren Rechtsprechung des Gerichtshofs der Europäischen Union scheidet jedoch eine Anwendung des Ausnahmetatbestands in Art. 2 Abs. 2 lit. a DSGVO auf Datenverarbeitungen im Rahmen der gesetzlichen Krankenversicherung aus. Danach ist dieser Ausnahmetatbestand eng auszulegen und erfasst nur Datenverarbeitungen „im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann“,

> EuGH, Urteil vom 22. Juni 2021, Rs. C-439/19 – Latvijas Republikas Saeima, Rn. 66.

Dementsprechend hat der Gerichtshof etwa angenommen, Datenverarbeitungen durch den Petitionsausschuss eines Landtags unterfielen dem Anwendungsbereich der DSGVO, obwohl die Europäische Union über keinerlei Regelungskompetenzen im Bereich des mitgliedstaatlichen Parlamentsrechts verfügt und die Tätigkeit des Petitionsausschusses unmittelbar keinen unionsrechtlichen Vorgaben unterliegt,

> vgl. EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19 – Land Hessen, Rn. 66 ff.

Auch wenn es an abstrakten Kriterien zur Bestimmung des Anwendungsbereichs des Unionsrechts i.S.v. Art. 2 Abs. 2 lit. a DSGVO bislang fehlt, lässt sich aus der jüngsten Rechtsprechung schließen, dass eine Anwendung des Ausnahmetatbestands nur dann in Betracht kommt, wenn eine Datenverarbeitung überhaupt keinen auch nur mittelbaren Bezug zum Unionsrecht hat,

> näher Bäcker, in: BeckOK Datenschutzrecht, Art. 2 DSGVO Rn. 7 ff.; ähnlich Grzeszick NVwZ 2018, 1505 (1507); zu Art. 16 AEUV, dessen Grenzen Art. 2 Abs. 2 lit. a nachzeichnet, Brühann, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 16 AEUV Rn. 65 ff.

Datenverarbeitungen im Rahmen des Systems der gesetzlichen Krankenversicherung weisen hingegen vielfältige Bezüge zu (auch) unionsrechtlich geprägten Tätigkeiten auf. Insoweit sei etwa auf die (beschränkten) Regelungskompetenzen der Union im Gesundheitswesen aus Art. 168 AEUV und die Relevanz der Unionsbürgerschaftsrechte sowie der Wirtschaftsfreiheiten des AEUV für die Ausgestaltung des Versicherungssystems verwiesen. Hinzu kommt, dass das Datentransparenzverfahren nicht allein den Zwecken der gesetzlichen Krankenversicherung dient, sondern maßgeblich auch Datenverarbeitungen zu Forschungszwecken ermöglichen soll. Solche Datenverarbeitungen weisen gleichfalls in weitem Umfang unionsrechtliche Bezüge auf. So ist die Europäische Union selbst nach Maßgabe von Art. 179 ff. AEUV forschungspolitisch tätig. Zudem werden Forschungsdaten regelmäßig grenzüberschreitend ausgetauscht, was wiederum den Anwendungsbereich primär- oder sekundärrechtlicher Regelungen des Unionsrechts eröffnen kann,

von einer Anwendbarkeit der DSGVO auf die Datenverarbeitungen im Rahmen des Datentransparenzverfahrens gehen ohne weiteres aus etwa Kühling/Schildbach, NZS 2020, 41 (43); Schulz, SGb 2020, 536 (538); Weichert, MedR 2020, 539 (540); Spiecker gen. Döhmann/Bretthauer, JZ 2020, 990 (994 f.).

Zweitens ergeben sich Anforderungen an die Gestaltung und Anwendung der Datenübermittlungserlaubnis in § 303b Abs. 1 Satz 1 SGB V i.V.m. § 3 DaTraV aus dem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verbürgten Recht auf informationelle Selbstbestimmung. Dieses Grundrecht ist anwendbar, da die Regelungen über das Datentransparenzverfahren nicht vollständig unionsrechtlich determiniert sind, sondern der Gesetzgeber mit ihnen von einem Regelungsspielraum Gebrauch gemacht hat, den ihm das europäische Datenschutzrecht überantwortet,

vgl. etwa BVerfGE 118, 79 (95 ff.); 155, 119 (165); stRspr.

Die gesetzlich vorgesehene Übermittlung und Weiterverarbeitung personenbezogener, wenn auch pseudonymisierter Daten, greift in das Recht auf informationelle Selbstbestimmung ein,

vgl. BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 19. März 2020 – 1 BvQ 1/20 –, juris, Rn. 13.

Die gesetzliche Übermittlungserlaubnis muss daher am Maßstab dieses Grundrechts gerechtfertigt werden.

Aus dem allgemeinen europäischen Datenschutzrecht und aus dem Recht auf informationelle Selbstbestimmung folgen materiell-, verfahrens- und organisationsrechtliche Anforderungen an die gesetzliche Übermittlungserlaubnis. Mit Blick auf das vorliegende Verfahren sind insbesondere zwei inhaltliche Anforderungskomplexe zu nennen: Zum einen müssen die Rechtsgrundlagen des Datentransparenzverfahrens in hinreichendem Maß gewährleisten, dass die Integrität und Vertraulichkeit der Daten als grundlegende Schutzziele der Datensicherheit bei der und im Anschluss an die Übermittlung gewahrt bleiben. Zum anderen muss die gesetzliche Übermittlungserlaubnis materiell sicherstellen, dass die Daten nur übermittelt werden, wenn das öffentliche Interesse daran das gegenläufige Datenschutzinteresse der betroffenen Person überwiegt.

Unionsrechtlich folgt dies vor allem aus fünf Regelungen. Erstens beruht die gesetzliche Übermittlungserlaubnis in § 303b Abs. 1 Satz 1 SGB V i.V.m. § 3 DaTraV auf den in Art. 6 Abs. 1 Satz 1 lit. c und e, Abs. 3 DSGVO enthaltenen

Öffnungsklauseln für mitgliedstaatliche Verarbeitungsregelungen; die genaue Zuordnung kann an dieser Stelle noch offenbleiben. In jedem Fall ergeben sich aus Art. 6 Abs. 3 DSGVO Anforderungen an das mitgliedstaatliche Recht, zu denen insbesondere der Verhältnismäßigkeitsgrundsatz zählt.

Zweitens hat die Übermittlungserlaubnis in weitem Umfang Gesundheitsdaten zum Gegenstand, für die gemäß Art. 9 Abs. 1 DSGVO ein grundsätzliches Verarbeitungsverbot besteht. Insoweit ergeben sich mit Blick auf die Zwecke des Datentransparenzverfahrens Ausnahmetatbestände, die durch mitgliedstaatliches Recht auszufüllen sind, aus Art. 9 Abs. 2 lit. h, i und j DSGVO. Die besondere Sensibilität von Gesundheitsdaten indiziert allerdings in materieller, prozeduraler und organisatorischer Hinsicht strenge Anforderungen an mitgliedstaatliche Ausnahmeregelungen.

Drittens sieht das Unionsrecht zur Wahrung der Verhältnismäßigkeit von Datenverarbeitungen in Art. 21 DSGVO vor, dass eine betroffene Person aus besonderen persönlichen Gründen einer allgemein gerechtfertigten Datenverarbeitung widersprechen kann. Aufgrund eines solchen Widerspruchs ist die Datenverarbeitung grundsätzlich einzustellen.

Viertens stellen die Integrität und Vertraulichkeit personenbezogener Daten als elementare Schutzziele der Datensicherheit nach Art. 5 Abs. 1 lit. f DSGVO einen zentralen Grundsatz des europäischen Datenschutzrechts dar.

Soweit fünftens das Datentransparenzverfahren Zwecken der wissenschaftlichen Forschung dient, ist schließlich die Querschnittsregelung in Art. 89 DSGVO zu beachten. Diese Norm errichtet einerseits – auch im Zusammenwirken mit weiteren Vorschriften der DSGVO – spezifische Privilegien für die wissenschaftliche Forschung, knüpft diese andererseits jedoch daran, dass geeignete Garantien für die betroffenen Personen geschaffen werden.

Verfassungsrechtlich sind die Anforderungen aus dem Verhältnismäßigkeitsgrundsatz abzuleiten. Aus diesem Grundsatz ergeben sich sowohl materielle Maßstäbe für Datenübermittlungen als auch Vorgaben für die Datensicherheit,

> vgl. mit Blick auf das Datentransparenzverfahren die geraffte Problemskizze bei BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 19. März 2020 – 1 BvQ 1/20 –, juris, Rn. 8.

II. Unzureichende Gewährleistung der Datensicherheit

Wegen der sehr hohen Sensibilität der personenbezogenen Daten, die im Rahmen des Datentransparenzverfahrens verarbeitet werden, müssen die Rechtsgrundlagen dieses Verfahrens ein besonders hohes Niveau der Datensicherheit gewährleisten (unten 1). Die Regelungen in §§ 303a ff. SGB V und in der DaTraV verfehlen diese Anforderung auf allen Stufen der Datenverarbeitung (unten 2). Der Antragsteller kann darum von der Antragsgegnerin verlangen, die Datenübermittlung an die Datensammelstelle zu unterlassen (unten 3).

1. Erforderlichkeit eines besonders hohen Sicherheitsniveaus

Sowohl aus dem europäischen Datenschutzrecht als auch aus dem Recht auf informationelle Selbstbestimmung ergeben sich Anforderungen an die Datensicherheit. Diese Anforderungen fallen desto strenger aus, je sensibler die verarbeiteten Daten sind. An die Sicherheit der im Rahmen des Datentransparenzverfahrens verarbeiteten Daten sind darum besonders strenge Maßstäbe anzulegen.

a) Schutzziele der Datensicherheit

Mit dem Begriff der Datensicherheit werden hier die in der Informationstechnik herausgearbeiteten, im Unions- und Verfassungsrecht aufgegriffenen Schutzziele der Vertraulichkeit und Integrität personenbezogener Daten bezeichnet. Daten sind vertraulich, wenn Unbefugte sie nicht zur Kenntnis nehmen können. Sie sind integer, wenn Unbefugte sie nicht verändern können (sog. starke Integrität) oder Veränderungen zumindest erkennbar sind (sog. schwache Integrität).

Die rechtlichen Anforderungen an die Datensicherheit haben – anders als die meisten anderen Regelungen im Datenschutzrecht – nicht die Voraussetzungen und Grenzen zulässiger Datenverarbeitungen, sondern die Vermeidung unzulässiger Datenverarbeitungen zum Gegenstand. Ihnen liegt zugrunde, dass die Verarbeitung personenbezogener Daten durch Unbefugte erhebliche Schäden verursachen kann. Diese Schäden können von Enttäuschungen im persönlichen Nahbereich über Nachteile im Geschäftsverkehr bis zu kriminellen Übergriffen wie Identitätstäuschungen oder Erpressungen reichen.

Vollkommene Datensicherheit lässt sich allerdings faktisch nie garantieren. Die rechtlichen Vorgaben zum Schutz der Vertraulichkeit und Integrität personenbezogener Daten verlangen daher lediglich ein hinreichendes

Schutzniveau für die Datensicherheit. Welches Schutzniveau im Einzelnen angezeigt ist, ist aus den maßgeblichen Regelungen mit Blick auf die Umstände des jeweiligen Datenverarbeitungsprozesses abzuleiten.

b) Vorgaben des höherrangigen Rechts

Das europäische Datenschutzrecht konkretisiert die Anforderungen an die Datensicherheit in mehreren spezifischen Regelungen. Insbesondere zu nennen sind Art. 24, Art. 25 und vor allem Art. 32 DSGVO. Diese spezifischen Regelungen wenden sich allerdings an den Verantwortlichen für eine Datenverarbeitung. Eine Pflicht des Gesetzgebers zur Gewährleistung der Datensicherheit bei Datenverarbeitungen, die er durch gesetzliche Verarbeitungsregelungen vorformt, ist ihnen unmittelbar nicht zu entnehmen. Für die Bindungen des Gesetzgebers kann jedoch auf den allgemeinen Grundsatz des Art. 5 Abs. 1 lit. f DSGVO sowie auf die dem europäischen Datenschutzrecht zugrunde liegenden Grundrechte aus Art. 7 und Art. 8 GRCh zurückgegriffen werden,

> vgl. zur grundrechtlichen Verpflichtung des europäischen Gesetzgebers auf die Datensicherheit EuGH, Urteil vom 8. April 2014, Rs. C-293/12 – Digital Rights Ireland, Rn. 54 f.

Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG errichtet gleichfalls grundrechtliche Anforderungen an die Datensicherheit. Soweit der Gesetzgeber Eingriffe in dieses Grundrecht durch eine gesetzliche Datenverarbeitungsermächtigung ermöglicht, muss er die Sicherheit der verarbeitenden Daten gewährleisten,

> vgl. zu Art. 10 GG BVerfGE 125, 260 (325 ff.); zu korrespondierenden Schutzpflichten BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 30 ff.

Auch inhaltlich errichten das europäische Datenschutzrecht und das Recht auf informationelle Selbstbestimmung zumindest im Ansatz gleichläufige Vorgaben. Der Gesetzgeber muss zur Gewährleistung der Datensicherheit prozedural, organisatorisch und technisch ansetzende Regelungen schaffen. Die Anforderungen an die Regelungsdichte und an das zu gewährleistende Schutzniveau hängen maßgeblich davon ab, wie sensibel die verarbeiteten Daten sind. Der für den Verantwortlichen geltende, insbesondere aus Art. 32 Abs. 1 und 2 DSGVO abzuleitende risikobasierte Ansatz ist damit prinzipiell auf den Gesetzgeber zu übertragen. Insbesondere wenn eine gesetzlich vorgesehene Datenverarbeitung ein hohes Risiko aufweist, können spezifisch

ansetzende Regelungen zur Datensicherheit gerade für diese Verarbeitung geboten und ein Verweis auf allgemeine Vorgaben unzureichend sein,

> vgl. zu Art. 7 und 8 GRCh EuGH, Urteil vom 8. April 2014, Rs. C-293/12 – Digital Rights Ireland, Rn. 66 f.; zu Art. 10 GG BVerfGE 125, 260 (325 ff., 348 ff.).

c) Sensibilität der verarbeiteten Daten

An die Sicherheit der Daten, die im Rahmen des Datentransparenzverfahrens verarbeitet werden, sind besonders strenge Anforderungen zu stellen. Dies folgt aus der äußerst hohen Sensibilität dieser Daten,

> Bretthauer, Die Verwaltung 54 (2021), 411 (423).

Die nach § 303b Abs. 1 Satz 1 SGB V i.V.m. § 3 DaTraV zu übermittelnden Daten sind überwiegend als Gesundheitsdaten einzustufen, deren besondere Sensibilität sich bereits aus dem grundsätzlichen Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO ergibt. Das europäische Datenschutzrecht nimmt diese Regelung verschiedentlich in Bezug, um im Rahmen eines risikobasierten Ansatzes einen besonderen Bedarf für prozedurale Schutzvorkehrungen zu markieren (vgl. Art. 30 Abs. 5, Art. 35 Abs. 3 lit. b, Art. 37 Abs. 1 lit. c DSGVO).

Im Rahmen des Datentransparenzverfahrens sind Gesundheitsdaten in besonders großem Umfang zu übermitteln und über einen langen, bis zu 30 Jahre umfassenden Zeitraum zu bevorraten. Erfasst werden Daten zur ambulanten Versorgung, zur Abgabe von Arzneimitteln, zur stationären Versorgung und zur Versorgung mit Heil- und Hilfsmitteln, von der Diagnose über die Art der Behandlung bis zur Dosierung eines Medikaments. Die bei dem Forschungsdatenzentrum gespeicherten Gesundheitsdaten ermöglichen es, höchst aussagekräftige Gesundheitsprofile der betroffenen Personen, also aller gesetzlich Versicherten zu erstellen. Die Sensibilität dieses Datenbestands, der auf den durch die Krankenversicherungen übermittelten Daten basiert, erscheint kaum noch steigerungsfähig. Das spiegelt sich in dem hohen Wert von Gesundheitsdatensätzen auf dem Schwarzmarkt: im Schnitt 250 US-Dollar pro Datenbankeintrag, mit Höchstwerten von 1.000 bis 2.600 US-Dollar,

> vgl. dazu das von dem Antragsteller vorprozessual eingeholte Gutachten von Professor Dominique Schröder **(Anlage 7)**, S. 42 ff. (im Folgenden: Gutachten Schröder).

Zudem werden diese Gesundheitsdaten im Rahmen eines Versorgungssystems erzeugt, zu dem die betroffenen Personen keine

realistische Alternative haben. Ihr Versichertenstatus beruht in den meisten Fällen auf der grundsätzlichen Versicherungspflicht. Die theoretisch denkbaren Wege, eine Datenverarbeitung abzuwenden, indem die betroffenen Personen die von ihnen in Anspruch genommenen Gesundheitsdienstleistungen selbst bezahlen, sich (soweit überhaupt möglich) freiwillig privat versichern oder auf solche Dienstleistungen verzichten, sind unzumutbar. So wäre für den Antragsteller eine private Krankenversicherung wegen seiner Vorerkrankungen nicht zu erlangen. Zugleich benötigt er wegen seiner Blutgerinnungsstörung wöchentlich Medikamente im Wert von etwa 6.000 Euro. Die faktische Unvermeidbarkeit der Datenerzeugung für die betroffenen Personen erhöht die Eingriffsintensität und damit auch die Sensibilität der im Datentransparenzverfahren verarbeiteten Daten.

Dem Befund einer hohen Sensibilität der verarbeiteten Daten lässt sich nicht entgegenhalten, dass die Daten in pseudonymisierter Form übermittelt und bevorratet werden. Die Pseudonymisierung ist Teil des gebotenen Schutzkonzepts, macht aber weitere Schutzvorkehrungen nicht entbehrlich.

Das Datentransparenzverfahren beruht auf einem Pseudonymisierungsmechanismus, der bei dem Forschungsdatenzentrum jeder versicherten Person dauerhaft ein bestimmtes periodenübergreifendes Pseudonym zuordnet. Mithin lässt sich anhand der Pseudonyme eindeutig bestimmen, welche der gespeicherten Daten einer bestimmten Person zuzuordnen sind. Es ist davon auszugehen, dass auf der Grundlage des sehr großen und aussagekräftigen Datenbestands des Forschungsdatenzentrums eine Reidentifikation der hinter dem Pseudonym stehenden Person mit nur geringem Zusatzwissen möglich ist,

> vgl. zu den niedrigen faktischen Hürden für eine Reidentifikation bei Gesundheitsdaten Gutachten Schröder, S. 7 ff.; ferner Kühling/Schildbach, NZS 2020, 41 (43 f.); Schrahe/Städter, DuD 2020, 713 (714).

So könnte ein Unbefugter, der Zugriff auf die im Datentransparenzverfahren verarbeiteten Daten erlangt, schon allein durch den Abgleich dieser Daten mit einem Vergleichsdatenbestand, der neben den Namen bestimmter Zielpersonen deren Geburtsjahre, Geschlechter und Postleitzahlen enthält, eine Treffermenge erzeugen, die eine weitreichende Eingrenzung ermöglicht. Wenn der Vergleichsdatenbestand auch nur eine der weiteren sehr spezifischen Angaben enthält, die aufgrund von § 3 DaTraV in das Datentransparenzverfahren einfließen, wird in vielen Fällen eine Identifikation

der Zielpersonen in dem Datenbestand des Datentransparenzverfahrens möglich sein – was dann eine Nutzung aller vorhandenen Daten über die Zielpersonen für unbefugte Zwecke ermöglichen würde.

Die Pseudonymisierung der verarbeiteten Daten mit einem für jede versicherte Person konstanten periodenübergreifenden Pseudonym bietet daher insgesamt bei einem so aussagekräftigen Datenbestand wie dem des Datentransparenzverfahrens nur einen schwachen Schutz. Sie reicht für sich genommen nicht aus, um ein Sicherheitsniveau zu gewährleisten, das der Sensibilität der verarbeiteten Daten auch nur annähernd Rechnung trägt.

2. Defizite der gesetzlichen Ausgestaltung des Datentransparenzverfahrens

Aufgrund der sehr hohen Sensibilität der übermittelten und gespeicherten Daten muss der Gesetzgeber durch prozedurale, organisatorische und technische Schutzvorkehrungen ein besonders hohes Niveau der Datensicherheit gewährleisten. Das gesetzlich vorgesehene Datentransparenzverfahren genügt dem nicht. Die gesetzlichen Regelungen legen einen Schutzmechanismus an, der erhebliche konzeptionelle Schwächen aufweist und darum strukturell nicht dazu geeignet ist, das gebotene Sicherheitsniveau zu erreichen.

Die folgenden Ausführungen beruhen in tatsächlicher Hinsicht auf dem Gutachten von Professor Dominique Schröder. Es wird **angeregt,** Professor Schröder im Verfahren anzuhören oder gegebenenfalls weitere sachverständige Stellungnahmen zu den Sicherheitsmängeln des Datentransparenzverfahrens und zu vorzugswürdigen alternativen Gestaltungen der Datenbereitstellung einzuholen.

a) Datentransfer über die Datensammelstelle

Das in §§ 303a ff. SGB V vorgesehene gestufte Verfahren der Datenzusammenführung beinhaltet im ersten Schritt eine Zentralisierung des Datentransfers. Der Spitzenverband Bund der Krankenkassen als Datensammelstelle erhält sämtliche im Laufe eines Berichtsjahrs angefallenen Berichtsdaten aller gesetzlich krankenversicherten Personen in Deutschland.

Die Zentralisierung des Datentransfers begründet sehr hohe Sicherheitsrisiken. Zwar sind diese Daten durch die Lieferpseudonyme pseudonymisiert. Die für das gesamte Berichtsjahr geltenden Lieferpseudonyme ermöglichen jedoch einem Angreifer, der sich den Datenbestand der Datensammelstelle beschafft, ohne weiteres eine auf die

pseudonymisierten Einzelpersonen bezogene Zusammenführung zahlreicher Gesundheitsdaten. Dadurch werden nicht nur weitreichende Rückschlüsse etwa auf den Gesundheitszustand der betroffenen Personen möglich. Sondern zumindest in vielen Fällen werden sich diese Personen auf der Grundlage der bei der Datensammelstelle vorhandenen Daten mit geringem Zusatzwissen identifizieren lassen, wie oben bereits dargestellt wurde. Gelingt es einem Angreifer mithin, sich unbefugt Zugriff auf den Datenbestand der Datensammelstelle zu verschaffen, so stehen ihm schlimmstenfalls zahlreiche personenbeziehbare, höchst sensible Informationen über fast 90% der Bevölkerung zur Verfügung. Angesichts des hohen ökonomischen Wertes von Gesundheitsdaten ist davon auszugehen, dass derartige Angriffe mit beträchtlichem Aufwand betrieben und früher oder später erfolgreich sein werden,

> vgl. Gutachten Schröder, S. 40 ff.; vgl. zu dem für den Umgang mit IT-Sicherheitslücken empfohlenen „Assume-Breach-Paradigma“ BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 38.

Aus der Perspektive der Datensicherheit bildet die Datensammelstelle mithin eine Art Aggregator, der die zuvor dezentral bei mehr als 100 Krankenkassen gespeicherten Gesundheitsdaten zusammenführt und für erfolgreiche Angreifer auf einen Schlag erschließbar macht. Ein hinreichend gewichtiger Grund dafür, einen derartig sensiblen Datenbestand bei der Datensammelstelle zum Zweck des Datentransfers zentral zusammenzuführen und dabei die genannten Risiken hinzunehmen, ist nicht ersichtlich.

Die Aufbereitung der Daten in standardisierte versichertenbezogene Datensätze und die Übermittlung der aufbereiteten Daten an das Forschungsdatenzentrum könnten stattdessen die Krankenkassen selbst übernehmen. Dabei würden die Daten durch Zwischenschaltung der Vertrauensstelle so pseudonymisiert, dass weder die Krankenkassen das periodenübergreifende Pseudonym des Forschungsdatenzentrums kennen noch das Forschungsdatenzentrum das Lieferpseudonym der Krankenkassen kennt. Ein solches Verfahren, das ohne eine Datensammelstelle auskommt, sieht § 363 Abs. 3 SGB V für die einwilligungsbasierte Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken vor.

Auch die in § 303b Abs. 2 SGB V i.V.m. § 4 Abs. 2 und 3 DaTraV geregelte Prüfung der Daten auf Vollständigkeit, Plausibilität und Konsistenz könnte den Krankenkassen übertragen werden. Diese Prüfung kann zwar einen Gesamtüberblick über die während des Berichtsjahrs angefallenen Daten

erfordern, über den eine einzelne Krankenkasse etwa dann nicht verfügt, wenn die versicherte Person während des Berichtsjahrs die Krankenkasse gewechselt hat. Für solche Fälle könnte jedoch ein besonderes Bereinigungsverfahren zwischen den betroffenen Krankenkassen eingerichtet werden, das ohne eine zentrale Datenspeicherung auskommt. Dabei könnte durch eine kryptographische Sicherung vermieden werden, dass eine der beteiligten Krankenkassen unverschlüsselten Zugriff auf Versichertendaten erhält, über die sie bisher nicht verfügt hat,

näher Gutachten Schröder, S. 51 ff.

Die Einrichtung der Datensammelstelle schafft daher ohne überzeugenden Sachgrund ein erhebliches Sicherheitsrisiko. Für den Datentransfer ist stattdessen ein dezentraler Ansatz klar vorzugswürdig, dessen genaue Gestaltung von den funktionalen Anforderungen an Überprüfung und Transfer der Daten abhängt,

vgl. beispielhaft zu einem ausbaubedürftigen Ansatz Gutachten Schröder, S. 53 ff.

Diese Gestaltung ist Sache des Normgebers und kann im vorliegenden Rechtsstreit nicht vorweggenommen werden. Maßgeblich ist hier allein, dass jedenfalls eine zentrale Datensammelstelle unter keinem Gesichtspunkt benötigt wird und darum auch nicht eingerichtet werden darf.

b) Datenhaltung im Forschungsdatenzentrum

Die Sicherung der Daten, die im Forschungsdatenzentrum bevorratet werden, ist unzureichend geregelt. Den Transparenzregelungen in §§ 303a ff. SGB V lässt sich nur entnehmen, dass das Forschungsdatenzentrum die periodenübergreifend pseudonymisierten Daten vorhält und den Nutzungsberechtigten zur Verfügung stellt. Aussagen über die technische und organisatorische Ausgestaltung der Datenhaltung finden sich im Gesetz nicht. In § 2 Abs. 4 Satz 1 DaTraV heißt es lediglich, die Sicherheit der Daten des Forschungsdatenzentrums sei nach dem Stand der Technik zu gewährleisten. Spezifischere Vorgaben zur Datensicherheit enthält die DaTraV nicht. Auch legt sie kein besonderes Verfahren zur Erarbeitung solcher Vorgaben an. Hinzu treten noch die ebenfalls allgemein gehaltenen Regelungen in Art. 24, Art. 25 und vor allem Art. 32 DSGVO.

Angesichts der äußerst hohen Sensibilität der vorgehaltenen Daten reicht dies nicht aus. Die gesetzlichen und verordnungsrechtlichen Rechtsgrundlagen des Datentransparenzverfahrens müssen vielmehr auf der Grundlage von

Art. 6 Abs. 2 und Abs. 3 Satz 3 sowie Art. 9 Abs. 2 lit. i und j DSGVO hinreichend normenklare Vorgaben für die Datensicherheit im Forschungsdatenzentrum errichten. Diese Vorgaben sind an die spezifischen Risiken wie Auswertungsbedarfe des Forschungsdatenzentrums anzupassen,

> vgl. zur Sicherung der gleichfalls sehr sensiblen Telekommunikations-Vorratsdaten EuGH, Urteil vom 8. April 2014, Rs. C-293/12 – Digital Rights Ireland, Rn. 54 f., 66 f.; BVerfGE 125, 260 (325 ff., 348 ff.).

Demgegenüber schließen die normativen Grundlagen des Datentransparenzverfahrens insbesondere eine zentrale Datenhaltung nicht aus, bei der die an das Forschungsdatenzentrum übermittelten Datensätze in pseudonymisierter, ansonsten aber unveränderter Form bevorratet werden. Eine zentrale Datenhaltung im Forschungsdatenzentrum lässt sich jedoch mit den unions- und verfassungsrechtlichen Anforderungen an die Integrität und Vertraulichkeit der Daten nicht vereinbaren.

Die zentrale Datenhaltung begründet im Ansatz dieselben Risiken für die betroffenen Personen wie der zentralisierte Datentransfer. Die Risiken wiegen im Vergleich zum Datentransfer insofern sogar noch schwerer, als das Forschungsdatenzentrum die Daten über einen noch weitaus längeren Zeitraum von bis zu 30 Jahren speichert. Der zentrale Datenbestand stellt ein potenziell äußerst lukratives Ziel für Angreifer dar, die sich durch einen erfolgreichen Angriff schlimmstenfalls auf einen Schlag eine Vielzahl höchst sensibler Informationen über einen Großteil der Bevölkerung verschaffen können. Die bevorrateten Daten können mit Hilfe der periodenübergreifenden Pseudonyme stets auf einzelne Versicherte bezogen werden. Die betroffenen Personen lassen sich, wie oben dargelegt, in der Regel mit geringem, teilweise mit für jedermann verfügbarem Zusatzwissen identifizieren. Wenn daher ein Angreifer nach erfolgreichem Angriff die erlangten Daten etwa veröffentlicht, kann er voraussichtlich sehr vielen Menschen dauerhaften erheblichen Schaden zufügen. Hieraus ergibt sich ein hohes Erpressungspotenzial. Zudem ließen sich die Daten auch durch einen „Verkauf“ an interessierte Stellen ökonomisieren.

Auch die Risiken der zentralen Datenhaltung sind nicht aufgrund überwiegender Gemeinwohlbelange hinnehmbar. Die Ziele des Datentransparenzverfahrens lassen sich auch auf der Grundlage einer dezentralen Datenbevorratung erreichen. Die für die Zwecke des Datentransparenzverfahrens erforderlichen Berechnungen könnten über

mehrere Datenbestände verteilt durchgeführt werden. Ein Zusammenfügen der Daten im Klartext ist hierfür nicht erforderlich,

vgl. Gutachten Schröder, S. 46 ff.

Geboten ist daher eine dezentrale Datenhaltung, deren genaue prozedurale, technische und organisatorische Spezifikationen an die Erfordernisse des Datentransparenzverfahrens anzupassen sind. Hierzu bedarf es konzeptioneller Vorarbeiten, die im Rahmen des vorliegenden Rechtsschutzverfahrens nicht zu leisten sind. Es ist vielmehr Aufgabe des Gesetzgebers, das gebotene Schutzkonzept zumindest in Grundzügen vorzugeben. Auf dieser Grundlage können durch delegierte Rechtsetzungsakte oder im Rahmen verbindlich vorgegebener Verfahren konkrete Anforderungen an die Sicherung des Forschungsdatenzentrums formuliert werden. Diese Aufgabe kann hingegen nicht, wie es das geltende Recht vorsieht, allein einer normativ nicht näher angeleiteten Selbstprogrammierung des Forschungsdatenzentrums überlassen werden, zumal § 2 Abs. 4 Satz 1 DaTraV mit dem Stand der Technik lediglich ein mittleres Schutzniveau vorgibt. Dieses Defizit begründet die Unvereinbarkeit der Regelungen über die Datenhaltung mit dem höherrangigen Recht, ohne dass hier positiv ein hinreichendes Schutzkonzept entwickelt werden könnte oder müsste.

c) Datenbereitstellung an die Nutzungsberechtigten

Die Regelungen zur Bereitstellung der Daten durch das Forschungsdatenzentrum an die Nutzungsberechtigten genügen gleichfalls nicht vollständig den Anforderungen, die an die Sicherheit der Daten zu stellen sind.

Keinen Bedenken unterliegt allerdings die Bereitstellung anonymisierter und aggregierter Daten mit größeren Fallzahlen nach § 303e Abs. 3 Satz 3 SGB V. Soweit aufgrund der Fallzahl davon auszugehen ist, dass eine Deanonymisierung mit realistischem Aufwand nicht möglich ist, ist mangels eines Personenbezugs der Anwendungsbereich des europäischen Datenschutzrechts gemäß Art. 2 Abs. 1 DSGVO nicht eröffnet und liegt auch kein Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vor,

Kühling/Schildbach, NZS 2020, 41 (44).

Allerdings ist unklar, welche praktische Relevanz dieser Regelung zukommt. Die informationstechnische Entwicklung führt nämlich dazu, dass aufgrund

zunehmender Rechen- und Speicherkapazitäten und immer weitergehender Verknüpfungsmöglichkeiten eine Reidentifikation betroffener Personen auch bei stark zerlegten anonymisierten Datensätzen nicht ausgeschlossen werden kann. Vielfach wird darum im Sinne einer Zweifelsregelung anzunehmen sein, dass eine Auswertung nicht unter § 303e Abs. 3 Satz 3 SGB V fällt, weil eine hinreichend zuverlässige Anonymisierung nicht gewährleistet werden kann.

Jedenfalls ist eine Identifikation einzelner betroffener Personen bei einer Bereitstellung anonymisierter und aggregierter Daten mit kleinen Fallzahlen nach § 303e Abs. 3 Satz 4 SGB V und erst recht bei einer Bereitstellung pseudonymisierter Einzeldatensätze nach § 303 Abs. 4 SGB V in vielen Fällen möglich. Auf der abstrakt-generellen Ebene der Rechtsgrundlagen des Datentransparenzverfahrens ist daher davon auszugehen, dass es sich in diesen Fallkonstellationen um eine Bereitstellung personenbezogener Daten handelt,

ähnlich Kühling/Schildbach, NZS 2020, 41 (45).

Für diese Fallkonstellationen enthält das Gesetz zwar eine Reihe von Schutzvorkehrungen, die insbesondere eine Identifikation konkreter Versicherter verhüten sollen. Diese Schutzvorkehrungen erreichen jedoch nicht in jeder Hinsicht das gebotene hohe Sicherheitsniveau.

Die Antragsprüfung durch das Forschungsdatenzentrum beschränkt sich hinsichtlich des Umfangs und der Struktur der beantragten Daten sowie hinsichtlich der Art der Datenbereitstellung gemäß § 303e Abs. 3 Satz 2 und 4, Abs. 4 Satz 1 SGB V i.V.m. § 8 Abs. 1 Nr. 4, § 10 Abs. 1 Nr. 3 DaTraV darauf, ob der Antragsteller die Erforderlichkeit der Bereitstellung „nachvollziehbar dargelegt“ hat. Es handelt sich also um eine nachvollziehende Plausibilitätsprüfung statt einer Vollprüfung, wie sie der Stellung des Forschungsdatenzentrums als Verantwortlichem für die Datenbereitstellung im Sinne von Art. 4 Nr. 7 DSGVO entsprechen würde. Anders gewendet wird dem Antragsteller ein Beurteilungsspielraum eingeräumt, dessen Wahrnehmung das Forschungsdatenzentrum nur begrenzt zu kontrollieren hat.

Für diese Absenkung der behördlichen Prüfungsdichte gibt es keinen rechtfertigenden Grund. Zwar ist einzuräumen, dass das Forschungsdatenzentrum nicht in jedem Fall über die Expertise verfügen wird, um die Erforderlichkeit des beantragten Datenzugangs hinsichtlich des Umfangs, der Struktur und der Bereitstellungsform selbst zu beurteilen. Soweit der Datenzugang dazu dient, Forschungsvorhaben durchzuführen, ist zudem

die durch Art. 13 GRCh und Art. 5 Abs. 3 GG gewährleistete Wissenschaftsfreiheit des Antragstellers zu beachten,

> hierauf verweisen zur Legitimation der bloßen Plausibilitätsprüfung Kühling/Schildbach, NZS 2020, 41 (47).

Die erforderliche Expertise könnte jedoch beschafft und den Belangen des Antragstellers könnte Rechnung getragen werden, indem das Verfahren des Datenzugangs ausgebaut würde. So hat das Forschungsdatenzentrum nach § 303d Abs. 2 SGB V einen Arbeitskreis der Nutzungsberechtigten einzurichten, der an der Ausgestaltung, Weiterentwicklung und Evaluation des Datenzugangs mitwirkt. Dieser Arbeitskreis könnte ein sachkundig und pluralistisch besetztes Gremium bestellen, das an der Entscheidung über den Datenzugang mitwirkt. Hierdurch würde eine Vollprüfung der Anträge ermöglicht, ohne die Wirksamkeit des Datenzugangs in Frage zu stellen,

> ähnlich der Vorschlag des Bundesrats im Gesetzgebungsverfahren, BT-Drs. 19/13438, S. 95; in diese Richtung auch Weichert, MedR 2020, 539 (545).

Auch andere Verfahrensgestaltungen, die eine Vollprüfung ermöglichen würden, sind denkbar. Der vom Gesetzgeber gewählte Ansatz geht hingegen ohne Not das beträchtliche Risiko ein, dass die vorgehaltenen Daten aufgrund überschießender Anträge in zu weitem Ausmaß zugänglich gemacht werden. So wird vielfach eine Reduktion der Datensätze um Daten in Betracht kommen, die für das konkrete Vorhaben nicht benötigt werden. Die Prüfung, ob eine solche Reduktion möglich und dann auch geboten ist, darf nicht weitgehend dem Nutzungsberechtigten überantwortet werden, der regelmäßig ein institutionelles Eigeninteresse verfolgt und nach seinem Aufgabenkreis nicht spezifisch auf die Sicherung der vorgehaltenen Daten programmiert ist.

Des Weiteren sind die technischen und organisatorischen Vorgaben für den besonders problematischen Zugang zu pseudonymisierten Einzeldatensätzen teils unschlüssig und lückenhaft.

Unschlüssig ist insbesondere die aus § 303d Abs. 1 Nr. 5 SGB V und § 10 Abs. 2 Satz 3, Abs. 3 DaTraV hervorgehende Vorgabe einer Sicherung nach Maßgabe des Reidentifikationsrisikos. Diese Vorgabe setzt voraus, dass das Forschungsdatenzentrum das spezifische Reidentifikationsrisiko für eine konkrete Datennutzung überhaupt tragfähig bewerten kann. Hierfür fehlt es jedoch bislang an belastbaren Methoden. Zudem und vor allem lässt sich das Reidentifikationsrisiko jedenfalls nur mit Blick auf das Hintergrundwissen desjenigen evaluieren, der die Daten befugt oder unbefugt erhält. Dieses

Hintergrundwissen wird dem Forschungsdatenzentrum in der Regel nicht bekannt sein,

> näher Gutachten Schröder, S. 56 ff.; kritisch auch Bretthauer, Die Verwaltung 54 (2021), 411 (424).

Die angeordnete Risikoanalyse erscheint deshalb kaum operationalisierbar. Sie taugt nicht dazu, das gebotene Sicherheitsniveau zu steuern.

Stattdessen liegt nahe, bei jeder Bereitstellung pseudonymisierter Einzeldatensätze von einem hohen Risiko auszugehen, das durch strengste Sicherheitsvorkehrungen abzuschirmen ist. Die Rechtsgrundlagen des Datentransparenzverfahrens sind insoweit vor allem deshalb lückenhaft, weil sie keine expliziten Aussagen dazu enthalten, in welcher Form die pseudonymisierten Datensätze bereitzustellen sind. Die bloße Pseudonymisierung der Daten vermindert das Risiko, das der Datenzugang für die betroffenen Personen birgt, in der Regel nicht in hinreichendem Ausmaß. Dies wurde oben bereits dargelegt. Regelmäßig werden weitergehende Schutzmaßnahmen möglich und geboten sein. So können die Daten über die Pseudonymisierung hinaus durch Verrauschen manipuliert werden, um eine Zuordnung zu bestimmten Personen zu verhindern oder zumindest zu erschweren. Vielfach leidet der aggregierte Erkenntniswert der Daten hierdurch nicht signifikant. Daneben können Berechnungen in vielen Fällen auf verschlüsselten Daten durchgeführt werden, sodass es einer Bereitstellung von (pseudonymisierten) Klardaten nicht bedarf,

> näher zu den unterschiedlichen Ansätzen Gutachten Schröder, S. 23 ff.

Derartige Schutzmaßnahmen legen die Rechtsgrundlagen des Datentransparenzverfahrens nicht hinreichend normenklar an. Zu unspezifisch ist die allgemeine Vorgabe in § 10 Abs. 2 Satz 3 DaTraV, dass das Forschungsdatenzentrum im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik die erforderlichen spezifischen, technischen und organisatorischen Maßnahmen festlegt, um die Datenverarbeitung durch den Nutzungsberechtigten auf das erforderliche Maß zu beschränken und um das Risiko einer Identifizierung einzelner Betroffener zu minimieren. Hierbei bleibt offen, um was für Maßnahmen es sich hierbei handeln könnte. Es ist jedoch angesichts der sehr hohen Sensibilität der vorgehaltenen Daten Sache des Normgebers, die gebotenen Maßnahmen zumindest im Ansatz zu konkretisieren,

> wie hier Bretthauer, Die Verwaltung 54 (2021), 411 (427).

Zudem ist vorzusehen, dass die Sicherheitsanforderungen veröffentlicht werden, um insbesondere eine (fach-)öffentliche Diskussion über mögliche Defizite und Verbesserungspotenziale zu ermöglichen. Eine solche Veröffentlichung sieht beispielsweise § 180 Abs. 3 Satz 2 TKG für den Anforderungskatalog vor, den die Bundesnetzagentur zur Sicherung der bei Telekommunikationsunternehmen auf Vorrat gespeicherten Telekommunikations-Verkehrsdaten erarbeitet.

Schließlich weist § 303e Abs. 5 SGB V, der die Zweckbindung der bereitgestellten Daten regelt, eine Lücke auf. Nach § 303e Abs. 5 Satz 1 Nr. 2 SGB V darf der Nutzungsberechtigte die zugänglich gemachten Daten an Dritte nur weitergeben, wenn das Forschungsdatenzentrum die Weitergabe im Rahmen eines nach § 303 Abs. 2 SGB V zulässigen Nutzungszwecks genehmigt. Jedoch fehlt die gemäß Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO gebotene Vorgabe, dass der Dritte einer Geheimhaltungspflicht unterliegen muss. Diese Vorgabe ist nur für den Nutzungsberechtigten, dem das Forschungsdatenzentrum den unmittelbaren Datenzugang gewährt, in § 303e Abs. 4 Satz 2 SGB V umgesetzt.

3. Rechtsfolge

Insgesamt weist das Datentransparenzverfahren auf allen gesetzlich vorgesehenen Verfahrensstufen Sicherheitsmängel auf. Diese Mängel lassen sich nicht durch eine das Gesetz konkretisierende, zum Teil auch von ihm abweichende Behördenpraxis heilen. Vielmehr sind sie schon aus Gründen der Normenklarheit vom Gesetzgeber zu beheben. Die Regelungen über das Datentransparenzverfahren verletzen darum insgesamt höherrangiges Recht. Insbesondere der Verstoß gegen die unionsrechtlichen Vorgaben führt dazu, dass diese Regelungen unanwendbar sind. Damit fehlt es für die Datenübermittlung durch die Antragsgegnerin an die Datensammelstelle an der erforderlichen Rechtsgrundlage. Die Antragsgegnerin hat diese Übermittlung zu unterlassen.

Der Antragsteller hat einen mit der Unterlassungspflicht der Antragsgegnerin korrespondierenden Unterlassungsanspruch. Zwar findet sich in der DSGVO kein besonderer Unterlassungsanspruch der betroffenen Person. Hieraus wird vereinzelt gefolgert, ein Unterlassungsanspruch bestehe nicht, da das System der Betroffenenrechte in der DSGVO abschließend sei,

> so insbesondere VG Regensburg, Gerichtsbescheid vom 6. August 2020 – RN 9 K 19.1061; Kreße, in: Sydow, DSGVO, Art. 79 Rn. 10 ff.

Diese Rechtsauffassung überzeugt jedoch nicht. Sie hätte zur Folge, dass die betroffene Person gegenüber einer konkret absehbaren zukünftigen Datenverarbeitung, die sie in ihrem Grundrecht auf Datenschutz verletzt, schutzlos gestellt würde. Hieraus ergäbe sich ein Rechtsschutzdefizit, das sich mit dem Rechtmäßigkeitsgrundsatz des Art. 5 Abs. 1 lit. a DSGVO, dem Datenschutzgrundrecht des Art. 8 GRCh und der Rechtsschutzgarantie des Art. 47 GRCh nicht vereinbaren ließe. Dem Rechtmäßigkeitsgrundsatz ist daher ein ungeschriebener Unterlassungsanspruch zu entnehmen,

> für einen datenschutzrechtlichen Unterlassungsanspruch mit unterschiedlicher Begründung die ganz herrschende Meinung, etwa VG Wiesbaden, Beschluss vom 1. Dezember 2021 – 6 L 738/21.WI; LG Frankfurt, Beschluss vom 15. Oktober 2020 – 2-03 O 356/20; Martini, in: Paal/Pauly, DSGVO, Art. 79 Rn. 17; Halder, jurisPR-ITR 4/2021 Anm. 5; ders., jurisPR-ITR 1/2022 Anm. 2; Leibold/Laoutoumai, ZD-Aktuell 2021, 05583.

III. Widerspruch des Antragstellers

Eine Übermittlung von Gesundheitsdaten, die den Antragsteller betreffen, durch die Antragsgegnerin an den Spitzenverband Bund der Krankenkassen ist zudem unzulässig, weil der Antragsteller der Übermittlung in dem Schreiben vom 1. März 2022 wirksam widersprochen hat. Sofern angenommen wird, dass dem Antragsteller nach dem gegenwärtigen Rechtsstand kein Widerspruchsrecht zukommt, verletzen die Rechtsgrundlagen des Datentransparenzverfahrens höherrangiges Recht und sind unanwendbar, weil sie zur Wahrung des Verhältnismäßigkeitsgrundsatzes ein Widerspruchsrecht vorsehen müssten.

1. Widerspruchsrecht aus Art. 21 DSGVO

Der Antragsteller hat mit seinem Schreiben vom 1. März 2022 ein ihm zustehendes Widerspruchsrecht aus Art. 21 DSGVO ausgeübt. Im Einzelnen ist hinsichtlich der jeweils maßgeblichen Regelung nach den Zwecken des Datentransparenzverfahrens zu differenzieren.

a) Datenverarbeitung zu Zwecken der Gesundheitsversorgung und Gesundheitsberichterstattung

Soweit das Datentransparenzverfahren dazu dient, Daten für Zwecke der Planung, Analyse und Evaluation der Gesundheitsversorgung im System der gesetzlichen Krankenversicherung sowie der Gesundheitsberichterstattung

bereitzustellen, bemisst sich das Widerspruchsrecht der betroffenen Person nach Art. 21 Abs. 1 DSGVO.

aa) Anwendbarkeit von Art. 21 Abs. 1 DSGVO

Das Widerspruchsrecht des Art. 21 Abs. 1 DSGVO ist auf das gesamte Datentransparenzverfahren und damit auch die Datenübermittlung von der Antragsgegnerin an den Spitzenverband Bund der Krankenkassen anwendbar, soweit das Datentransparenzverfahren Zwecken der Gesundheitsversorgung und Gesundheitsberichterstattung dient. Die Regelungen über das Datentransparenzverfahren sehen insoweit in ihrer Gesamtheit Datenverarbeitungen zur Wahrnehmung von Aufgaben im öffentlichen Interesse i.S.v. Art. 6 Abs. 1 Satz 1 lit. e DSGVO vor.

Eine Anwendung von Art. 6 Abs. 1 Satz 1 lit. e DSGVO auf die Datenverarbeitungen im Datentransparenzverfahren wird nicht dadurch ausgeschlossen, dass die verarbeiteten Daten überwiegend als Gesundheitsdaten i.S.v. Art. 9 Abs. 1 DSGVO anzusehen sind. Die Verbotsregelung in Art. 9 Abs. 1 DSGVO mit eng auszulegenden Ausnahmetatbeständen in Art. 9 Abs. 2 DSGVO ist keine spezielle Regelung, die Art. 6 Abs. 1 DSGVO verdrängt. Vielmehr sind beide Vorschriften nebeneinander anzuwenden. Nur so kann das Normziel von Art. 9 DSGVO vollumfänglich erreicht werden, bestimmte Datenkategorien mit besonderem Schutz zu versehen. Würde Art. 6 Abs. 1 DSGVO durch Art. 9 DSGVO verdrängt, wären hingegen die besonderen Datenkategorien unter bestimmten Gesichtspunkten sogar schwächer geschützt als andere personenbezogene Daten,

> wie hier für eine parallele Anwendung von Art. 6 Abs. 1 und Art. 9 DSGVO etwa Albers/Veit, in: BeckOK Datenschutzrecht, Art. 9 DSGVO Rn. 11; Weichert, in: Kühling/Buchner, DSGVO/BDSG, Art. 9 DSGVO Rn. 4; diese Frage ist Gegenstand des anhängigen Vorabentscheidungsersuchens des BAG, Beschluss vom 26. August 2021 – 8 AZR 253/20 (A) –, juris, Rn. 28 ff.

Dies zeigt sich gerade auch am Widerspruchsrecht des Art. 21 Abs. 1 DSGVO, das nur anwendbar ist, wenn sich eine Datenverarbeitung auf Art. 6 Abs. 1 Satz1 lit. e oder f DSGVO stützt. Es gibt keinen Grund, warum ein Widerspruchsrecht im Anwendungsbereich des Art. 9 DSGVO nie bestehen sollte. Selbst wenn ein Spezialitätsverhältnis zwischen Art. 9 DSGVO und Art. 6 DSGVO bestünde, müsste zur Vermeidung einer Schutzlücke zumindest das

Widerspruchsrecht des Art. 21 DSGVO auch auf Datenverarbeitungen angewandt werden, die sich nach Art. 9 DSGVO richten,

so Dochow, MedR 2021, 13 (22).

Die Anwendung von Art. 6 Abs. 1 Satz 1 lit. e DSGVO scheitert auch nicht von vornherein daran, dass die Datenverarbeitung im Datentransparenzverfahren datenschutzrechtlich eine Zweckänderung der ursprünglich zu Abrechnungszwecken erhobenen Daten darstellt, für die sich besondere Vorgaben in Art. 6 Abs. 4 DSGVO finden. Nach vorzugswürdiger, wenngleich umstrittener Auffassung treten diese Vorgaben neben das allgemeine Erfordernis einer Verarbeitungserlaubnis aus Art. 6 Abs. 1 DSGVO,

wie hier etwa Albers/Veit, in: BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 107 f.; Heberlein, in: Ehmann/Selmayr, DSGVO, Art. 6 Rn. 48; Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Rn. 12 ff. vor Art. 6 DSGVO; a.A. etwa Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 6 DSGVO Rn. 12.

Selbst wenn man jedoch davon ausgeht, dass eine zweckändernde Datenweiterverarbeitung allein an Art. 6 Abs. 4 DSGVO und nicht an Art. 6 Abs. 1 DSGVO zu messen ist, muss das Widerspruchsrecht aus Art. 21 Abs. 1 DSGVO anwendbar bleiben. Ansonsten würde die datenschutzrechtlich besonders problematische und darum spezifisch regulierte Zweckänderung hinsichtlich des Widerspruchsrechts gegenüber der Datenverarbeitung im Rahmen des ursprünglichen Verarbeitungszwecks privilegiert. Es käme also, ähnlich wie im Verhältnis zu Art. 9 DSGVO, zu einem Wertungswiderspruch, dem durch eine extensive Auslegung von Art. 21 Abs. 1 DSGVO abzuhelfen wäre.

Die im Rahmen des Datentransparenzverfahrens vorgesehenen Datenverarbeitungen zu den Zwecken der Planung, Analyse und Evaluation der Gesundheitsversorgung im System der gesetzlichen Krankenversicherung sowie der Gesundheitsberichterstattung sind – zumindest für das Widerspruchsrecht des Art. 21 Abs. 1 DSGVO – insgesamt dem Erlaubnistatbestand des Art. 6 Abs. 1 Satz 1 lit. e DSGVO zuzuordnen. Hiervon ging ausweislich der Gesetzesbegründung auch der Gesetzgeber aus,

vgl. zu § 303b SGB V BT-Drs. 19/13438, S. 72.

Allerdings sind die Krankenkassen nach § 303b Abs. 1 Satz 1 SGB V zur Datenübermittlung an die Datensammelstelle verpflichtet. Wird nur dieser Verarbeitungsschritt isoliert betrachtet, so liegt es nahe, als unionsrechtliche Verarbeitungsregelung Art. 6 Abs. 1 Satz 1 lit. c DSGVO und nicht lit. e dieser Vorschrift heranzuziehen,

so Weichert, MedR 2020, 539 (542 f.).

Jedoch ist eine solche isolierte Betrachtung jedenfalls für die Frage, ob das Widerspruchsrecht des Art. 21 Abs. 1 DSGVO anwendbar ist, nicht angemessen. Diese Frage muss vielmehr in einer Gesamtschau des Verarbeitungszusammenhangs beantwortet werden, der durch den Verarbeitungszweck definiert wird.

Die Datenübermittlung durch die Krankenkassen an die Datensammelstelle ist der erste Schritt eines mehrstufigen Verfahrens, das darauf gerichtet ist, den Nutzungsberechtigten gemäß § 303e SGB V Zugang zu den übermittelten Daten zu verschaffen. Allein dieses Anliegen rechtfertigt alle vorhergehenden Verarbeitungsschritte, die ohne den Datenzugang der Nutzungsberechtigten sinnlos und darum nicht erforderlich wären. Für die Nutzungsberechtigten handelt es sich bei dem Datenzugang um eine Datenverarbeitung, die in ihrem Ermessen steht und darum Art. 6 Abs. 1 Satz 1 lit. e DSGVO unterfällt.

Würde die Anwendbarkeit von Art. 21 Abs. 1 DSGVO für jede einzelne Datenverarbeitungshandlung gesondert bestimmt, könnte dies den Schutz der betroffenen Person aushöhlen. Die betroffene Person könnte dann bei den Nutzungsberechtigten Widerspruch gegen eine Datennutzung einlegen, hätte jedoch keinerlei Handhabe gegen die vorgelagerten Verarbeitungsschritte. Hierdurch würde erstens die Ausübung des Widerspruchsrechts unzumutbar erschwert, da die betroffene Person sich an eine für sie nicht überschaubare Vielzahl potenzieller Nutzungsberechtigter wenden müsste, statt auf der vorgelagerten Stufe der Datenübermittlung einen einzigen Ansprechpartner für einen Widerspruch zu haben. Zweitens wäre ein Widerspruchsrecht gegenüber den Nutzungsberechtigten sinnlos, da diese nach dem gesetzlichen Schutzkonzept gerade nicht in der Lage sein sollen und jedenfalls nicht berechtigt sind, die betroffene Person zu identifizieren, sodass sie bei rechtskonformem Verhalten einem begründeten Widerspruch überhaupt nicht abhelfen könnten. Drittens würde ein Widerspruchsrecht, das erst bei den Nutzungsberechtigten ansetzt, die vor der Datennutzung liegende Übermittlung und Bevorratung der Transparenzdaten unberührt lassen. Diese vorgelagerten Schritte erlangen ihren Sinn jedoch nur aus der nachgelagerten Datennutzung. Dürfen die Daten nicht genutzt werden, so gibt es keinen

Grund, sie überhaupt in das Datentransparenzverfahren einzuführen. Ein Widerspruchsrecht muss sich darum zwingend auch auf die vorgelagerten Verarbeitungsschritte erstrecken,

> zum Widerspruchsrecht aus Art. 21 Abs. 6 DSGVO wie hier Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 29. Tätigkeitsbericht, S. 51.

Da die Datenübermittlung mit Blick auf die Anwendung des Widerspruchsrechts als unselbstständiger Teil des übergreifenden Datentransparenzverfahrens anzusehen ist und die Datennutzung im Ermessen der Nutzungsberechtigten steht, ist das Widerspruchsrecht auch nicht nach § 84 Abs. 5 Alt. 2 SGB X ausgeschlossen.

bb) Voraussetzungen des Widerspruchsrechts

Voraussetzung des Widerspruchsrechts ist nach Art. 21 Abs. 1 Satz 1 DSGVO, dass die betroffene Person gegen eine grundsätzlich zulässige Datenverarbeitung aufgrund ihrer besonderen Situation spezifische Gründe vorbringt. Der Antragsteller erfüllt diese Voraussetzung.

Die besondere Situation des Antragstellers ergibt sich aus zwei Umständen. Erstens besteht für ihn ein besonders hohes Risiko einer Reidentifikation aufgrund der im Datentransparenzverfahren verarbeiteten Gesundheitsdaten. Bereits wegen seiner seltenen Blutgerinnungsstörung gehört der Antragsteller einer kleinen Teilmenge der betroffenen Personen an. Für ganz Deutschland wird von etwa 6.000 an Hämophilie A erkrankten Personen ausgegangen, von denen die Hälfte an einer schweren Form leidet. Dabei ist anzunehmen, dass die allermeisten, allerdings nicht alle Erkrankten gesetzlich krankenversichert sind. Hinzu kommt die psychische Erkrankung des Antragstellers, durch die er sich auch aus dem kleinen Kreis der an Hämophilie A erkrankten Personen heraushebt. Es erscheint naheliegend, dass allenfalls sehr wenige gesetzlich krankenversicherte Personen bundesweit das spezifische Krankheitsbild des Antragstellers aufweisen. Spätestens wenn die nach § 303b Abs. 1 Satz 1 Nr. 1 SGB V i.V.m. § 3 Abs. 1 Nr. 1 DaTraV zu übermittelnden Angaben zum Geburtsjahr und zur Postleitzahl seines Wohnorts hinzugenommen werden, dürfte der Antragsteller im gesamten Datenbestand des Forschungsdatenzentrums eine einmalige Merkmalskombination aufweisen.

Zweitens liegen schwere Nachteile durch eine Reidentifikation für den Antragsteller besonders nahe. Um diese Nachteile zu ermitteln, muss wiederum berücksichtigt werden, dass das Datentransparenzverfahren ein spezifisches Sicherheitsrisiko birgt. Selbst wenn entgegen der oben

begründeten Auffassung angenommen wird, dass die Rechtsgrundlagen des Datentransparenzverfahrens den unions- und verfassungsrechtlichen Vorgaben zum Schutz der Vertraulichkeit und Integrität der verarbeiteten Daten genügen, lassen sich jedenfalls Sicherheitslücken nie ausschließen. Sowohl die Schwerbehinderung des Antragstellers, die sich aus den zu übermittelnden Gesundheitsdaten folgern lässt, als auch seine psychische Krankheit bergen ein sehr hohes Risiko von Diskriminierungen und Stigmatisierungen, wenn die Daten an Unbefugte gelangen. Nachteile könnten sich für ihn beispielsweise im Verhältnis zu Versicherungsunternehmen, potenziellen Arbeitgebern oder Personen aus seinem privaten Umfeld ergeben. Auch Erpressungsversuche durch Kriminelle liegen nicht fern. Insgesamt ist der Antragsteller mit Blick auf die gesetzlich vorgesehenen Datenverarbeitungen darum als höchst vulnerabler Betroffener anzusehen.

Des Weiteren ist gemäß Art. 21 Abs. 1 Satz 2 DSGVO (und gleichläufig § 84 Abs. 5 Alt. 1 SGB X) negative Voraussetzung des Widerspruchsrechts, dass kein zwingendes öffentliches Interesse an der Datenverarbeitung die gegenläufigen Interessen der betroffenen Person überwiegt. Dies lässt sich für die Datenverarbeitung im Datentransparenzverfahren zumindest nicht generell annehmen.

Die Zwecke der Planung, Analyse und Evaluation der Gesundheitsversorgung im System der gesetzlichen Krankenversicherung sowie der Gesundheitsberichterstattung, denen das Datentransparenzverfahren dient, können zwar durchweg beträchtliches Gewicht haben. Wie schwer diese Zwecke im Rahmen der gebotenen Abwägung wiegen, lässt sich jedoch nicht pauschal angeben, sondern hängt auch von dem konkreten Auswertungsprojekt ab, für das die Daten genutzt werden sollen. Es liegt jedenfalls fern, dass die Nutzungszwecke zwingend in jedem Einzelfall schwerer wiegen als das besonders gewichtige Widerspruchsinteresse des Antragstellers.

Im Gegenteil sprechen sogar gute Gründe dafür, dass das Widerspruchsinteresse des Antragstellers die gegenläufigen öffentlichen Belange der Gesundheitsplanung und Gesundheitsberichterstattung *immer* überwiegt. Denn die im Datentransparenzverfahren vorgesehene Datenbevorratung führt generell zu einem hohen Risiko für die betroffenen Personen, wie bereits oben im Rahmen der Ausführungen zur Datensicherheit begründet wurde. Jedenfalls wenn dann noch, wie im Fall des Antragstellers, eine besondere individuelle Vulnerabilität hinzutritt, kann der betroffenen Person nicht mehr zugemutet werden, dieses Risiko gegen ihren erklärten

Willen hinzunehmen. Daher muss solchen vulnerablen Personen generell ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten im Datentransparenzverfahren zustehen.

Der Antragsteller verkennt nicht, dass vulnerable Personen durch einen Widerspruch im Einzelfall legitime und gewichtige öffentliche Erkenntnisinteressen beeinträchtigen können. Allerdings werden zum einen Daten gerade über solche Personen für viele Auswertungen nicht zwingend benötigt. Dies ist immer dann der Fall, wenn die Auswertung keinen spezifischen Bezug zu den besonderen Eigenschaften einer vulnerablen Person aufweist. In solchen Fällen kommt es zu keiner signifikanten Beeinträchtigung öffentlicher Interessen, wenn Daten über diese Person nicht zur Verfügung stehen. Zum anderen resultiert eine mögliche spürbare Beeinträchtigung nicht aus dem einzelnen Widerspruch, sondern erst aus einer Häufung solcher Widersprüche, die eine kritische Schwelle überschreitet. Das Gewicht der Beeinträchtigung öffentlicher Erkenntnisinteressen ergibt sich darum erst aus der Prognose, dass dann, wenn vulnerablen Personen ein Widerspruchsrecht zuerkannt wird, ein kritischer Anteil dieses Personenkreises von diesem Recht tatsächlich Gebrauch machen wird. Diese Prognose liegt jedoch fern. Aus der verhaltensökonomischen Forschung ist das Phänomen des sogenannten Status-Quo-Bias bekannt. Danach bevorzugen Menschen bei einer Optionenwahl die Option, die am wenigsten Aufwand verursacht. Gibt es bei einer solchen Wahl eine Voreinstellung (sogenannter Default), so bleiben die meisten Wählenden hierbei,

> vgl. hierzu grundlegend Samuelson/Zeckhauser, Journal of Risk and Uncertainty 1988, 7 ff.; zu politischen Gestaltungsempfehlungen, die dieses Phänomen und weitere Biases zur gezielten Verhaltenssteuerung ausnutzen, grundlegend Thaler/Sunstein, Nudge: Wie man kluge Entscheidungen anstößt, 2009.

Es ist darum davon auszugehen, dass von einem bestehenden Widerspruchsrecht nur eine Minderheit der vulnerablen Personen Gebrauch machen wird, sodass sich negative Auswirkungen auf öffentliche Erkenntnisinteressen in Grenzen halten dürften. Der Antragsteller verlangt hingegen ausdrücklich nicht, dass die Datenübermittlung an eine positive Einwilligung der betroffenen Person gekoppelt wird, wie dies § 75 Abs. 1 Satz 2 SGB X für die Weiterverarbeitung von Sozialdaten für Forschungs- und Planungszwecke grundsätzlich vorsieht,

für ein Einwilligungserfordernis hingegen Platzer, NZS 2020, 289 (294).

Im Übrigen kann ein behutsamer und bewusster Umgang mit dem Widerspruchsrecht durch entsprechende Publikumsinformationen öffentlicher Stellen gefördert werden, die etwa den Nutzen der Gesundheitsdaten für die Gesundheitsversorgung und das – allerdings noch herzustellende – hohe Niveau der Datensicherheit hervorheben könnten.

b) Datenverarbeitung zu Forschungszwecken

Soweit das Datentransparenzverfahren Forschungszwecken dient, ist Rechtsgrundlage des Widerspruchsrechts der betroffenen Person Art. 21 Abs. 6 DSGVO. Diese Vorschrift geht in ihrem Anwendungsbereich Art. 21 Abs. 1 DSGVO vor. Bereits die Datenübermittlung von den Krankenkassen an die Datensammelstelle dient (auch) der wissenschaftlichen Forschung als einem Nutzungszweck, der dem gesamten Datentransparenzverfahren zugrunde liegt. Ebenso wie im Rahmen von Art. 21 Abs. 1 DSGVO würde eine Aufspaltung des Verfahrens in einzelne Verarbeitungsschritte das Widerspruchsrecht sinnwidrig leerlaufen lassen. Für die Anwendbarkeit von Art. 21 Abs. 6 DSGVO kommt es im Übrigen anders als bei Art. 21 Abs. 1 DSGVO nicht auf die Rechtsgrundlage der Verarbeitung an.

Das Widerspruchsrecht ist nicht durch eine gesetzliche Regelung ausgeschlossen. Zwar erlaubt Art. 89 Abs. 2 DSGVO den Mitgliedstaaten, bei Datenverarbeitungen zu Forschungszwecken Ausnahmen von bestimmten datenschutzrechtlichen Betroffenenrechten, darunter auch Art. 21 DSGVO, vorzusehen. Eine auf dieser Grundlage ergehende Ausnahmeregelung muss aber hinreichend deutlich regeln, von welchem Recht unter welchen Voraussetzungen und in welchen Grenzen abgewichen wird. Hingegen nehmen §§ 303a ff. SGB V das Widerspruchsrecht an keiner Stelle ausdrücklich in Bezug. Auch ansonsten findet sich nirgends eine Regelung, die das Widerspruchsrecht des Art. 21 Abs. 6 DSGVO gerade mit Blick auf das Datentransparenzverfahren beschränkt. Die Ausnahmeregelung in § 84 Abs. 5 SGB bezieht sich nur auf das Widerspruchsrecht des Art. 21 Abs. 1 DSGVO. Die forschungsbezogene Ausnahmeregelung in § 27 Abs. 2 Satz 1 BDSG ist gemäß § 35 Abs. 2 Satz 1 SGB I im Bereich des Sozialdatenschutzes nicht anwendbar.

Aus der besonderen Situation des Antragstellers ergibt sich ein Widerspruchsgrund. Insoweit kann auf die Darlegungen zu Art. 21 Abs. 1 Satz

1 DSGVO verwiesen werden, da für Art. 21 Abs. 6 DSGVO derselbe Maßstab gilt,

> vgl. statt aller Munz, in: Taeger/Gabel, DSGVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 21 DSGVO Rn. 58.

Der Widerspruch ist auch nicht – jedenfalls nicht generell – aufgrund gegenläufiger öffentlicher Interessen ausgeschlossen.

Nach Art. 21 Abs. 6 DSGVO besteht kein Widerspruchsrecht, wenn die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Ob eine Forschungseinrichtung mit einem Forschungsvorhaben eine im öffentlichen Interesse liegende Aufgabe erfüllt, lässt sich nicht pauschal beurteilen. So reicht hierzu die allgemeine Aufgabe der öffentlichen Hochschulen nicht aus, zur wissenschaftlichen Forschung beizutragen (etwa aus § 3 Abs. 1 HessHG). Ansonsten liefe das Widerspruchsrecht gegenüber diesen Einrichtungen von vornherein leer. Maßgeblich kommt es vielmehr auf eine Würdigung des einzelnen Forschungsvorhabens an,

> ähnlich Forgó, in: BeckOK Datenschutzrecht, Art. 21 DSGVO Rn. 31; für eine Regelvermutung zugunsten eines öffentlichen Interesses hingegen Caspar, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art 21 DSGVO Rn. 39.

Zudem muss die Datenverarbeitung für den jeweiligen Forschungszweck erforderlich sein. Das mit dem Forschungszweck verfolgte öffentliche Interesse darf also nicht gleichwertig mit anderen Mitteln (etwa mit anonymisierten Daten oder auf der Grundlage eines reduzierten Datenbestands) erreichbar sein,

> Kamann/Braun, in: Ehmann/Selmayr, DSGVO, Art. 21 Rn. 65.

Auch die Erforderlichkeit lässt sich nicht generell, sondern nur mit Blick auf das einzelne Forschungsvorhaben beurteilen. So wird es bei breit angelegten Reihenuntersuchungen vielfach unerheblich sein, wenn ein gewisser (niedriger) Anteil der Versichertendaten aufgrund von Widersprüchen nicht zur Verfügung steht. Bei spezifisch auf bestimmte seltene Krankheiten ausgerichteten Studien kann es hingegen auf eine möglichst weitreichende Erfassung des betroffenen Personenkreises ankommen.

Nach zutreffender, wenngleich umstrittener Auffassung bedarf es darüber hinaus auch im Rahmen von Art. 21 Abs. 6 DSGVO einer Interessenabwägung, um die kollidierenden Grundrechte (Datenschutz

einerseits, Wissenschaftsfreiheit andererseits) einander zuzuordnen. Das Erfordernis einer Abwägung ergibt sich zwar nicht ausdrücklich aus dem Wortlaut der Norm, folgt aber aus dem in Art. 52 Abs. 1 Satz 2 GRCh niedergelegten Verhältnismäßigkeitsgrundsatz,

> wie hier etwa Kamann/Braun, in: Ehmann/Selmayr, DSGVO, Art. 21 Rn. 65; Martini, in: Paal/Pauly, DSGVO/BDSG, Art. 21 DSGVO Rn. 60.

Im Rahmen dieser Abwägung ist die datenschutzrechtliche Privilegierung wissenschaftlicher Forschungszwecke zu beachten.

Gleichwohl ergibt die angezeigte Abwägung auch für die Fälle, in denen die Verarbeitung der Gesundheitsdaten des Antragstellers in personenbezogener oder personenbeziehbarer Form überhaupt erforderlich ist, um ein öffentliches Forschungsinteresse zu erreichen, einen Vorrang des Datenschutzinteresses des Antragstellers. Gründe hierfür sind zum einen die außerordentliche Sensibilität der Daten, die bei dem Forschungsdatenzentrum bevorratet werden, nach Art, Umfang und Aussagekraft, zum anderen die besondere Vulnerabilität des Antragstellers. Insoweit kann auf die Ausführungen zu Art. 21 Abs. 1 Satz 2 DSGVO verwiesen werden,

> nach Auffassung von Platzer, NZS 2020, 289 (293), sind an ein überwiegendes öffentliches Forschungsinteresse „angesichts der Bedeutung des gefährdeten individuellen Rechtsgutes außerordentlich hohe Anforderungen zu stellen."

c) Rechtsfolge

Oben wurde begründet, dass der Antragsteller der Übermittlung der ihn betreffenden Daten durch die Antragsgegnerin an den Spitzenverband Bund der Krankenkassen generell widersprechen kann. Auf der Grundlage dieser Rechtsauffassung muss die Datenübermittlung seit dem am 1. März 2022 erhobenen Widerspruch unterbleiben. Für das Widerspruchsrecht aus Art. 21 Abs. 1 Satz 1 DSGVO wird dies in Art. 21 Abs. 1 Satz 2 DSGVO ausdrücklich angeordnet. Für das Widerspruchsrecht aus Art. 21 Abs. 6 DSGVO kann sich nichts anderes ergeben,

> wie hier Martini, in: Paal/Pauly, DSGVO/BDSG, Art. 21 DSGVO Rn. 61.

Wird hingegen angenommen, dass sich in bestimmten Fallkonstellationen ein öffentliches Nutzungsinteresse gegen das Datenschutzinteresse des Antragstellers durchsetzen kann, so muss dem Antragsteller zumindest ein

beschränktes Widerspruchsrecht eingeräumt werden. Denn nicht alle nach § 303e SGB V zulässigen Datennutzungen dienen einem so gewichtigen öffentlichen Interesse, dass das Widerspruchsinteresse des Antragstellers in jedem Fall und vollumfänglich zurückstehen muss.

Ein beschränkter Widerspruch ließe sich in unterschiedlicher Weise realisieren. So könnte sich ein gegenüber der Krankenkasse geltend gemachter Widerspruch etwa auf bestimmte Datenkategorien, Kategorien von Forschungsprojekten oder Zugangsmodalitäten beziehen. Einem solchen Widerspruch wäre etwa durch eine Ausnahme bestimmter Daten von der Übermittlung oder durch eine Markierung der Daten, die ihre Nutzung beschränkt, Rechnung zu tragen. Denkbar wäre auch, eine Widerspruchsmöglichkeit erst auf der nachgelagerten Ebene der Datenbereitstellung zu eröffnen. Hierzu müsste bei dem Forschungsdatenzentrum ein Verfahren eingerichtet werden, das eine auf die einzelnen Nutzungsprojekte bezogene Information der betroffenen Personen vorsieht und ihnen einen gleichfalls projektbezogenen Widerspruch ermöglicht.

Eine beschränkte Widerspruchsmöglichkeit steht gegenwärtig jedoch nicht zur Verfügung. Denn die normativen Grundlagen des Datentransparenzverfahrens sehen eine umfassende Datenübermittlung an das Forschungsdatenzentrum vor. Sie ermöglichen keine Beschränkungen der Datenübermittlung an das Forschungsdatenzentrum oder der Datenbereitstellung durch das Forschungsdatenzentrum aus besonderen persönlichen Gründen. Jedenfalls solange dieser Zustand anhält, ist dem Antragsteller ein umfassendes Widerspruchsrecht gegen die Datenübermittlung durch die Antragsgegnerin an die Datensammelstelle zuzubilligen.

2. Hilfsweise: Erforderlichkeit eines gesetzlichen Widerspruchsrechts

Wenn entgegen der oben begründeten Rechtsauffassung angenommen wird, dass die Widerspruchsrechte aus Art. 21 Abs. 1 und 6 DSGVO auf die Datenübermittlungen von den Krankenkassen an die Datensammelstelle nicht anwendbar sind, so ist der Gesetzgeber verpflichtet, ein Widerspruchsrecht der betroffenen Personen zu schaffen. Diese Regelungspflicht ergibt sich aus dem aufgrund von Art. 6 Abs. 3 Satz 3 und 4 und Art. 9 Abs. 2 lit. h, i und j DSGVO sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu beachtenden Verhältnismäßigkeitsgrundsatz. Da die gegenwärtigen Rechtsgrundlagen des Datentransparenzverfahrens kein gesetzliches Widerspruchsrecht vorsehen,

verletzen diese Regelungen insgesamt höherrangiges Recht und sind unanwendbar.

Ein gesetzliches Widerspruchsrecht gegenüber den Krankenkassen wird zumindest für die Fälle benötigt, in denen der betroffenen Person gegenüber einem Nutzungsberechtigten ein Widerspruchsrecht nach Art. 21 Abs. 1 Satz 1 oder Abs. 6 DSGVO zusteht. In diesen Fällen kann die betroffene Person, wie oben dargelegt, ihr Widerspruchsrecht faktisch nicht wirksam ausüben. Der Gesetzgeber muss darum einen Widerspruchsmechanismus schaffen, der einen tatsächlich effektiven Widerspruch ermöglicht. Hierzu muss er den Versicherten ermöglichen, bereits der Datenübermittlung an die Datensammelstelle zu widersprechen,

> wie hier Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 29. Tätigkeitsbericht, S. 51.

Da die nach Art. 21 Abs. 1 und Abs. 6 DSGVO widerspruchsberechtigten Personen, wie oben ausgeführt, jeder Datennutzung widersprechen könnten, besteht kein Grund, ihre Daten überhaupt im Datentransparenzverfahren zu verarbeiten.

Wird entgegen der oben begründeten Auffassung davon ausgegangen, dass selbst Versicherte, in deren Person besondere Widerspruchsgründe im Sinne von Art. 21 Abs. 1 Satz 1 und Abs. 6 DSGVO bestehen, der Datennutzung nicht in jedem Fall widersprechen können, so muss der gesetzliche Widerspruchsmechanismus zumindest einen beschränkten Widerspruch ermöglichen. Hierzu könnten die Krankenkassen, wie oben erörtert, bestimmte Datenkategorien von der Übermittlung ausnehmen oder die übermittelten Daten markieren, damit der Widerspruch bei der Datennutzung berücksichtigt wird. Denkbar wäre auch, das Datentransparenzverfahren so umzugestalten, dass den Versicherten zumindest vor besonders sensiblen Datennutzungen (etwa vor jeder Bereitstellung pseudonymisierter Einzeldatensätze) eine auf die einzelne Datennutzung bezogene Widerspruchsmöglichkeit eingeräumt wird. Ein beschränkter Widerspruch könnte je nach dem eingerichteten Mechanismus an die Krankenkassen oder an das Forschungsdatenzentrum zu richten sein. Mithin bestünden bei der Ausgestaltung eines beschränkten Widerspruchsrechts Regelungsspielräume, deren Grenzen im vorliegenden Verfahren nicht im Einzelnen zu klären sind.

Im Übrigen sprechen gute Gründe dafür, dass der Gesetzgeber aufgrund des Verhältnismäßigkeitsgrundsatzes sogar *allen* Versicherten – und damit erst recht auch besonders vulnerablen Personen wie dem Antragsteller – ein

Widerspruchsrecht gegen die Bereitstellung sie betreffender Gesundheitsdaten im Datentransparenzverfahren einräumen muss,

> in diese Richtung auch Schulz, SGb 2020, 536 (541); Schrahe/Städter, DuD 2020, 713 (714); für ein projektspezifisches Widerspruchsrecht aller betroffenen Personen Weichert, MedR 2020, 539 (543); Bretthauer, Die Verwaltung 54 (2021), 411 (426); vgl. ferner für ein ungeschriebenes Widerspruchsrecht im Rahmen von § 27 BDSG Spitz/Jungkunz/Schickhardt/Cornelius, MedR 2021, 499 (503).

Dies ergibt sich aus der äußerst hohen Eingriffsintensität der im Datentransparenzverfahren gesetzlich vorgesehenen Datenverarbeitungen. Diese beziehen sich, wie oben ausgeführt, auf äußerst sensible Daten in einem äußerst großen Umfang. Die Sicherheit der Daten ist nach dem derzeitigen Rechtsstand, wie gleichfalls oben ausgeführt, nicht auf einem hinreichenden Niveau gewährleistet. Selbst wenn die gesetzlichen Vorgaben für die Datensicherheit verbessert würden, verbliebe jedoch ein Risiko, das den betroffenen Versicherten nicht gegen ihren Willen zugemutet werden kann. Zumindest aber ist die Zumutbarkeitsgrenze überschritten, wenn die bevorrateten Daten gegen den Willen der betroffenen Person in Form pseudonymisierter Einzeldatensätze bereitgestellt werden. Jedenfalls dieser besonders riskanten Bereitstellungsform muss die betroffene Person widersprechen können.

Gegen das Erfordernis eines allgemeinen Widerspruchsrechts lässt sich nicht anführen, dass Art. 21 Abs. 1 und Abs. 6 DSGVO einen Widerspruch nur unter besonderen Voraussetzungen ermöglichen. Diese Normen sind nicht als abschließende Regelungen zu verstehen. Sie sind auf Datenverarbeitungen zugeschnitten, die im Normalfall unabhängig vom Willen der betroffenen Person gerechtfertigt werden können, und sollen Härten in Sonderfällen ausgleichen, die vom Normalfall deutlich abweichen,

> vgl. statt aller Herbst, in: Kühling/Buchner, DSGVO/BDSG, Art. 21 DSGVO Rn. 1.

Hiervon zu unterscheiden ist die hier vorliegende Fallkonstellation, in der den betroffenen Personen eine bestimmte Datenverarbeitung gegen ihren Willen generell nicht zugemutet werden kann. Über diese Fallkonstellation sagt Art. 21 DSGVO schlicht nichts aus. Sie ist vielmehr im Rahmen von Art. 6 und Art. 9 DSGVO anhand des allgemeinen Verhältnismäßigkeitsgrundsatzes zu bewältigen.

Derzeit besteht überhaupt keine gesetzliche Widerspruchsmöglichkeit. Hierbei handelt es sich jedoch um einen wesentlichen Baustein eines Datentransparenzregimes, das den Datenschutzrechten der betroffenen Personen hinreichend Rechnung trägt. Ohne jegliches Widerspruchsrecht ist die Datenverarbeitung im Datentransparenzverfahren unverhältnismäßig. Die Regelungen über das Datentransparenzverfahren sind darum insgesamt unanwendbar, sodass die Übermittlung der den Antragsteller betreffenden Daten durch die Antragsgegnerin an die Datensammelstelle mangels einer anwendbaren Übermittlungsregelung unzulässig ist.

IV. Pflicht zur Einschränkung der Verarbeitung

Der Anordnungsanspruch des Antragstellers ergibt sich schließlich auch aus Art. 18 Abs. 1 lit. d DSGVO. Nach dieser Vorschrift kann eine betroffene Person verlangen, dass der Verantwortliche die Verarbeitung der sie betreffenden Daten einschränkt, wenn die betroffene Person gemäß Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Der Antragsteller hat mit seinem Schreiben vom 1. März 2022 der Datenübermittlung an die Datensammelstelle widersprochen und sich dabei auch auf Art. 21 Abs. 1 DSGVO gestützt. Da die Datenübermittlung nur entweder vollständig durchgeführt werden oder vollständig unterbleiben kann, erstreckt sich dieser Widerspruch auf den gesamten Übermittlungsvorgang. Der Anwendungsbereich des Art. 21 Abs. 1 DSGVO ist eröffnet, da – wie oben näher ausgeführt – die Datenübermittlung auf Art. 6 Abs. 1 Satz 1 lit. e DSGVO beruht und der Antragsteller sich auf eine besondere persönliche Situation berufen kann, deretwegen die Übermittlung seine Rechte besonders intensiv beeinträchtigt.

Bislang ist nicht verbindlich geklärt, ob die berechtigten Gründe der Antragsgegnerin gegenüber denen des Antragstellers überwiegen. Eine solche Klärung kann im Sinne von Art. 18 Abs. 1 lit. d DSGVO auch nicht im vorliegenden vorläufigen Rechtsschutzverfahren erfolgen. Das Abwägungsergebnis steht vielmehr erst dann fest, wenn über den (datenschutzrechtlichen) Widerspruch bestands- oder rechtskräftig entschieden ist. Da derzeit noch das (verfahrensrechtliche) Widerspruchsverfahren gegen die Weigerung der Antragsgegnerin läuft, ist eine verbindliche Klärung nicht konkret absehbar. Der Antragsteller wird, falls erforderlich, den Rechtsweg auch in der Hauptsache beschreiten und den Instanzenzug ausschöpfen.

Gemäß Art. 18 Abs. 2 DSGVO darf die Antragsgegnerin derzeit die Daten, auf die sich der Widerspruch bezieht, nicht verarbeiten, insbesondere also nicht an die Datensammelstelle übermitteln. Entgegen dem Vorbringen der Antragsgegnerin in ihrem Schreiben vom 12. April 2022 liegt auch keiner der Ausnahmetatbestände aus dieser Norm vor. Insbesondere ist die Datenübermittlung nicht aus Gründen eines wichtigen öffentlichen Interesses erlaubt.

Die Ausnahmetatbestände des Art. 18 Abs. 2 DSGVO erfassen in den Fällen des Art. 18 Abs. 1 lit. d DSGVO eine Situation, in der zum einen eine Datenverarbeitung nach den allgemeinen Regelungen in Art. 6 DSGVO grundsätzlich zulässig ist, zum anderen die betroffene Person gewichtige besondere Gründe vorgebracht hat, die gleichwohl gegen die Verarbeitung sprechen. Art. 18 DSGVO würde ausgehöhlt, wenn der Verantwortliche sich – wie es die Antragsgegnerin in ihrem Schreiben vom 12. April 2022 in der Sache unternommen hat – nun schlicht wiederum auf ihre allgemeine Datenverarbeitungserlaubnis berufen könnte, um die vorgeschriebene Einschränkung der Verarbeitung zu umgehen. Das wichtige öffentliche Interesse nach Art. 18 Abs. 2 DSGVO ist daher eng zu verstehen und darf nicht einfach mit dem stets erforderlichen allgemeinen Interesse an der Datenverarbeitung gleichgesetzt werden.

Insbesondere in den Fällen des Art. 18 Abs. 1 lit. d DSGVO ist ein wichtiges öffentliches Interesse nur anzuerkennen, wenn die beabsichtigte Verarbeitung nicht lediglich einem erheblichen Interesse dient, sondern zudem zeitkritisch ist. Art. 18 Abs. 1 lit. d DSGVO enthält eine Übergangsregelung für einen begrenzten Zeitraum, in dem die Berechtigung eines geltend gemachten Widerspruchs geklärt wird. In der Regel kann auch ein gewichtiges öffentliches Interesse für diesen Zeitraum zurückgestellt werden. Anders kann es liegen, wenn das materielle Ziel der Verarbeitung durch Zeitablauf verfehlt zu werden droht. In einem solchen Eilfall kann das Verarbeitungsinteresse das durch Art. 18 Abs. 2 DSGVO geschützte Interesse am einstweiligen Erhalt des Status Quo überwiegen.

Hier ist für einen solchen Eilfall nichts ersichtlich. Werden die Daten nicht sogleich, sondern erst nach abschließender Prüfung des Widerspruchs übermittelt, so stehen sie ab dieser Übermittlung vollumfänglich für die Weiterverarbeitung im Datentransparenzverfahren zur Verfügung. Durch die Verzögerung der Datenübermittlung mögen sie für einzelne Auswertungsprojekte fehlen. Konkret absehbar ist ein solcher Verzögerungsnachteil jedoch nicht. Er wöge auch nicht besonders schwer, da

es für die allermeisten Auswertungsprojekte nicht gerade auf die Daten des Antragstellers ankommt. Das verbleibende Restrisiko einer überhaupt spürbaren Beeinträchtigung öffentlicher Verarbeitungsinteressen durch die Verzögerung der Übermittlung ist angesichts des gewichtigen Stillhalteinteresses des Antragstellers, dem durch die Datenübermittlung irreversible Nachteile drohen, hinnehmbar.

E. Anordnungsgrund

Für die beantragte einstweilige Anordnung besteht auch ein Anordnungsgrund. Dieser folgt daraus, dass die jederzeit und spätestens zum 1. Oktober 2022 drohende Datenübermittlung einen für sich genommen nicht reversiblen Eingriff in die Grundrechte des Antragstellers aus Art. 7 und Art. 8 GRCh sowie aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bewirken würde. Zudem drohen aufgrund einer Übermittlung weitere nachteilige Folgen, die sich gleichfalls in vielen Fällen nicht mehr rückgängig machen ließen. Durch die Übermittlung gibt die Antragsgegnerin die Daten aus der Hand und kann die weitere Datenverarbeitung nicht mehr beeinflussen. Ab diesem Zeitpunkt werden die Daten zentral verarbeitet, zunächst bei der Datensammelstelle und anschließend bei dem Forschungsdatenzentrum, was – wie oben ausgeführt – ein erhebliches, für den Antragsteller nicht hinzunehmendes Sicherheitsrisiko begründet. Zudem stehen die Daten ab der zeitlich nicht absehbaren Weiterübermittlung an das Forschungsdatenzentrum für Nutzungen durch die Nutzungsberechtigten zur Verfügung, die weitere Risiken begründen können, was gleichfalls oben näher ausgeführt wurde.

Dem Erlass der einstweiligen Anordnung steht nicht entgegen, dass das Bundesverfassungsgericht einen Antrag auf Erlass einer einstweiligen Anordnung nach § 32 BVerfGG gegen die Vorschriften über das Datentransparenzverfahren abgelehnt hat,

> BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 19. März 2020 – 1 BvQ 1/20.

Unmittelbar hat der Beschluss des Bundesverfassungsgerichts für das vorliegende Verfahren keine Bindungswirkung. Er taugt auch nicht im Sinne einer Rechtserkenntnisquelle als Vorbild für die Behandlung des vorliegenden Eilantrags. Denn zwischen dem vorliegenden Verfahren und dem Verfahren vor dem Bundesverfassungsgericht bestehen drei erhebliche Unterschiede, die eine Übertragung der Erwägungen des Bundesverfassungsgerichts auf dieses Verfahren ausschließen.

Erstens haben beide Verfahren unterschiedliche Gegenstände. Der Eilantrag vor dem Bundesverfassungsgericht zielte darauf ab, das Inkrafttreten der Regelungen über das Datentransparenzverfahren insgesamt, also für alle Hoheitsträger und betroffenen Personen, hinauszuschieben. Eine solche Eilentscheidung berührt unmittelbar die Normsetzungskompetenz des demokratisch legitimierten Gesetzgebers und damit die verfassungsrechtliche Gewaltengliederung. Deshalb ergehen einstweilige Anordnungen, die sich

unmittelbar gegen ein Gesetz richten, nach ständiger Rechtsprechung des Bundesverfassungsgerichts nur unter besonders strengen Voraussetzungen,

vgl. etwa BVerfGE 140, 99 (106 f.); 157, 394 (402 f.).

Ob das Bundesverfassungsgericht diese Voraussetzungen hinsichtlich der Regelungen über das Datentransparenzverfahren überzeugend gehandhabt hat, mag hier dahinstehen,

beachtliche Kritik bei Bretthauer/Spiecker gen. Döhmann, JZ 2020, 990 ff.

Jedenfalls lassen sie sich auf das vorliegende Verfahren nicht übertragen. Der Antragsteller begehrt nicht – und könnte im sozialgerichtlichen Eilverfahren auch nicht erlangen – eine generelle Außerkraftsetzung der Vorschriften über das Datentransparenzverfahren. Es geht ihm lediglich um die vorläufige Unterlassung einer Übermittlung der ihn betreffenden Gesundheitsdaten durch die Antragsgegnerin. Eine Entscheidung hierüber zeitigt keine Rechtswirkungen über den Einzelfall hinaus. Es besteht kein Anlass, sie an gesteigerte Voraussetzungen zu binden.

Zweitens unterscheiden sich die Prüfungsmaßstäbe im Eilverfahren vor dem Bundesverfassungsgericht und im sozialgerichtlichen Eilverfahren. Das Bundesverfassungsgericht entscheidet über Eilanträge nach § 32 BVerfGG nach ständiger Rechtsprechung grundsätzlich – und so auch im Fall des Datentransparenzverfahrens – auf der Grundlage einer Folgenabwägung. Die Erfolgsaussichten in der Hauptsache bleiben dabei in der Regel außer Betracht,

vgl. etwa BVerfGE 132, 195 (232); 151, 152 (160).

Hingegen kommt es im Eilverfahren nach § 86b Abs. 2 SGG maßgeblich auf den Anordnungsanspruch und damit den in der Hauptsache geltend gemachten materiellen Anspruch an. Da sich im vorliegenden Verfahren aufgrund einer reinen Rechtsprüfung eindeutig feststellen lässt, dass der Anordnungsanspruch besteht, ist eine Folgenabwägung, wie sie das Bundesverfassungsgericht vorgenommen hat, hier entbehrlich und auch nicht zulässig.

Drittens beruht der von dem Antragsteller geltend gemachte Unterlassungsanspruch nicht allein auf den Grundrechten des Grundgesetzes, auf die sich die Kontrollbefugnis des Bundesverfassungsgerichts grundsätzlich beschränkt, sondern auch auf unionsrechtlichen Regelungen. Damit ist der unionsrechtliche

Effektivitätsgrundsatz zu beachten, der die Verfahrensautonomie der Mitgliedstaaten beschränkt. Der Effektivitätsgrundsatz gebietet den Mitgliedstaaten unter anderem, einen wirksamen Eilrechtsschutz bereitzustellen, durch den der Vollzug unionsrechtswidriger mitgliedstaatlicher Gesetze vorläufig unterbunden werden kann,

> EuGH, Urteil vom 19. Juni 1990, Rs. C-213/89 – Factortame, Rn. 17 ff.

Die Wirksamkeit des sozialgerichtlichen Eilrechtsschutzes gegen bevorstehende behördliche Handlungen auf der Grundlage eines unionsrechtswidrigen Gesetzes darf darum nicht durch überzogene Anforderungen an die Nachteile beeinträchtigt werden, die der betroffenen Person durch diese Handlungen drohen. Insbesondere der von dem Bundesverfassungsgericht hervorgehobene Respekt vor den Regelungsentscheidungen des demokratisch legitimierten Gesetzgebers mag im Rahmen der Gewaltengliederung des Grundgesetzes einen Grund für besonders hohe Anforderungen im Eilverfahren darstellen. Dieser Grund lässt sich jedoch nicht auf die unionsrechtlichen Bindungen der Mitgliedstaaten übertragen. Aus unionsrechtlicher Sicht kommt es nicht darauf an, welchem Hoheitsorgan eines Mitgliedstaats ein Unionsrechtsverstoß primär zuzurechnen ist. Wesentlich ist, dass der Verstoß wirksam abgestellt wird. Dies haben die mitgliedstaatlichen Gerichte zu gewährleisten.

(Prof. Dr. Bäcker)

Anlagen

1. Verfahrensvollmacht
2. Schreiben des Antragstellers vom 1. März 2022
3. Schreiben der Antragsgegnerin vom 8. März 2022
4. Schreiben des Antragstellers vom 15. März 2022 (Widerspruch)
5. Schreiben der Antragsgegnerin vom 12. April 2022
6. Schreiben des Antragstellers vom 19. April 2022
7. Gutachten von Professor Dominique Schröder