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

Mannheim, den 2. Mai 2022

Sozialgericht Berlin
Invalidenstraße 52
10557 Berlin

Klage

und

Antrag auf Erlass einer einstweiligen Anordnung

der Frau Dr. Constanze Kurz,
... Berlin

– Klägerin und Antragstellerin –

g e g e n

Novitas BKK,
Schifferstr. 92-100, 47059 Duisburg

– Beklagte und Antragsgegnerin –

Namens und in beigefügter Vollmacht der Klägerin **(Anlage 1)** erhebe ich Klage mit dem Antrag,

> die Beklagte zu verurteilen, die Übermittlung der die Klägerin 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 zu unterlassen.

Des Weiteren beantrage ich, im Wege der einstweiligen Anordnung

> der Beklagten die Übermittlung der die Klägerin 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 bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens zu untersagen.

Ich rege an, spätestens vor einer Entscheidung in der Hauptsache dem Gerichtshof der Europäischen Union im Vorabentscheidungsverfahren nach Art. 267 AEUV die folgenden Fragen zur Auslegung des Unionsrechts 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: Sind Art. 6 Abs. 1 Satz 1 lit. c und e, Abs. 3 Satz 3 und 4 und Art. 9 Abs. 2 lit. h, i und j DSGVO im Lichte von Art. 7 und Art. 8 GRCh so auszulegen, dass eine mitgliedstaatliche Regelung, die ein Datentransparenzverfahren wie das in §§ 303a ff. SGB V vorgesehene einrichtet, den betroffenen Versicherten das Recht einräumen muss, der Verarbeitung sie betreffender Gesundheitsdaten im Rahmen des Datentransparenzverfahrens generell oder hinsichtlich bestimmter Datennutzungen zu widersprechen?

4. Falls Frage 2 und/oder Frage 3 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?

Darüber hinaus rege ich an, die nach Auffassung des Gerichts relevantesten Fragen zur Auslegung des Unionsrechts dem Gerichtshof der Europäischen Union bereits vor einer Entscheidung über den Antrag auf Erlass einer einstweiligen Anordnung im beschleunigten Vorabentscheidungsverfahren (Art. 23a der Satzung des Gerichtshofs der Europäischen Union, Art. 105 f. der Verfahrensordnung des Gerichtshofs der Europäischen Union) vorzulegen.

Gliederung

A. Vorbemerkung: Verfahrensgegenstand und aufgeworfene Rechtsfragen im Überblick

Die Klägerin und Antragstellerin wendet sich dagegen, dass die Beklagte im Rahmen des sogenannten Datentransparenzverfahrens sie 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.

Das vorliegende Verfahren zielt nicht darauf ab, das Datentransparenzverfahren ersatzlos zu beseitigen. Die Klägerin und Antragstellerin stellt nicht in Frage, dass dieses Verfahren legitimen und gewichtigen Zielen dient. Die gesetzliche Ausgestaltung des Datentransparenzverfahrens weist jedoch in zweierlei Hinsicht gravierende Mängel auf. Wegen dieser Mängel verletzen die Rechtsgrundlagen des Verfahrens in ihrer gegenwärtigen Form sowohl Verfassungsrecht als auch Unionsrecht und sind deshalb unanwendbar.

Erstens ist die Sicherheit der im Datentransparenzverfahren verarbeiteten Gesundheitsdaten gegen unbefugte Zugriffe nur unzureichend gewährleistet. 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.

Zweitens sehen die Rechtsgrundlagen des Datentransparenzverfahrens vor, dass die betroffenen Versicherten auf die Verarbeitung der sie betreffenden Daten keinen Einfluss haben. Auch wenn das Anliegen nachvollziehbar ist, einen möglichst umfassenden Datenbestand zusammenzutragen, ist eine derartige zwangsweise Datenhaltung und Datennutzung den Versicherten nicht zumutbar. Angesichts der außerordentlichen Sensibilität der verarbeiteten Daten muss den Versicherten vielmehr zumindest gegen besonders riskante Datennutzungen ein Widerspruchsrecht eingeräumt werden.

Die Klägerin und Antragstellerin regt an, spätestens vor einer Entscheidung in der Hauptsache den Gerichtshof der Europäischen Union im Wege des Vorabentscheidungsverfahrens zu befassen, um die im vorliegenden Verfahren aufgeworfenen Grundsatzfragen des europäischen Datenschutzrechts verbindlich klären zu lassen. Sie regt weiterhin an, die nach Auffassung des Gerichts bedeutsamsten Fragen bereits vor einer Entscheidung über den Antrag auf Erlass einer einstweiligen Anordnung im Wege eines beschleunigten Vorabentscheidungsverfahrens 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 und 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.

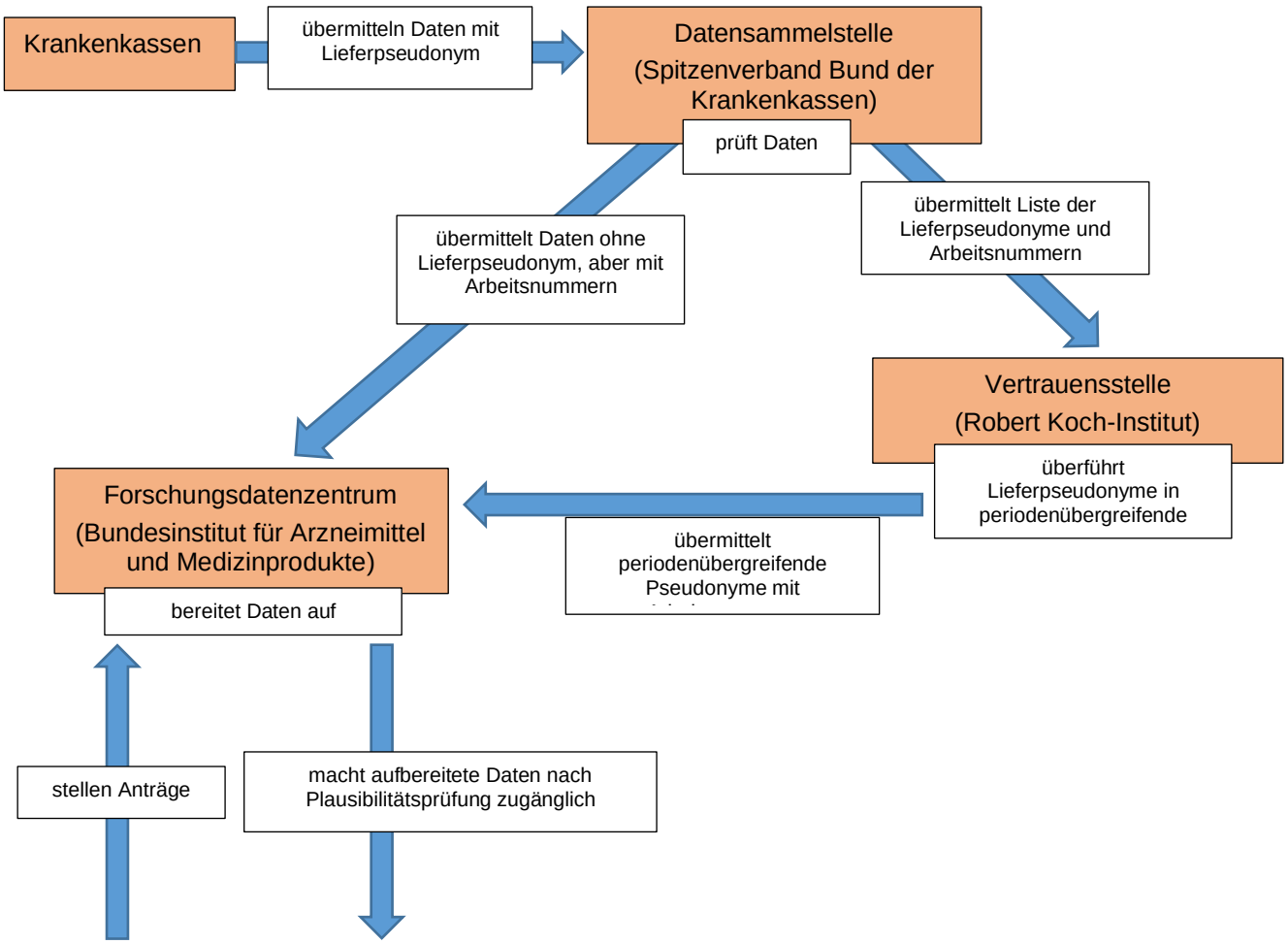
Das Robert Koch-Institut überführt gemäß § 303c SGB V i.V.m. § 6 DaTraV die ihm übermittelten Lieferpseudonyme in periodenübergreifende Pseudonyme. Die periodenübergreifenden Pseudonyme ermöglichen es, die Daten dauerhaft einer bestimmten versicherten Person zuzuordnen, um auf dieser Grundlage beispielsweise 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 der pseudonymisierten 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. Verfahrensgeschichte

Die am ... geborene Klägerin und Antragstellerin ist Informatikerin und Hackerin. Sie ist eine anerkannte Expertin unter anderem für Fragen des Datenschutzes und der IT-Sicherheit. Sie ist Autorin mehrerer Sachbücher zu Fragen der Digitalisierung, wurde mehrfach als Sachverständige vom Bundesverfassungsgericht angehört und war Mitglied der Enquête-Kommission Internet und digitale Gesellschaft des Deutschen Bundestags. Die Klägerin und Antragstellerin ist bei der Beklagten und Antragsgegnerin in der gesetzlichen Krankenversicherung pflichtversichert (Krankenversicherungsnr. ...).

Mit Schreiben vom 12. März 2022 **(Anlage 2)** forderte die Klägerin und Antragstellerin die Beklagte und Antragsgegnerin auf, von einer Übermittlung sie betreffender personenbezogener Daten an die Datensammelstelle abzusehen. Zur Begründung berief sich die Klägerin und Antragstellerin zum einen auf verschiedene Sicherheitsmängel des Datentransparenzverfahrens, die durch die gesetzliche und verordnungsrechtliche Gestaltung dieses Verfahrens angelegt würden. Zum anderen machte die Klägerin und Antragstellerin geltend, die Regelungen über das Datentransparenzverfahrens seien unverhältnismäßig, weil sie den betroffenen Versicherten kein Recht zum Widerspruch gegen die Datenverarbeitung einräumten.

Die Beklagte und Antragsgegnerin erwiderte hierauf mit Schreiben vom 26. April 2022 **(Anlage 3)**, die Datenverarbeitung beruhe auf Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 303b SGB V, ein Widerspruchsrecht bestehe nicht. Sie könne der Aufforderung der Klägerin und Antragstellerin daher nicht nachkommen.

C. Zulässigkeit der Klage

Die Klage ist gemäß § 54 Abs. 5 SGG als Leistungsklage in der Form der (vorbeugenden) Unterlassungsklage statthaft. Die Klägerin begehrt von der Beklagten die Unterlassung eines Realakts, nämlich der Datenübermittlung an die Datensammelstelle. Ein Verwaltungsakt ergeht in diesem Zusammenhang nicht.

Zwar soll es nach verbreiteter Rechtsauffassung einen Verwaltungsakt darstellen, wenn eine Behörde sich weigert, ein geltend gemachtes datenschutzrechtliches Betroffenenrecht zu erfüllen. Hiergegen sollen ein Anfechtungswiderspruch und nachfolgend eine Anfechtungsklage statthaft sein, wobei die Anfechtungsklage mit einem Leistungsantrag zu verbinden sei,

> vgl. etwa zum Widerspruchsrecht des Art. 21 DSGVO Kamann/Braun, in: Ehmann/Selmayr, DSGVO, Art. 21 Rn. 69; 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; hingegen für eine Verpflichtungsklage zum Auskunftsrecht des Art. 15 DSGVO BVerwG, Urteil vom 16. September 2020 – 6 C 10.19 –, juris, Rn. 12.

Dieser Rechtsauffassung liegt die Erwägung zugrunde, dass die Behörde die tatbestandlichen Voraussetzungen des geltend gemachten Betroffenenrechts zu prüfen und verbindlich zu klären hat, bevor sie dieses Recht durch einen Realakt erfüllt, und dass die Behörde besondere verfahrensrechtliche Vorkehrungen wie die Begründungspflichten des Art. 12 DSGVO zu beachten hat,

> so BVerwG, Urteil vom 16. September 2020 – 6 C 10.19 –, juris, Rn. 12.

Der vorliegende Fall liegt jedoch anders. Die Klägerin hat gegenüber der Beklagten keines der Betroffenenrechte der Art. 12 ff. DSGVO ausgeübt. Sie macht vielmehr geltend, dass es für die Datenübermittlung durch die Beklagte an die Datensammelstelle an der erforderlichen Übermittlungserlaubnis fehlt, weil die Rechtsgrundlagen des Datentransparenzverfahrens höherrangiges Recht verletzen und unanwendbar sind. Maßgeblich für die Berechtigung ihres Begehrens sind danach nicht die tatbestandlichen Voraussetzungen einer spezifischen Anspruchsgrundlage und zugehörige Verfahrensregelungen, sondern eine Prüfung des materiellen Rechts, wie sie jedem

Verwaltungshandeln (einschließlich Realakten) zugrunde liegt. Im Ergebnis dieser Prüfung liegt keine verbindliche Einzelfallentscheidung, die als Verwaltungsakt einzustufen wäre.

Die Unterlassungsklage ist zulässig. Die Klägerin ist analog § 54 Abs. 1 Satz 2 SGG klagebefugt, da die gesetzlich angeordnete Datenübermittlung in ihre 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 die Klägerin von der Beklagten verlangen kann, die Datenübermittlung zu unterlassen.

Das für die von der Klägerin erhobene vorbeugende Unterlassungsklage erforderliche qualifizierte Rechtsschutzinteresse besteht. Die Datenübermittlung, gegen die sich die Klägerin wendet, ist gesetzlich zu einem bestimmten Stichtag vorgesehen und darum konkret absehbar. Die Klägerin kann nicht auf einen nachträglichen Rechtsschutz verwiesen werden, da dieser für sie mit unzumutbaren Nachteilen verbunden wäre. In der gesetzlich vorgesehenen Datenübermittlung liegt gegenüber der Klägerin ein Grundrechtseingriff, der sich im Rahmen eines nachträglichen Rechtsschutzverfahrens nicht mehr rückgängig machen ließe. Zudem könnte die Klägerin auf diese Weise die sie belastenden Folgen der Datenübermittlung nicht mehr zuverlässig ausräumen.

Die Beklagte hat, sobald sie die Daten an die Datensammelstelle übermittelt hat, auf die weitere Datenverarbeitung keinen Einfluss mehr. Die Klägerin könnte gegenüber der Beklagten nach der Datenübermittlung daher lediglich die Feststellung begehren, dass die Datenübermittlung rechtswidrig war. Das Ziel der Klägerin, dass es zu einer Datenübermittlung und zu den daran anschließenden Datenverarbeitungsschritten gar nicht erst kommt, ließe sich auf diesem Weg nicht erreichen.

Ein nachträglicher Rechtsschutz, der die Datenverarbeitung stoppt, käme darum von vornherein nur gegenüber den anderen am Datentransparenzverfahren beteiligten Stellen in Betracht. Hierzu müsste die Klägerin von einer dieser Stellen die Löschung der sie betreffenden Daten verlangen. Dies ist der Klägerin jedoch nicht zumutbar, da sie so ihre 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 die Klägerin nur anhand von Pseudonymen identifizierbar, die ihr nicht bekannt sind. Um einen

Löschungsanspruch überhaupt substantiieren zu können, müsste sich die Klägerin zunächst das Pseudonym beschaffen, unter dem ihre Daten in dem jeweiligen Datenbestand gespeichert sind. Hierzu müsste sie sich mindestens an eine weitere, teils an mehrere Stellen wenden. Um beispielsweise gegenüber dem Forschungsdatenzentrum die zu löschenden Daten zu bezeichnen, müsste sich die Klägerin zunächst bei der Beklagten das Lieferpseudonym beschaffen, unter dem die Beklagte die Daten an die Datensammelstelle übermittelt hat. Anschließend müsste die Klägerin 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. Die Klägerin müsste sich insbesondere gegenüber der Vertrauensstelle und nachfolgend dem Forschungsdatenzentrum identifizieren, obwohl diese Stellen ihre Identität gerade nicht kennen sollen.

Zum anderen könnte die Klägerin durch einen nachträglichen Rechtsschutz nicht verhindern, dass bis zur gerichtlichen Entscheidung die sie betreffenden Daten im Rahmen des Datentransparenzverfahrens verarbeitet werden. Die Klägerin wendet sich gegen die bevorstehende Datenübermittlung aber gerade, weil nach ihrer Auffassung das Datentransparenzverfahren unzumutbare Sicherheitsrisiken begründet und die Datenverarbeitung den betroffenen Personen nicht gegen ihren Willen zugemutet werden kann. Mit einem Verweis auf einen nachträglichen Rechtsschutz würde der Klägerin angesonnen, gerade die Rechtsbeeinträchtigungen und Grundrechtsgefährdungen, gegen die sie sich wendet, für einen nicht genau absehbaren gerichtlichen Entscheidungszeitraum irreversibel hinzunehmen.

D. Begründetheit der Klage

Die Klage ist begründet. Die Datenübermittlung von der Beklagten an den Spitzenverband Bund der Krankenkassen bedarf einer gesetzlichen Übermittlungserlaubnis, die mit höherrangigem Recht in Einklang steht (unten I). Die Erlaubnisregelung in § 303b Abs. 1 SGB V ist jedoch sowohl unionsrechts- als auch verfassungswidrig. Hierfür gibt es zwei Gründe. Erstens ist die Sicherheit der übermittelten Daten im Datentransparenzverfahren nur unzureichend gewährleistet (unten II). Zweitens ist es den Versicherten nicht zumutbar, die Verarbeitung der sie betreffenden Daten im Datentransparenzverfahren generell gegen ihren Willen hinzunehmen (unten III). Die Verstöße gegen höherrangiges Recht führen zur Unanwendbarkeit der Regelungen über das Datentransparenzverfahren. Die Klägerin kann daher von der Beklagten verlangen, die Übermittlung der sie betreffenden Daten zu unterlassen (unten IV).

I. Erfordernis einer unionsrechts- und verfassungskonformen gesetzlichen Übermittlungserlaubnis

Die Datenübermittlung von der Beklagten an den Spitzenverband Bund der Krankenkassen als Datensammelstelle hat personenbezogene Daten der Klägerin 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 DSGVO in den sachlichen 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.).

Sollte das Gericht gleichwohl Zweifel haben, ob die in § 303b Abs. 1 Satz 1 SGB V i.V.m. § 3 DaTraV vorgesehene Datenübermittlung in den sachlichen Anwendungsbereich der DSGVO fällt, so wird **angeregt**, diese Frage durch

ein Vorabentscheidungsverfahren nach Art. 267 AEUV verbindlich klären zu lassen.

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 vier 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 ist für dieses Verfahren ohne Belang. 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 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 viertens 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).

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 etwa 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, zur Versorgung mit Heil- und Hilfsmitteln und mehr, 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 der Klägerin vorprozessual eingeholte Gutachten von Professor Dominique Schröder **(Anlage 4)**, 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. 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. Zu weiteren Erläuterungen ist auch die Klägerin als anerkannte Expertin für IT-Sicherheit in der Lage.

Sollte das Gericht die unionsrechtlichen Anforderungen an die Datensicherheit für offen halten, wird **angeregt**, den Gerichtshof der Europäischen Union im Wege eines Vorabentscheidungsverfahrens nach Art. 267 AEUV zu befassen.

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 Vorgehen, 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 bei den Krankenkassen verortet 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.

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 überhaupt 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 Antragsteller 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, derzufolge 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.

III. Fehlen eines Widerspruchsrechts

Die Regelungen über das Datentransparenzverfahren verletzen auch in materieller Hinsicht höherrangiges Recht. Sie stehen mit 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 nicht in Einklang, da sie die lang andauernde Speicherung und Nutzung höchst sensibler Daten in großem Umfang auch gegen den erklärten Willen der betroffenen Personen vorsehen.

Die betroffenen Versicherten haben grundsätzlich keine Möglichkeit, die Verarbeitung der sie betreffenden Gesundheitsdaten im Datentransparenzverfahren zu verhindern oder einzuschränken. In manchen Fällen mögen die Widerspruchsrechte aus Art. 21 Abs. 1 und 6 DSGVO greifen. Diese setzen jedoch voraus, dass sich die widersprechende betroffene Person in einer „besonderen Situation“ befindet, gelten also jedenfalls nicht für alle Versicherten. Auch die Klägerin und Antragstellerin befindet sich nicht in einer solchen besonderen Situation. Im Übrigen geht zumindest die Bundesregierung davon aus, dass ein Widerspruchsrecht nach Art. 21 Abs. 6 DSGVO gegen die Datenverarbeitungen im Datentransparenzverfahren generell nicht besteht,

> Stellungnahme der Bundesregierung zum Tätigkeitsbericht 2020 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 1. Juli 2021, S. 11 **(Anlage 5)**.

Zur Wahrung des Verhältnismäßigkeitsgrundsatzes bedarf es jedoch eines allgemeinen Widerspruchsrechts aller betroffenen Versicherten zumindest gegen bestimmte Datenverarbeitungen im Datentransparenzverfahren,

> 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.

Dem Erfordernis eines gesetzlichen Widerspruchsrechts lässt sich nicht entgegenhalten, an den Datenverarbeitungen im Datentransparenzverfahren bestehe ein großes öffentliches Interesse, das dem Widerspruchsinteresse der betroffenen Versicherten im Rahmen einer Abwägung vorgehe. 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. Ihr konkretes Gewicht hängt jedoch von dem einzelnen Auswertungsprojekt ab, für das die Daten genutzt werden sollen. Es liegt jedenfalls fern, dass die Nutzungszwecke zwingend in jedem Einzelfall schwerer wiegen als das Widerspruchsinteresse der betroffenen Versicherten.

Hierbei ist auch zu beachten, dass ein einzelner Widerspruch das öffentliche Nutzungsinteresse für sich genommen nur marginal beeinträchtigt, da für die Ziele des Datentransparenzverfahrens eine lückenlose Sammlung der Gesundheitsdaten aller gesetzlich Versicherten nicht benötigt wird. Schließlich kommt das Verfahren auch ohne Gesundheitsdaten der privat Versicherten aus. Zu einer signifikanten Beeinträchtigung öffentlicher Erkenntnisinteressen kommt es erst durch eine Häufung von Widersprüchen, die eine kritische Schwelle überschreitet. Einem denkbaren generellen Vorrang des

Nutzungsinteresses vor dem Widerspruchsinteresse läge somit die Prognose zugrunde, dass dann, wenn den betroffenen Personen ein Widerspruchsrecht zuerkannt wird, ein kritischer Anteil von ihnen 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 ausnutzen, grundlegend Thaler/Sunstein, Nudge: Wie man kluge Entscheidungen anstößt, 2009.

Es ist darum davon auszugehen, dass von einem bestehenden Widerspruchsrecht nur eine kleine Minderheit der Versicherten Gebrauch machen wird, sodass sich negative Auswirkungen auf öffentliche Erkenntnisinteressen in Grenzen halten dürften. Die Klägerin 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.

Gegen das Erfordernis eines allgemeinen Widerspruchsrechts lässt sich auch 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 auch 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.

Für die Gestaltung des Widerspruchsrechts sind unterschiedliche Optionen denkbar. Wird davon ausgegangen, dass die Datenverarbeitung im Datentransparenzverfahren den betroffenen Versicherten generell nicht gegen ihren Willen zuzumuten ist, so muss ein Widerspruchsrecht bereits gegen die Datenübermittlung durch die Krankenkassen an die Datensammelstelle vorgesehen werden. Nimmt man hingegen an, dass die Versicherten lediglich einzelnen Datennutzungen widersprechen können müssen, so ist ein beschränktes Widerspruchsrecht einzurichten, das gegen die Krankenkassen oder auch gegen das Forschungsdatenzentrum geltend zu machen wäre. Ein Widerspruchsrecht gegenüber dem Forschungsdatenzentrum würde allerdings voraussetzen, dass das gesamte Verfahren der Datensammlung umgestaltet wird. Im Einzelnen müssen diese Optionen im vorliegenden Verfahren nicht näher erörtert werden. Die Rechtsgrundlagen des Datentransparenzverfahrens verletzen jedenfalls deshalb höherrangiges Recht, weil sie überhaupt kein Widerspruchsrecht vorsehen.

Sollte das Gericht Zweifel haben, ob sich aus dem Verhältnismäßigkeitsgrundsatz für bestimmte Fallkonstellationen oder allgemein das Erfordernis eines gesetzlichen Widerspruchsrechts ableiten lässt, wird **angeregt**, diese Frage durch ein Vorabentscheidungsersuchen nach Art. 267 AEUV klären zu lassen.

IV. Rechtsfolge

Sowohl die mangelhafte Gewährleistung der Datensicherheit als auch das Fehlen eines gesetzlichen Widerspruchsrechts haben zur Folge, dass die Regelungen über das Datentransparenzverfahren insgesamt höherrangiges Recht verletzen. Insbesondere der Unionsrechtsverstoß führt dazu, dass diese Regelungen unanwendbar sind. Der Beklagten fehlt es darum an der erforderlichen gesetzlichen Erlaubnis zur Datenübermittlung an die Datensammelstelle. Sie hat diese Datenübermittlung zu unterlassen.

Auf diese Unterlassung hat die Klägerin einen Anspruch. 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.

Sollte das Gericht Zweifel daran haben, dass die betroffene Person von dem Verantwortlichen verlangen kann, eine konkret absehbare rechtswidrige Datenverarbeitung zu unterlassen, so wird **angeregt**, diese Frage durch ein Vorabentscheidungsersuchen nach Art. 267 AEUV klären zu lassen.

E. Antrag auf Erlass einer einstweiligen Anordnung

Der Eilantrag ist als Antrag auf Erlass einer Sicherungsanordnung nach § 86b Abs. 2 Satz 1 SGG statthaft und auch ansonsten zulässig.

Der Antrag ist begründet. Der Anordnungsanspruch ergibt sich aus dem oben im Einzelnen begründeten Anspruch der Antragstellerin gegen die Antragsgegnerin, die Übermittlung der die Antragstellerin betreffenden Gesundheitsdaten an die Datensammelstelle zu unterlassen. Der Anordnungsgrund folgt daraus, dass die jederzeit und spätestens zum 1. Oktober 2022 drohende Datenübermittlung einen für sich genommen nicht reversiblen Eingriff in die Grundrechte der Antragstellerin 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 die Antragstellerin 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 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. Die Antragstellerin begehrt nicht – und könnte im sozialgerichtlichen Eilverfahren auch nicht erlangen – eine generelle Außerkraftsetzung der Vorschriften über das Datentransparenzverfahren. Es geht ihr lediglich um die vorläufige Unterlassung einer Übermittlung der sie 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.

Drittens beruht der von der Antragstellerin 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 der Klägerin und Antragstellerin vom 1. März 2022
3. Schreiben der Beklagten und Antragsgegnerin vom 26. April 2022
4. Gutachten von Professor Dominique Schröder
5. Stellungnahme der Bundesregierung zum Tätigkeitsbericht 2020 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 1. Juli 2021 (Auszug)